International Telecommunication Union

Security in Telecommunications and Information Technology

An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications

re-published

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

2024

Foreword

Seizo Onoe
Director
ITU Telecommunication Standardization Bureau

Information and communication technologies (ICTs) continue growing in number and variety. They are essential to business and daily life, and every industry sector is transforming with the help of ICTs. This calls for a culture of security by design, and attention to security throughout ICT lifecycles.

This 8th edition of our Security Manual supports our work to help everyone capitalize on ITU standards and associated security best practices.

ITU standards make an essential contribution to building confidence and security in the use of ICTs, a core component of ITU's mandate. Our standardization work on security is led by ITU-T Study Group 17, where experts from around the world work together year-round to ensure that ITU standards keep pace with the evolution of ICTs and threats to security.

The unique membership composition of ITU – including governments, companies, academia, and civil society – makes Study Group 17 a valuable platform to support synergy in security actions relevant to policy, business, and technology.

Key topics on the group's agenda include security aspects of artificial intelligence and machine learning, distributed ledger technologies and blockchain, cloud computing and Internet of Things autonomous driving, IMT-2020 (5G), quantum information technologies, privacy protection, and software supply chain security. In addition, the group's work on cybersecurity and incident response supports the monitoring, reporting, and sharing of security and vulnerability information.

This Security Manual provides an overview of our well-established and emerging security work and highlights the extensive ITU resources available for ICT developers and users to understand and address today's security challenges.

I thank the experts from the around the world contributing to Study Group 17 for their dedication to the development and promotion of our standards, guidelines, best practices, and awareness-building publications. The content of this manual is the result of your tireless work to safeguard our digital environment and everyone that relies on it.

.

Pre-published

Acknowledgements

This manual was prepared with the contribution of numerous authors who either contributed to the generation of the relevant ITU-T Recommendations or participated in the ITU-T Study Group meetings, workshops, and seminars. Credit should be given to the Chairs, Secretariats, Rapporteurs, editors, and security coordinators of the ITU Study Groups, to Xiaoya Yang, SG17 counsellor, Martin Euchner, the former SG17 Advisor, Georges Sebek, the former SG17 counsellor, and in particular to Herbert Bertine and Arkadiy Kremer, the former SG17 Chairs, and Heung Youl Youm, the Chair of the lead Study Group in ITU-T for work on telecommunications security, Kyeong Hee Oh, the editor of this manual and Mike Harrop, the former editor of this manual.

Pre-published

Welcome remark to this Security Manual

Heung Youl Youm
Chair of ITU-T SG17

This version of Security Manual mainly describes major security works that have been achieved by ITU-T study groups, especially by ITU-T SG17 since 2003.

Given that building confidence and security in the use of information and communication technologies (ICTs) is one of the top priorities of the ITU, it is critical that this security competence in ITU-T be nurtured, expanded, and enhanced, and not fragmented. Study Group 17 is a center of excellence – a core competency in security, and technical aspects of data protection, as the lead study group in security in ITU-T.

New security approaches and measures to adequately address security threats and risks may be required. Study Group 17 has a key role to play in development of international standards in the security area.

Providing security by ICTs and ensuring security for ICTs are both major study areas for Study Group 17. Security of and for telecommunications and ICT remains an area where security standards will be needed. Managing new emerging threats in telecommunication and ICTs, including network infrastructure, applications and services, is extremely critical. It is understood the imperative for developing implementable standards and guidelines on security that meet the needs of all countries.

Strengthening the security framework and protection of personally identifiable information (PII) is a prerequisite for the development of the highly connected Information Society and for building confidence, trust and security among users of Information and Communication Technologies (ICTs).

Emerging ICT technologies such as smart factory, intelligent transportation systems, the 6th generation of cellular network and beyond, Internet of things, distributed ledger technologies, metaverse, digital twin, AI/ML related security and quantum safe communication, need technical and organizational measures to address various threats and risks.

SG17 is also addressing identity management (IdM), a key technological enabler for managing digital identities, establishing trust, protecting personally identifiable information, operating networks, and performing online e-transactions. As it plays such a critical role in building confidence and security in the use of ICTs, identity management is integral to the activities of Study Group 17 as the study group.

PKI was originally not designed to cope with entities constrained in terms of processing power, storage, bandwidth, battery capacity, etc. However, in the era of IoT, millions or billions constrained devices are connected and communicated without human intervention. In recent editions of Rec. ITU-T X.509 | ISO/IEC 9594-8, PKI has been extended to cope with this new environment. Further extensions in the area have high priority.

I believe that this manual provides a basis for promoting greater awareness to stakeholders on SG17 and other study groups achievements carried out within the ITU-T in strengthening security culture and in building confidence and security in the use of ICTs.

In closing, I would like to thank the many dedicated individuals within ITU-T study groups, especially editor of this manual, Ms Kyeong Hee Oh, who contributed to this Security Manual.

Pre-published

Executive Summary

Telecommunications/ICT has become a fundamental way of doing business in the highly connected world for public, private, and non-profit organizations, as well as individual consumers and citizens. Its undoubted benefits also bring new threats and risks. These can range those arising from devices, networks, applications, and services. New organizational and technical security measures may be required to adequately address these security threats and risks.

This manual provides a broad introduction to the Information and Communication Technology (ICT) security work of the ITU-T, and more specifically, it summarizes how the ITU-T is responding to global cybersecurity challenges with Recommendations, technical reports, guidance documents and outreach initiatives. It is primarily directed towards those who have responsibility for, or are interested in, information and communications security in organizations and the related standards, as well as those who simply need to better understand ICT security issues.

The manual can be used in various ways according to the organization, role and needs of the user. The introductory chapters provide an overview of the key areas of the current ITU-T security work together with a discussion of the basic requirements for the protection of ICT applications, services, and information. The threats and vulnerabilities that drive security requirements are highlighted and the role of standards in meeting the requirements is examined. Some of the features that are needed to protect the various entities involved in providing, supporting, and using information and communications technology and services are discussed. In addition, the importance of ICT security standards is explained, and examples are given of how the ITU-T security work is evolving to meet security requirements.

The generic security architectures for open systems and end-to-end communications are then introduced together with some examples of application-specific architectures. These architectures each establish a framework within which the multiple facets of security can be applied in a consistent manner. They also standardize the underlying concepts of security services and mechanisms and contribute to a standardized vocabulary for ICT security terms and basic concepts. The general principles introduced in these architectures form the basis for many of the other standards on security services, mechanisms, and protocols, some of which are discussed later in the text.

Security management embraces many activities and processes associated with controlling and protecting access to system and network resources, event monitoring and reporting, and auditing, as well as managing the information related to these functions and activities according to policies. The topics of information security management, risk management and asset management are the focus of one section. Management activities associated with securing the network infrastructure are discussed later in the text in a section that covers the need to secure the data used to monitor and control the telecommunications network, as well as topics related to network management, common security management services and the governance of information security. Telecommunications operators need to care about the management of personally identifiable information (PII) because they may need to process the PII of their customers.

The Directory and its role in supporting authentication and other security services are explained along with some of the key areas that depend on Directory services. In particular, this section explains some of the cryptographic concepts that rely on Directory services and provides an introduction to public key infrastructures, digital signatures and privilege management infrastructures. The importance of protecting the Directory information base is also discussed.

The topic of identity management is of growing importance in response to the proliferation of identity theft. Strong authentication protocols and the use of biometric characteristics for personal identification and authentication are becoming essential in telecommunication environments.

Some specific examples and approaches to network security are reviewed. These include the security requirements for Next Generation Networks and mobile communications networks which are in transition from

Pre-published

a single technology (such as CDMA or GSM) to mobility across heterogeneous platforms using the Internet protocol. Also, this section includes an examination of security provisions for home networks, cable television, ubiquitous sensor networks, and software-defined networking.

A section on cybersecurity and incident response looks at how best to develop an effective response to cyber-attacks, and the importance of understanding the source and nature of attacks and the need to share information with monitoring agencies. This section discusses the development of a framework for sharing cybersecurity-related information and requirements for detecting, protecting against, mitigating the effects of, and recovering from cyber-attacks.

The security needs of a number of application areas are examined with particular emphasis on the security features that are defined in ITU-T Recommendations. Topics discussed include Voice over Internet Protocol (VoIP), Internet protocol television (IPTV) and web services. Also included in this section is the topic of identification tags (including RFID tags) which are widely deployed but which are also the subject of growing concern over the risk of privacy infringement. As the application area is continuously expanding, the security concerns now include fax, web, tag-based and value-added services.

Technical measures for countering common network threats such as spam, malicious code and spyware are presented, and the importance of timely notification and dissemination of software updates and the need for organization and consistency in handling security incidents are discussed.

As the adoption of cloud services rapidly increases, security concerns are also growing. A security framework based on the characteristics of cloud computing services is presented. The security management controls of cloud services are provided from customers' and providers' perspectives. Discussions are expanding to other services in the cloud environment, such as virtual management systems based on cloud services.

Finally, recent activities are introduced in evolving areas, such as the Internet of Things (IoT), Intelligent Transport Systems (ITS), Distributed Ledger Technologies (DLT), and quantum-based communications for the future of ICT security standardization. These clauses should be treated as separate chapters in the next edition as technologies advance. IMT2020 (5G) might be included in the near future.

At the end of the text, a review of sources of additional information is included, along with Annexes on definitions and acronyms used in the manual, a summary of security-related Study Groups, and a complete listing of Recommendations referenced in this manual. In the electronic version of the text, links to some of the key ITU-T security resources and outreach information are included throughout.

Pre-published

Introduction to the 8th edition

Since the first edition of the manual was published in 2003, the ITU-T has embarked on many new areas of work and great many new Recommendations have been completed and published. In addition, the Study Groups themselves were restructured following the World Telecommunication Standardization Assembly (WTSA) 2016.

Since publication of the 7th edition of the manual, the work has continued to expand, and the number of security-related Recommendations has grown in response to continued demand for standardized solutions to counter evolving threats to ICT security. Once again, the editor has faced the challenge of presenting a representative cross-section of the work in a limited amount of space. For the 8th edition of this manual, the basic structure follows the 7th edition. Still, some chapters have additional clauses to cover the new areas, and updates have been made to reflect the achievement in this study period (2020-2024). The guiding principles established for the 4th edition of this manual, have again been followed for this edition.

The guiding principles, which were developed in consultation with ITU-T members, are as follows:

- The publication should appeal to a wide audience and should try to avoid complex terminology and terms that are likely to be understood only within specialized domains;
- The text should complement, not duplicate, existing material available in other forms (e.g. Recommendations);
- The text should be developed to accommodate publication as an electronic document;
- The text should employ web links to Recommendations and other referenced sources of publicly-available material as much as possible. Detailed information, over and above, needed to fulfil the basic objectives should be referenced by web links; and
- To the greatest extent possible, the text should focus on work that has been completed and published, rather than work that is planned or in progress.

In keeping with these objectives, the Security Manual does not attempt to cover all the ITU-T security work that has either been completed or is underway. Instead, it focuses on key selected topics and accomplishments that has been published and provides web links to additional information.

For readers using the electronic version of the text, direct hyperlinks are provided to the referenced Recommendations and to other on-line documentation. All referenced Recommendations are listed in Annex D. These can be accessed on line at: www.itu.int/rec/T-REC.

Note: This manual is purely illustrative. It has no normative character and does not supersede the ITU-T Recommendations referenced herein.

Pre-published

Table of Contents

Page

Pre-published

Pre-published

Pre-published

1. How to use this Security Manual

Pre-published

1 How to use this Security Manual

This manual has been developed to introduce the telecommunications security work of the ITU-T to senior executives and managers who have responsibility for, or an interest in, ICT security and the related standards. In addition, the manual will be of interest to others who want to gain a better understanding of ICT security issues and the corresponding ITU-T Recommendations that address those issues.

The manual provides an overview of telecommunication and information technology security, examines some of the associated practical issues, and indicates how different aspects of ICT security are being addressed by the ITU-T standardization work. The manual provides tutorial material as well as links to more detailed guidance and additional reference material. In particular, it provides direct links to ITU-T Recommendations and to related reference and outreach documents. It brings together selected security-related material from ITU-T Recommendations and it explains relationships of various aspects of the work. Results achieved in ITU-T security-related standardization since the sixth edition of the manual are included. For the most part, the manual focuses on work that has already been completed. The results of work currently in progress will be reflected in future editions of this manual.

In addition to the work of ITU-T, security work is also being undertaken by the General Secretariat and the other Sectors of the ITU. Examples include: Child Online Protection, an international collaborative network for action to promote the online protection of children worldwide; the Global Cybersecurity Index, a project to measure the cybersecurity capabilities of nation states and hence enable informed decisions to foster a global culture of cybersecurity; the Enhancing Cybersecurity in Least Developed Countries project which aims to ensure that LDCs can maximize the socio-economic benefits of access to ICTs in a cybersecure environment; National CIRT Capacity Building which addresses the absence of institutional structures to deal with cyber incidents and attacks by establishing national Computer Incident Response Teams (CIRTs); and the work of ITU-R on security for International Mobile Communications and satellite services.

This manual is intended to provide a broad, high-level overview of the security standards activities of the ITU-T. For those requiring more detailed information on the published Recommendations and related documentation, direct links are provided in the electronic version of the text. The manual can be used in several ways. Table 1 indicates how it can be used to address the needs of different audiences.

Pre-published

Table 1 – How the manual addresses the needs of different audiences

Organization	Specific audience	Needs	How the manual can address the needs
Telecommunication service providers	Senior executives / managers	Broad overview of scope of ICT security standardization efforts. High level roadmap to relevant ICT security standards	The manual directly addresses these needs
	Design and deployment engineers	Roadmap to relevant ICT security standards plus technical details associated with specific areas	The manual provides a roadmap plus links to detailed explanatory text The Recommendations provide technical details
Telecommunication service vendors	Senior executives / managers	Broad overview of scope of ICT security standardization efforts High level roadmap to relevant ICT security standards	The manual directly addresses these needs
	Product managers	Roadmap to relevant standards	The manual provides a roadmap plus links to detailed explanatory text
	Product design	Technical details associated with specific areas	The manual provides links to detailed explanatory text on specific areas The Recommendations provide technical details
End users	Technical	May be interested in technical details associated with specific areas	The manual provides links to detailed explanatory text on specific areas
	Non-technical	May be interested in broad overview of scope of ICT security standardization efforts	The manual directly addresses these needs
Academia	Students / Instructors	Roadmap to relevant standards Technical details associated with specific areas Awareness of new and upcoming ICT security standardization efforts	The manual provides a roadmap plus links to detailed explanatory text on specific areas
Government	Senior executives and managers Regulators Policy makers	Broad overview of scope of ICT security standardization efforts High level roadmap to relevant ICT security standards	The manual directly addresses these needs
Non-government organizations	Senior executives / managers	Broad overview of scope of ICT security standardization efforts High level roadmap to relevant ICT security standards	The manual directly addresses these needs
	Development and capacity building	Roadmap to relevant ICT security standards Technical details associated with specific areas	The manual provides links to detailed explanatory text on specific areas The Recommendations provide technical details

2. Overview of ITU-T security activities

Pre-published

2 Overview of ITU-T security activities

The ITU-T work on ICT security has been underway for over three decades, during which time Recommendations and guidance have been developed in a number of key areas by several Study Groups. Study Group 17 (SG17) now has primary responsibility for the ITU-T ICT security work and has also been designated the Lead Study Group on Security. However, aspects of security extend to most areas of the ITU-T work and most Study Groups are undertaking security work related to their own area of responsibility.

As part of its responsibility as Lead Study Group on Security, SG17 has developed a number of reference and outreach publications. These publications, which include this manual, help with the internal coordination of the ITU-T security work and also help to promote the work to a much wider community and to encourage the use of the Recommendations.

This section provides readers with a brief introduction to the major security topics together with examples of some of the security-related Recommendations. It also provides pointers to sources of further information on the outreach publications and the work currently underway.

2.1 Reference and outreach documentation

The ITU-T maintains a number of publications and web sites from which more detailed information about Recommendations and the ITU-T security work may be obtained.

The SG17 website provides a summary of the responsibilities and activities of SG17. Included on this website are summaries of, and links to, documentation and outreach material, information on past workshops, presentations and outreach activities, and links to ICT security guidance, including a tutorial on writing safe and secure programs.

One of the guidance is the Technical Report XSTR-SUSS, *Successful use of security standards*, which provides examples of how ITU-T Recommendations are used today in the marketplace to help protect networks, people, data, and critical infrastructure. This X.STR-SUSS focuses on how approved security-related ITU-T Recommendations can be successfully deployed. Examples of individual Recommendations (such as ITU-T X.805) and families of Recommendations (such as CYBEX) are considered.

More detailed information on various aspects of the security work along with direct links to further information is contained in section 16.

2.2 Overview of major security topics and Recommendations

Table 2 provides a quick reference to some of the major topics and associated Recommendations discussed in this manual. Hyperlinks are provided to the text on each topic and subtopic and to the listed Recommendations. Annex D contains a complete list of Recommendations referenced in this manual. Hyperlinks are included in Annex D to allow readers to download the Recommendations directly.

Pre-published

Table 2 – Overview of some of the key topics and selected Recommendations (Part 1 of 5)

Topic	Sub-topics	Examples of relevant Recommendations and publications	
Security requirements	Threats, risks and vulnerabilities (3.1)	ITU-T E.408	*Telecommunication networks security requirements*
		ITU-T X.1205	*Overview of cybersecurity*
	Personnel and physical security requirements (3.5)	ITU-T X.1051	*Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations*
	Next Generation Networks (10.1)	ITU-T Y.2701	*Security requirements for NGN release 1*
		ITU-T Y.2740	*Security requirements for mobile remote financial transactions in next generation networks*
	Security requirements for IPCablecom (10.4)	ITU-T J.170	*IPCablecom security specification*
	IPTV (12.2)	ITU-T X.1191	*Functional requirements and architecture for IPTV security aspects*
	Software-defined networking (10.7)	ITU-T X.1038	*Security requirements and reference architecture for software-defined networking*
	Security for Internet of Things(IoT) (15.1)	ITU-T Y.4100	*Common requirements of the Internet of things*
Security architectures	Open systems security architecture (4.1)	ITU-T X.800	*Security architecture for Open Systems Interconnection for CCITT applications*
	Security services (4.2)	ITU-T X.810	*Security frameworks for open systems: Overview*
	Security architecture for end-to-end communications (4.3)	ITU-T X.805	*Security architecture for systems providing end-to-end communications*
	Availability of the network and its components (4.3.2)	ITU-T G.827	*Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths*
	Application-specific architectures (4.5)	ITU-T X.1162	*Security architecture and operations for peer-to-peer networks*
		ITU-T X.1161	*Framework for secure peer-to-peer communications*
	Message security (4.5.2)	ITU-T X.1143	*Security architecture for message security in mobile web services*
	Network management architecture (9.2)	ITU-T M.3010	*Principles for a telecommunications management network*
	IPCablecom architecture (10.4.1)	ITU-T J.160	*Architectural framework for the delivery of time-critical services over cable television networks using cable modems*
	IPTV (12.2)	ITU-T X.1191	*Functional requirements and architecture for IPTV security aspects*
Security management	Information security management (5.1)	ITU-T X.1051	*Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations*
		ITU-T X.1052	*Information security management framework*
	Risk management (5.3)	ITU-T X.1055	*Risk management and risk profile guidelines for telecommunication organizations*
		ITU-T Y.Sup19	*Supplement on the risk analysis service in next generation networks*
	Personally Identifiable Information Protection (5.7)	ITU-T X.1058	*Code of practice for personally identifiable information protection*
	Security management for cyber defence centre (5.8)	ITU-T X.1060	*Framework for the creation and operation of a cyber defence centre*
	Incident handling (11.4)	ITU-T E.409	*Incident organization and security incident handling: Guidelines for telecommunication organizations*
	Asset management (5.4)	ITU-T X.1057	*Asset management guidelines in telecommunication organizations*
	Governance of information security (5.5)	ITU-T X.1054	*Governance of information security (equates to: ISO/IEC 27014)*
	Telecommunications management (9.1)	ITU-T M.3410	*Guidelines and requirements for security management systems to support telecommunications management*

Table 2 – Overview of some of the key topics and selected Recommendations (Part 2 of 5)

Sub-topics	Sub-topics	Sub-topics	
The role of the Directory	Directory concepts (6)	ITU-T X.500	*The Directory: Overview of concepts, models and services*
	Public-key security mechanisms (6.2)	ITU-T X.509	*The Directory: Public-Key and attribute certificate frameworks*
	Protocol for secure operations	ITU-T X.510	*The Directory: Protocol specifications for secure operations*
	Privilege management infrastructure (6.3)	ITU-T X.1171	*Threats and requirements for protection of personally identifiable information in applications using tag-based identification*
	Protection of Directory information (6.4)		
	Privacy protection (6.4.3)		
Identity management and telebiometrics	Identity management (7.1)	ITU-T X.1250	*Baseline capabilities for enhanced global identity management and interoperability*
	Overview of identity management (7.1.1)	ITU-T X.1251	*A framework for user control of digital identity*
	Key ITU-T identity management standards (7.1.2)	ITU-T X.1253	*Security guidelines for identity management systems*
		ITU-T Y.2720	*An NGN identity management framework*
		ITU-T Y.2722	*NGN identity management mechanisms*
		ITU-T X.1252	*Baseline identity management terms and definitions*
		ITU-T X.1277	*Universal authentication framework*
		ITU-T X.1278	*Client to authenticator protocol/Universal 2-factor framework*
		ITU-T X.1280	*Framework for out-of-band server authentication using mobile devices*
	Telebiometric authentication (7.2.1)	ITU-T X.1084	*Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems*
	Security and safety aspects of telebiometrics (7.2.3)	ITU-T X.1081	*The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics*
	Telebiometrics related to human physiology (7.2.4)	ITU-T X.1084	*Telebiometrics related to human physiology*
	Telebiometircs authentication using biosignals (7.2.5)	ITU-T X.1094	*Telebiometric authentication using biosignals*
	Telebiometrics in e-health and telemedicine (7.2.7)	ITU-T X.1092	*Integrated framework for telebiometric data protection in e-health and telemedicine*
	Telebiometircs in access control (7.2.9)	ITU-T X.1095	*Entity authentication service for pet animals using telebiometrics*
	Telebiometircs in entity authentication service for pet animals (7.2.9)	ITU-T X.1080.0	*Access control for telebiometrics data protection*
	Other developments in telebiometrics standards (7.2.11)	ITU-T X.1089	*Telebiometrics authentication infrastructure (TAI)*
Examples of approaches to authentication and non-repudiation	Secure password-based authentication protocol with key exchange (8.1)	ITU-T X.1151	*Guideline on secure password-based authentication protocol with key exchange*
	One-time password authentication (8.3)	ITU-T X.1153	*Management framework of a one time password-based authentication service*
	Non-repudiation framework based on one-time password (8.4)	ITU-T X.1156	*Non-repudiation framework based on a one-time password*
	Delegated non-repudiation (8.4)	ITU-T X.1159	*Delegated non-repudiation architecture based on ITU-T X.813*
Securing the network infrastructure	The telecommunications management network (9.1)	ITU-T M.3010	*Principles for a telecommunications management network*
	Securing monitoring and control activities (9.4)	ITU-T M.3016.0	*Security for the management plane: Overview*
	Securing network operation activities and management applications (9.5)	ITU-T M.3210.1	*TMN management services for IMT-2000 security management*
	Protection against electromagnetic threats (9.6)	ITU-T X.790	*Trouble management function for ITU-T applications*
	Common security management services (9.7)	ITU-T X.711	*Common Management Information Protocol*
	CORBA-based security services (9.7.4)	ITU-T X.736	*Systems Management: Security alarm reporting function*
		ITU-T X.740	*Systems Management: Security audit trail function*
		ITU-T X.780	*TMN Guidelines for defining CORBA managed objects*

Table 2 – Overview of some of the key topics and selected Recommendations (Part 3 of 5)

Sub-topics	Sub-topics	Sub-topics	
Some specific approaches to network security	Next Generation Network (NGN) security (10.1)	ITU-T Y.2001	*General overview of NGN*
		ITU-T Y.2701	*Security requirements for NGN release 1*
	NGN Identity management (7.1.2)	ITU-T Y.2720	*NGN identity management framework*
		ITU-T Y.2741	*Architecture of secure mobile financial transactions in NGN*
	Mobile communications security (10.2)	ITU-T Y.2760	*Mobility security framework in NGN*
		ITU-T X.1121	*Framework of security technologies for mobile end-to-end data communications*
	Security for home networks (10.3)	ITU-T X.1111	*Framework for security technologies for home network*
	Ubiquitous Sensor Networks (10.6)	ITU-T X.1311	*Security framework for ubiquitous sensor networks*
	Software Defined Networking (10.7)	ITU-T Y.3300	*Framework of software-defined networking*
		ITU-T Y.3302	*Functional architecture of software-defined networking*
		ITU-T X.1038	*Security requirements and reference architecture for software-defined networking*
		ITU-T X.1042	*Security services using software-defined networking*
Cybersecurity and incident response	Cybersecurity information exchange (11.1)	ITU-T X.1205	*Overview of cybersecurity*
		ITU-T X.1500	*Overview of cybersecurity information exchange*
	Exchange of vulnerability information (11.1.3)	ITU-T X.1520	*Common vulnerabilities and exposures*
	Discovery of cybersecurity information (11.1.5)	ITU-T X.1570	*Discovery mechanisms in the exchange of cybersecurity information*
	Incident handling (11.4)	ITU-T E.409	*Incident organization and security incident handling: Guidelines for telecommunication organizations*
		ITU-T X.1056	*Security incident management guidelines for telecommunications organizations*
	Access control for incident exchange network (11.3)	ITU-T X.1550	*Access control models for incident exchange networks*
Application security	Voice over IP (VoIP) and multimedia (12.1)	ITU-T H.235.x sub-series	*H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*
		ITU-T H.460.22	*Negotiation of security protocols to protect H.225.0 call signalling messages*
	IPTV (12.2)	ITU-T X.1195	*Service and content protection interoperability scheme*
	DRM for Cable Television Multiscreen (12.3)	ITU-T H.751	*Metadata for rights information interoperability in IPTV services*
	Secure fax (12.4)	ITU-T T.36	*Security capabilities for use with Group 3 facsimile terminals*
	Web services (12.5)	ITU-T X.1141	*Security Assertion Markup Language (SAML 2.0)*
		ITU-T X.1142	*eXtensible Access Control Markup Language (XACML 2.0)*
	Tag-based services (12.6)	ITU-T X.1171	*Threats and requirements for protection of personally identifiable information in applications using tag-based identification*

Table 2 – Overview of some of the key topics and selected Recommendations (Part 4 of 5)

Sub-topics	Sub-topics	Sub-topics	
Countering common network threats	Spam (13.1)	ITU-T X.1231	*Technical strategies on countering spam*
		ITU-T X.1240	*Technologies involved in countering e-mail spam*
		ITU-T X.1241	*Technical framework for countering e-mail spam*
		ITU-T X.1244	*Overall aspects of countering spam in IP-based multimedia applications*
		ITU-T X.1247	*Technical framework for countering mobile messaging spam*
	Malicious code, spyware and deceptive software (13.2)	ITU-T X.1207	*Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software*
	Notification and dissemination of software updates (13.3)	ITU-T X.1206	*A vendor-neutral framework for automatic notification of security related information and dissemination of updates*
Security aspects of cloud computing	Overview of of cloud computing (14.1)	ITU-T Y.3500	*Cloud computing – Overview and vocabulary*
	A security framework for cloud computing (14.2)	ITU-T X.1601	*Security framework for cloud computing*
	Information security management control for cloud services (14.3)	ITU-T X.1602	*Security requirements for software as a service application environments*
		ITU-T X.1603	*Data security requirements for the monitoring service of cloud computing*
		ITU-T X.1604	*Security requirements of Network as a Service (NaaS) in cloud computing*
		ITU-T X.1605	*Security requirements of public Infrastructure as a Service (IaaS) in cloud computing*
		ITU-T X.1606	*Security requirements for communications as a service application environments*
		ITU-T X.1631	*Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
	Cloud computing security best practices and guidelines (14.4)	ITU-T X.1641	*Guidelines for cloud service customer data security*
		ITU-T X.1642	*Guidelines for the operational security of cloud computing*
		ITU-T X.1643	*Security requirements and guidelines for virtualization containers*
		ITU-T X.1644	*Security guidelines for distributed cloud*
		ITU-T X.1645	*Requirements of network security situational awareness platform for cloud computing*
		ITU-T X.1411	*Guideline on blockchain as a service (BaaS) security*
	Virtual measurement systems (14.5)	ITU-T Y.1550	*Considerations for realizing virtual measurement systems*
	Big data infrastructure security(14.6)	ITU-T Y.3600	*Big data - Cloud computing based requirements and capabilities*
		ITU-T X.1750	*Guidelines on security of big data as a service for big data service providers*
		ITU-T X.1751	*Security guidelines for big data lifecycle management by telecommunication operators*
		ITU-T X.1752	*Security guidelines for big data infrastructure and platform*

Pre

Table 2 – Overview of some of the key topics and selected Recommendations (Part 5 of 5)

Sub-topics	Sub-topics	Sub-topics	
The future of ICT security standardization	Security for Internet of Things (15.1)	ITU-T Y.4100	*Common requirements of the Internet of things*
		ITU-T X.1363	*Technical framework of personally identifiable information (PII) handling in Internet of things (IoT) environment*
		ITU-T X.1331	*Security guidelines for home area network (HAN) devices in smart grid systems*
		ITU-T X.1336	*Aggregate message authentication schemes for Internet of things environment*
		ITU-T X.1352	*Security requirements for Internet of things devices and gateways*
		ITU-T X.1367	*Standard format for Internet of things error logs for security incident operations*
		ITU-T X.1368	*Secure firmware or software update for Internet of things devices*
		ITU-T X.1369	*Security requirements for IoT service platform*
	Security for Intelligent Transport Systems (15.2)	ITU-T X.1371	*Security threats to connected vehicles*
	Security for Distributed Ledger Technology (15.3)	ITU-T X.1401	*Security threats of distributed ledger technology*
		ITU-T X.1402	*Security framework for distributed ledger technology*
		ITU-T X.1403	*Security guidelines for using DLT for decentralized identity management*
		ITU-T X.1405	*Security threats and requirements for digital payment services based on distributed ledger technology*
		ITU-T X.1408	*Security threats and requirements for data access and sharing based on distributed ledger technology*
	Security for Quantum-based communications (15.4)	ITU-T X.1702	*Quantum noise random number generator architecture*

This table illustrates *some* of the topics and Recommendations discussed in this publication. It is not intended to be comprehensive. A complete list of security-related Recommendations mentioned in the text is contained in Annex D. For a complete set of ITU-T Recommendations please see http://www.itu.int/ITU-T/recommendations/.
Bracketed numbers following the subtopics refer to the corresponding topics in the body of the text.

Pre-pu

3. Security requirements

Pre-published

3 Security requirements

In developing any kind of security framework, it is very important to have a clear understanding of the requirements. A comprehensive review of security requirements must take into account: the parties involved; the assets that need to be protected; the threats against which those assets must be protected; the vulnerabilities associated with the assets and the environment; and the overall risk to the assets from those threats and vulnerabilities.

This section introduces the basic requirements for protection of ICT applications, services and information, looks at the threats and vulnerabilities that drive the requirements, examines the role of standards in meeting the requirements, and identifies some of the features that are needed to protect the various parties involved in the use and operation of ICT facilities.

Security requirements are both generic and context-specific. In addition, some requirements are well-established while others continue to evolve with new applications and the evolving threat environment. For the most part, the discussion in this section is generic. Requirements for particular applications and environments are discussed in later sections.

3.1 Threats, risks and vulnerabilities

In general terms, there is a need to protect assets for:

- *customers/subscribers* who need confidence in the network and the services offered, including availability of services (especially emergency services);
- *public community/authorities* who demand security by directives and/or legislation, in order to ensure availability of services, privacy protection, and fair competition; and
- *network operators* and service providers who need security to safeguard their operation and business interests and to meet their obligations to customers, their business partners and the public.

The assets to be protected include:

- communication and computing services;
- information and data, including software and data relating to security services;
- personnel; and
- equipment and facilities.

A *security threat* is defined as a potential violation of security. Examples of threats include:

- unauthorized disclosure of information;
- unauthorized destruction or modification of data, equipment or other resources;
- theft, removal or loss of information or other resources;
- interruption or denial of services; and
- impersonation, or masquerading as an authorized entity.

Threats may be *accidental* (also sometimes called *inadvertent*) or *intentional* and may be *active* or *passive*. An accidental threat is one with no premeditated intent such as a system or software malfunction or a physical failure. An intentional threat is one that is realized by someone committing a deliberate act. Intentional threats may range from casual examination, using easily-available monitoring tools, to sophisticated attacks using special system knowledge. When an intentional threat is realized it is called an *attack*. An active threat is one that results in some change to the state or operation of a system, such as alteration of data or destruction of physical equipment. A passive threat involves no change of state. Eavesdropping and wiretapping are examples of passive threats.

Pre-published

A *security vulnerability* is a flaw or weakness that could be exploited to violate a system or the information it contains. If a vulnerability exists, then it is possible for a threat to be realized successfully unless effective countermeasures are in place.

ITU-T Recommendations recognize four types of vulnerability:

- threat model vulnerabilities, which result from failure to foresee possible future threats;
- design and specification vulnerabilities, which result from errors or oversights in the design of a system or protocol and make it inherently vulnerable;
- implementation vulnerabilities, which are introduced by errors or oversights during system or protocol implementation; and
- operation and configuration vulnerabilities, which originate from improper usage of options in implementations or weak deployment policies and practices (such as failure to use encryption in a wireless network).

Security risk is a measure of the adverse effects that can result if a security vulnerability is exploited, i.e., if a threat is realized. While risk can never be eliminated, one objective of security is to reduce risk to an acceptable level. In order to do that, it is necessary to understand the applicable threats and vulnerabilities and to apply appropriate countermeasures. These are usually specific security services and mechanisms which may be complemented by non-technical measures such as physical and personnel security.

While threats and threat agents change, security vulnerabilities exist throughout the life of a system or protocol, unless specific steps are taken to address them. With standardized protocols being very widely-used, vulnerabilities associated with the protocols can have very serious implications and be global in scale. Hence, it is particularly important to understand and identify vulnerabilities in protocols and to take steps to eliminate them as and when they are identified.

Standards bodies have both a responsibility and a unique ability to address security vulnerabilities that may be inherent in specifications such as architectures, frameworks and protocols. Even with adequate knowledge about the threats, risks and vulnerabilities associated with information processing and communications networks, adequate security cannot be achieved unless security measures are systematically applied in accordance with relevant security policies. The security policies themselves must be reviewed and updated periodically. Also, adequate provision must be made for security management and incident response. This will include assigning responsibility and specifying action that must be taken to prevent, detect, investigate and respond to any security incident.

Security services and mechanisms can protect telecommunication networks against malicious attacks such as denial of service, eavesdropping, spoofing, tampering with messages (modification, delay, deletion, insertion, replay, re-routing, misrouting, or re-ordering of messages), repudiation or forgery. Protection techniques include prevention, detection and recovery from attacks, as well as management of security-related information. Protection must include measures to prevent service outages due to natural events (such as storms and earthquakes) and malicious attacks (deliberate or violent actions). Provisions must also be made to facilitate interception and monitoring by duly-authorized legal authorities.

Telecommunication network security also demands extensive cooperation between service providers. Recommendation ITU-T E.408 provides an overview of security requirements and a framework that identifies security threats to telecommunication networks in general (both fixed and mobile; voice and data) and gives guidance for planning countermeasures that can be taken to mitigate the risks arising from the threats. Implementing the requirements of ITU-T E.408 would facilitate international cooperation in the following areas relating to telecommunication network security:

- information sharing and dissemination;
- incident coordination and crisis response;
- recruitment and training of security professionals;
- law enforcement coordination;
- protection of critical infrastructure and critical services; and

- development of appropriate legislation.

However, to succeed in obtaining such cooperation, implementation of the requirements for the national components of the network is essential.

Recommendation ITU-T X.1205 provides a taxonomy of security threats from an organizational point of view along with a discussion of the threats at the various layers of a network.

3.2 General security objectives for ICT networks

The general security objectives for ICT networks are as follows:

a) Access to, and use of networks and services should be restricted to authorized users;

b) Authorized users should be able to access and operate on assets they are authorized to access;

c) Networks should support confidentiality to the level prescribed in the network security policies;

d) All network entities should be held accountable for their own, but only their own, actions;

e) Networks should be protected against unsolicited access and unauthorized operations;

f) Security-related information should be available via the network, but only to authorized users;

g) Plans should be in place to address how security incidents are to be handled;

h) Procedures should be in place to restore normal operation following detection of a security breach; and

i) The network architecture should be able to support different security policies and security mechanisms of different strengths.

Achieving these objectives requires that close attention be paid to security during network design, implementation and operation. Security policies must be developed, appropriate security services must be applied and risk must be managed consistently and continuously.

3.3 Rationale for security standards

The use of internationally-agreed standards as a basis for network security promotes commonality of approaches and aids interconnection as well as being more cost effective than developing individual approaches for each jurisdiction.

In some cases, the provisioning and usage of security services and mechanisms can be quite expensive relative to the value of the assets being protected, so it is important to have the ability to customize the security services and mechanisms to meet local needs. However, the ability to customize security also can result in a number of possible combinations of security features. Therefore, it is desirable to have *security profiles* that cover a broad range of telecommunication network services to ensure alignment of options in different implementations. Standardization and the use of standardized profiles facilitate interoperability and the reuse of solutions and products, meaning that security can be introduced faster, more consistently and at lower cost.

Standardized network security solutions benefit both suppliers and service providers through economy of scale in product development and component interoperability.

3.4 Evolution of ITU-T security standards

The ITU-T security work continues to evolve in response to requirements raised by the ITU-T members. Here, some key aspects of this evolution are discussed, particularly as they relate to security requirements. Some of the individual Recommendations are discussed in more detail later.

Pre-published

In general, ICT security requirements are defined in terms of the threats to the network and/or system, the inherent vulnerabilities in the network and/or system, and the steps that must be taken to counter the threats and reduce the vulnerabilities. Protection requirements extend to the network and its components. Fundamental concepts of security, including threats, vulnerabilities and security countermeasures, are defined in Recommendation ITU-T X.800, which was published in 1991. The previously-mentioned Recommendation ITU-T E.408, which was published in 2004, builds on the concepts and terminology of ITU-T X.800. Recommendation ITU-T E.408 is generic in nature and does not address requirements for specific networks or identify any new security services. Instead, the Recommendation focuses on the use of existing security services defined in other ITU-T Recommendations and relevant standards from other bodies.

The need to counter the growing number and variety of cybersecurity threats (viruses, worms, Trojan horses, spoofing attacks, identity theft, spam and other forms of cyber-attack) is reflected in the 2008 Recommendation ITU-T X.1205. This Recommendation aims to build a foundation of knowledge that can help secure future networks. Various threat countermeasures are discussed including routers, firewalls, antivirus protection, intrusion detection systems, intrusion protection systems, secure computing, and audit and monitoring. Network protection principles such as defence-in-depth and access management are also discussed. Risk management strategies and techniques are reviewed, including the value of training and education in protecting the network. Examples of securing various networks based on the discussed techniques are also provided.

Recommendation ITU-T X.1205 defines cybersecurity as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, the organization and the user's assets”. The referenced assets include connected computing devices, computing users, applications/services, communications systems, multimedia communication, and the totality of transmitted and/or stored information in the cyber environment. As defined here, cybersecurity ensures the attainment and maintenance of the security properties of the organization (including availability, integrity and confidentiality) and protects a user's assets against relevant security risks in the cyber environment.

In today's business environment, the concept of the perimeter is disappearing. The boundaries between inside and outside networks are becoming "thinner". Applications run on top of networks in a layered fashion. Security must exist within and between each of these layers. A layered approach to security enables organizations to create multiple levels of defence against threats.

Cybersecurity techniques can be used to ensure system availability, integrity, authenticity, confidentiality, and non-repudiation as well as to ensure that user privacy is respected. Cybersecurity techniques can also be used to establish a user's trustworthiness. Some of the most important current cybersecurity techniques include:

– Cryptography, which supports a number of security services including confidentiality of data during transmission and in storage, as well as electronic signature;

– Access controls, which aim to prevent unauthorized access to, or use of information;

– System and data integrity, which aims to ensure that a system and its data cannot be modified or corrupted by unauthorized parties, or in an unauthorized manner without detection;

– Audit, logging and monitoring, which provides information to help evaluate the effectiveness of the security strategy and techniques being deployed; and

– Security management, which includes security configuration and controls, risk management, incident handling and management of security information.

Organizations need to devise a comprehensive plan for addressing security in each particular context. Security is not "one-size-fits-all". Security should be viewed as an on-going process that covers protection of systems, data, networks, applications, and resources. Also, security must be comprehensive across all layers of a system. A layered approach to security, combined with strong policy management and enforcement, provides a choice of security solutions that can be modular, flexible, and scalable.

Pre-published

3.5 Personnel and physical security requirements and controls

For the most part, ITU-T security-related Recommendations focus on the technical aspects of the system and network. Some aspects of personnel security are identified in Recommendation ITU-T X.1051. Physical security is also a very important dimension of protection but it is largely outside the scope of most of the ITU-T work. However, Recommendation ITU-T X.1051 provides controls on general physical security and requirements for physical security relating to the outside plant is addressed in the two documents identified below.

Physical protection requirements for outside plant include the need to make sure the hardware is able to resist the threat of fire, natural disaster and accidental or intentional damage. Methods for achieving protection of components, cables, closures, cabinets, etc., are addressed in the *ITU-T Handbook on outside plant technologies for public networks* and the *ITU-T Handbook on application of computers and microprocessors to the construction, installation and protection of telecommunication cables*. These documents also address the monitoring of systems to prevent damage and suggest how to respond to problems and restore system functionality in the most expeditious manner.

Pre-published

4. Security architectures

Pre-published

4 Security architectures

Security architectures, and related models and frameworks, provide a structure and context within which related technical standards can be developed in a consistent manner. In the early 1980s, the need for a framework in which security could be applied in a layered communications architecture was identified. This led to the development of the Recommendation ITU-T X.800. This was the first of a suite of architectural standards to support security services and mechanisms. This work, most of which was done in collaboration with ISO, led to further standards, including security models and frameworks that specify how particular types of protection can be applied in particular environments.

Later, the need for both generic and application-specific security architectures was identified. This resulted in the development of the Recommendation ITU-T X.805, as well as a number of application-specific architectures to address areas such as network management, peer-to-peer communications and mobile web servers. Recommendation ITU-T X.805, which is described later in this section, complements other Recommendations of the ITU-T X.800 series by offering security solutions directed towards providing end-to-end network security.

4.1 The open systems security architecture and related standards

The first of the communications security architectures to be standardized was Recommendation ITU-T X.800, the open systems security architecture. This Recommendation defines the security-related architectural elements that can be applied according to the circumstances for which protection is required. In particular, it provides a general description of security services and the related mechanisms that may be used to provide the services. It also defines, in terms of the seven-layer Open Systems Interconnection (OSI) Basic Reference Model, the most appropriate location (i.e. the layer) at which the security services should be implemented.

Recommendation ITU-T X.800 is concerned only with those visible aspects of a communications path that permit end systems to achieve the secure transfer of information between them. It does not attempt to provide any kind of implementation specification and it does not provide the means to assess conformance of any implementation to this or any other security standard. Nor does it indicate, in any detail, any additional security measures that may be needed in end-systems to support the communication security features.

Although Recommendation ITU-T X.800 was developed specifically as the OSI security architecture, the underlying concepts have been shown to have much broader applicability and acceptance. The standard is particularly important as it represents the first internationally-agreed consensus on the definitions of the basic security services (*authentication*, *access control*, *data confidentiality*, *data integrity* and *non-repudiation*) along with more general (pervasive) services such as *trusted functionality*, *event detection*, *security audit and security recovery*. It also indicates which security mechanisms can be used to provide the security services. Prior to Recommendation ITU-T X.800 there had been a wide range of views on what basic security services were required and what exactly each service would do. The value and general applicability of Recommendation ITU-T X.800 results from the fact that it represents a significant international consensus on the meaning of the terms used to describe security features, on the set of security services needed to provide protection for data communications, and on the nature of those security services.

Pre-published

During the development of Recommendation ITU-T X.800, the need for additional related communications security standards was identified. As a result, work on a number of supporting standards and complementary architectural Recommendations was initiated. Some of these Recommendations are discussed below.

4.2 Security services

Security frameworks have been developed to provide comprehensive and consistent descriptions of each of the security services defined in Recommendation ITU-T X.800. These standards are intended to address all aspects of how the security services can be applied in the context of a specific security architecture, including possible future security architectures. The frameworks focus on providing protection for systems, objects within systems, and interaction between systems. They do not address the methodology for constructing systems or mechanisms. Recommendation ITU-T X.810 introduces the other frameworks and describes common concepts including security domains, security authorities and security policies that are used in all the frameworks. It also describes a generic data format that can be used to convey both authentication and access control information securely.

Authentication is the provision of assurance of the claimed identity of an entity. Entities include not only human users, but also devices, services and applications. Authentication can also provide assurance that an entity is not attempting a masquerade or an unauthorized replay of a previous communication. Recommendation ITU-T X.800 identifies two forms of authentication: *data origin authentication* (i.e., corroboration that the source of data received is as claimed) and *peer entity authentication* (i.e., corroboration that a peer entity in an association is the one claimed). Recommendation ITU-T X.811 defines the basic concepts of authentication; identifies possible classes of authentication mechanism; defines the services for these classes of mechanism; identifies functional requirements for protocols to support these classes of mechanism; and identifies the general management requirements for authentication.

Access control is the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. Access control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. Recommendation ITU-T X.812 describes a model that includes all aspects of access control in Open Systems, the relationship to other security functions (such as authentication and audit), and the management requirements for access control.

Non-repudiation is the ability to prevent entities later falsely denying that they performed (or did not perform) an action. Non-repudiation is concerned with establishing evidence that can later be used to counter false claims. Recommendation ITU-T X.800 describes two forms of non-repudiation service: *non-repudiation with proof of delivery*, which is used to counter false denial by a recipient that the data has been received, and *non-repudiation with proof of origin*, which is used to counter false denial by an originator that the data has been sent. However, in a more general sense, the concept of non-repudiation can be applied to many different contexts including non-repudiation of creation, submission, storage, transmission and receipt of data. Recommendation ITU-T X.813 extends the concepts of non-repudiation security services described in Recommendation ITU-T X.800 and provides a framework for the development of these services. It also identifies possible mechanisms to support these services and identifies general management requirements for non-repudiation.

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. The purpose of the confidentiality service is to protect information from unauthorized disclosure. Recommendation ITU-T X.814 addresses the confidentiality of information by defining the basic concepts and possible classes of confidentiality and the facilities required for each class of confidentiality mechanism. It also identifies the management and supporting services required, and the interaction with other security services and mechanisms.

Data integrity is the property that data has not been altered in an unauthorized manner. In general, an integrity service addresses the need to ensure that data is not corrupted or, if it is corrupted, that the user is aware of that

Pre-published

fact. Recommendation ITU-T X.815 addresses the integrity of data in information retrieval, transfer and management. It defines the basic concepts of integrity, identifies possible classes of integrity mechanism and the facilities, management requirements and related services needed to support the class of mechanism. (Note that, although the security architecture standards focus primarily on data integrity, other aspects of integrity, such as system integrity, are also important to security.)

4.3 Security architecture for systems providing end-to-end communications

In 2003, following a more in-depth look at the security architecture for networks, Recommendation ITU-T X.805, was approved. This architecture, which builds on, and extends some of the concepts of ITU-T X.800 and the security frameworks discussed above, can be applied to various kinds of network and is technology-neutral.

4.3.1 Elements of the Recommendation ITU-T X.805 architecture

The Recommendation ITU-T X.805 architecture is defined in terms of three major concepts, security layers, planes, and dimensions, for an end-to-end network. A hierarchical approach is taken in dividing the security requirements across the layers and planes so that the end-to-end security is achieved by designing security measures in each of the dimensions to address the specific threats. Figure 1 illustrates the elements of this architecture.

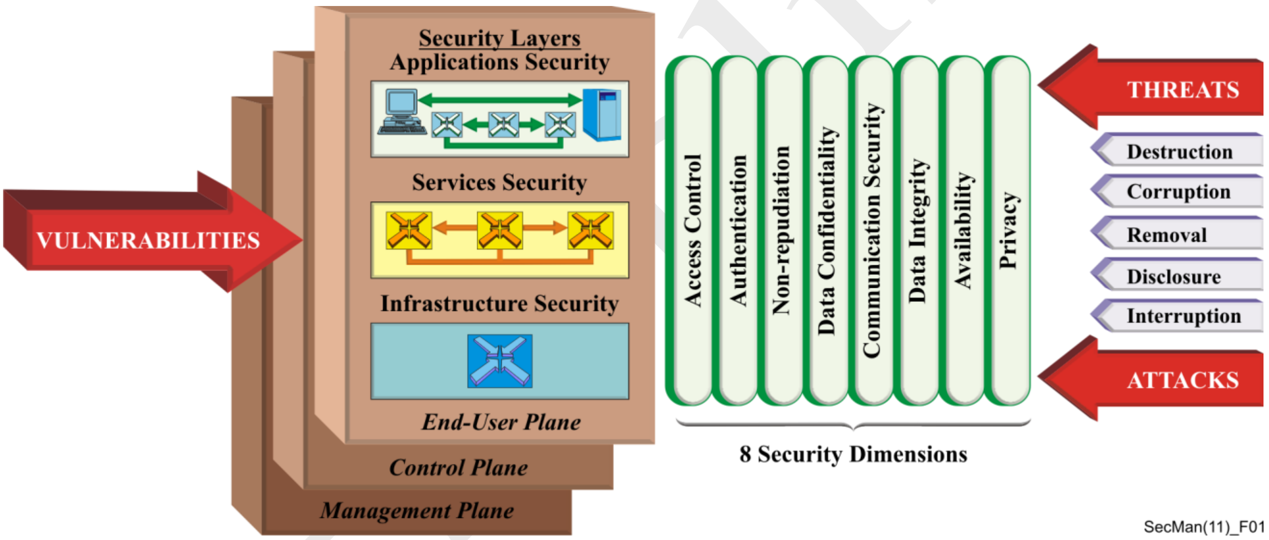


Figure 1 – Security architectural elements in Recommendation ITU-T X.805

A *security dimension* is a set of security measures designed to address a particular aspect of network security. The basic security services of Recommendation ITU-T X.800 (*Access Control*, *Authentication*, *Data Confidentiality*, *Data Integrity* and *Non-repudiation*) are reflected in the functionalities of the corresponding *security dimensions* of Recommendation ITU-T X.805 (as depicted in Figure 1). In addition, Recommendation ITU-T X.805 introduces three dimensions (*Communication Security*, *Availability* and *Privacy*) that are not in Recommendation ITU-T X.800:

- the *Communication Security* dimension, which ensures that information flows only between the authorized end points, i.e., information is not diverted or intercepted as it flows between these end points;
- the *Availability* dimension, which ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network; and

Pre-published

- the *Privacy* dimension, which provides for the protection of information that might be derived from the observation of network activities. Examples include websites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a service provider network.

These dimensions offer additional network protection and protect against all major security threats. These dimensions are not limited to the network, but also extend to applications and end-user information. The security dimensions apply to service providers or enterprises offering security services to their customers.

In order to provide an end-to-end security solution, the security dimensions must be applied to a hierarchy of network equipment and facility groupings, which are referred to as *security layers*. A *security plane* represents a certain type of network activity protected by security dimensions. Each security plane represents a type of protected network activity.

The security layers address requirements that are applicable to the network elements and systems and to services and applications associated with those elements. One of the advantages of defining the layers is to allow for reuse across different applications in providing end-to-end security. The vulnerabilities at each layer are different and thus countermeasures must be defined to meet the needs of each layer. The three layers are:

- *the Infrastructure* layer, which represents the fundamental building blocks of networks, their services and applications. Examples of components that belong to this layer include individual network elements, such as routers, switches and servers, as well as the communication links between them;
- *the Services* layer, which addresses the security of network services offered to customers. These services range from basic connectivity offerings, such as leased line services, to value-added services, such as instant messaging; and
- *the Applications* layer, which addresses requirements of the network-based applications used by the customers. These applications may be as simple as e-mail or as sophisticated as, for example, collaborative visualization, where very high-definition video transfers are used, e.g., in oil exploration or automobile design.

The security planes address specific security needs associated with network management activities, network control or signalling activities, and end-user activities. Networks should be designed in such a way that events on one security plane are isolated from the other security planes.

The security planes are:

- *the Management* plane, which is concerned with operations, administration, maintenance and provisioning activities such as provisioning a user or a network;
- *the Control* plane, which is associated with the signaling aspects for setting up (and modifying) the end-to-end communication through the network irrespective of the medium or technology used in the network; and
- *the End-User* plane, which addresses security of access and use of the network by subscribers. This plane also deals with protecting end-user data flows.

The Recommendation ITU-T X.805 architecture can be used to guide the development of security policy, technology architectures, and incident response and recovery plans. The architecture can also be used as the basis for a security assessment. Once a security program has been deployed, it must be maintained in order to remain current in the ever-changing threat environment. This security architecture can assist in the maintenance of a security program by ensuring that modifications to the program address applicable security dimensions at each security layer and plane.

Pre-published

Although Recommendation ITU-T X.805 is a network security architecture, some of the concepts may be extended to end-user devices. This topic is considered in Recommendation ITU-T X.1031 *Roles of end users and telecommunications networks within security architecture*.

4.3.2 Availability of the network and its components

Network availability is an important aspect of ICT security. As noted above, the purpose of the *Availability* security dimension of ITU-T X.805 is to ensure continuity of service and authorized access to network elements, information, and applications. Disaster recovery solutions are also included in this dimension.

The functional, implementation and operational requirements to limit the risks and consequences of unavailability of network resources are numerous and diverse. Factors to be considered are many but they include error performance, congestion control, failure reporting and corrective actions. Recommendation ITU-T G.827, defines network performance parameters and objectives for the path elements and end-to-end availability of international, constant bit-rate digital paths. These parameters are independent of the type of physical network supporting the end-to-end path. Annex A of Recommendation ITU-T G.827 gives detailed guidance on methodologies for evaluating the end-to-end availability and provides examples of path topologies and end-to-end path availability calculations. Other Recommendations that address network performance include: Recommendation ITU-T G.1000, Recommendation ITU-T G.1030, Recommendation ITU-T G.1050 and Recommendation ITU-T G.1081.

4.4 Implementation guidance

The ITU-T security architecture standards are all part of the ITU-T X.800-849 series of security Recommendations. Implementation guidance is provided in Supplement 3 to the ITU-T X-series Recommendations. This supplement provides guidelines for critical activities during the network security life-cycle. These guidelines address four areas: technical security policy; hierarchical-asset identification; threats, vulnerabilities and mitigations based on hierarchical-assets; and security assessment. The guidelines and their associated templates are intended to enable systematic implementation of network security planning, analysis and assessment.

4.5 Some application-specific architectures

In this section, aspects of some of the architectures relating to specific applications are introduced.

4.5.1 Peer-to-peer communications

In a peer-to-peer (P2P) network, all peer entities have equivalent authority and responsibility. In contrast to the client/server model, a peer communicates with other peers directly when data or messages are exchanged. Because traffic and processing are distributed to each peer, the P2P network does not require high-performance computing power or a high-bandwidth network.

The P2P network is an overlay network on top of the telecommunication network and Internet. It exploits diverse connectivity between nodes and the computing power and storage available at each node, rather than conventional centralized resources.

P2P networks are typically used for connecting nodes via ad hoc connections. Such networks are useful for many purposes including the sharing of data files containing audio, video, text and other digital data. Real-time communications data, such as telephony traffic, also exploits P2P technology.

Pre-published

4.5.1.1 Security architecture and operations for peer-to-peer networks

A general security-related architectural model which can be applied in various P2P networks is described in Recommendation ITU-T X.1162.

Figure 2 shows a basic P2P service architecture. Information processed by each peer is exchanged directly among users. Because there is no central sever to store information, each peer needs to find which peers have target data before being able to retrieve it. Moreover, each peer must permit accesses from other peers to allow exchange of the data.

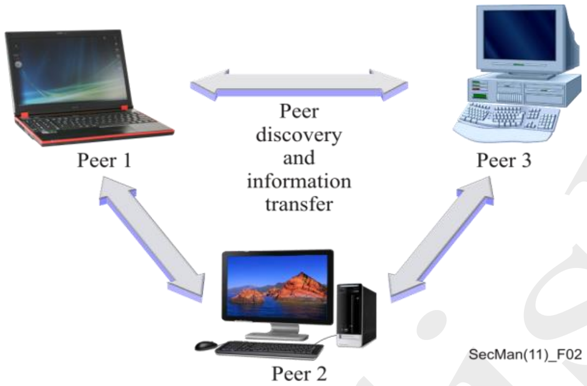


Figure 2 – P2P service architecture

In the physical P2P network, a user can join the P2P services through a device. Generally the term *peer* is used to represent a user, or a device owned by the user. The connection types between the entities in a P2P network can be categorized as follows:

- connection with an intra-domain peer;
- connection with an inter-domain peer; and
- connection with a service provider peer located in another network domain.

Figure 3 shows the logical P2P network architecture as a virtual network over the transportation stratum. It is assumed that the operation of each peer is not limited by the physical network architecture and that a peer can communicate with any other peer regardless of its location (through the help of a super-peer, if necessary). The structure of the peer-to-peer network is divided into two stratums: the P2P overlay stratum and the transportation stratum. The transportation stratum is responsible for transferring the packets from/to the upper layer, and the overlay stratum is responsible for providing the P2P services.

Pre-published

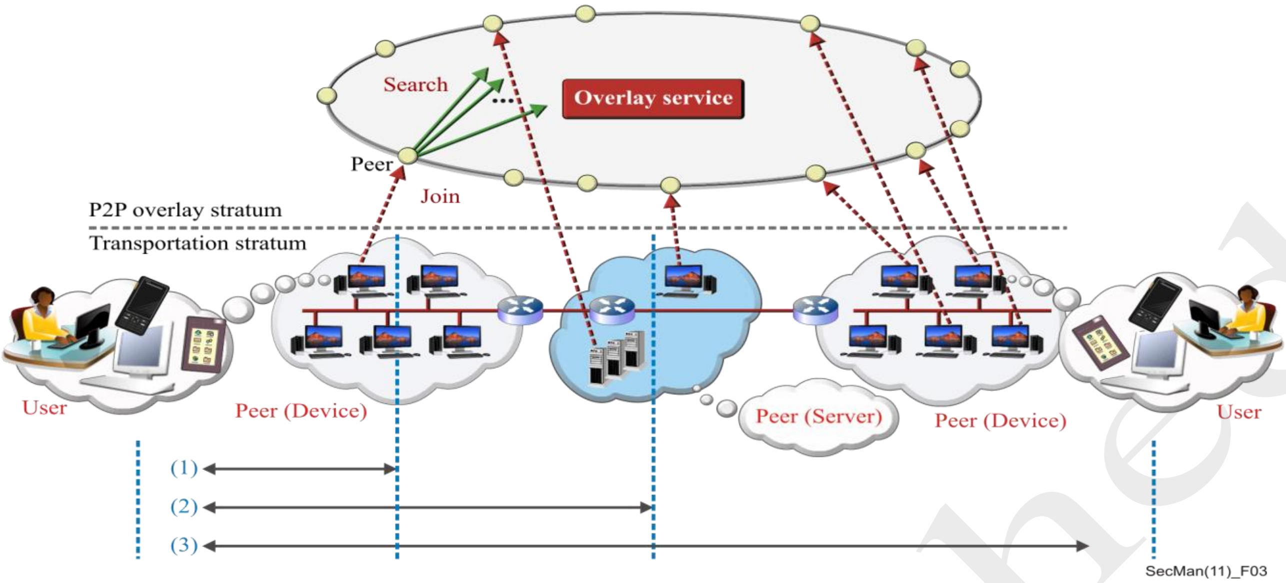


Figure 3 – Architectural reference model for the P2P network

4.5.1.2 Framework for secure peer-to-peer communications

Security requirements for P2P networks, together with the services and mechanisms needed to satisfy these requirements are specified in Recommendation ITU-T X.1161.

Threats to P2P communications include eavesdropping, jamming, injection & modification, unauthorized access, repudiation, man-in-the-middle attacks, and Sybil attacks. Countermeasures to P2P threats are shown in Table 3.

Table 3 – Relationship between P2P security requirements and countermeasures

Countermeasures Requirements	Encipherment	Key exchange	Digital signature	Trust management	Access control	Data integrity mechanism	Authentication exchange	Notarization	Secure routing	Traffic control mechanism	ID assignment
User authentication	X	X	X	X	X		X				X
Anonymity	X			X							X
Privacy	X				X		X				
Data integrity	X	X	X		X	X	X				
Data confidentiality	X	X			X		X				
Access control					X		X				X
Non-repudiation			X				X	X			X
Usability					X						
Availability					X		X		X	X	
Traceability			X						X		X
Traffic control		X								X	

Published

4.5.2 Security architecture for message security in mobile web services

The security architecture and scenarios for message security in mobile web services are described in Recommendation ITU-T X.1143. This standard provides:

- a security architecture for message security that relies on suitable web service policy mechanisms;
- interworking mechanisms and service scenarios between applications that support the full web services security protocol stacks and legacy applications that do not support the full web services security protocol stack;
- message authentication, integrity and confidentiality mechanisms;
- a message filtering mechanism based on the message contents; and
- a reference message security architecture and security service scenarios.

Figure 4 illustrates the ITU-T X.1143 security architecture for mobile web services.

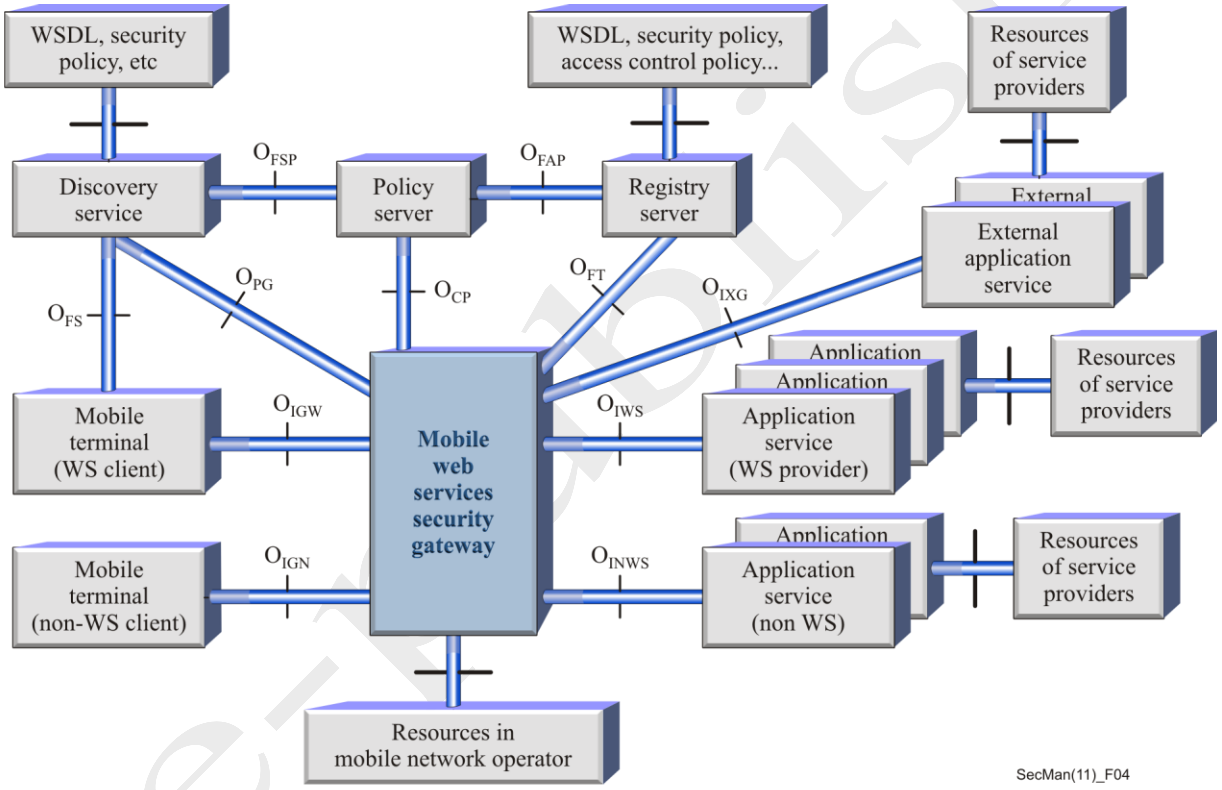

WSDL, security policy, etc
WSDL, security policy, access control policy...
Resources of service providers
Discovery service
O_{FSP}
Policy server
O_{FAP}
Registry server
External
External application service
O_{PG}
O_{CP}
O_{FT}
O_{IXG}
O_{FS}
Application
Application
Resources of service providers
Mobile terminal (WS client)
O_{IGW}
Mobile web services security gateway
O_{IWS}
Application service (WS provider)
Mobile terminal (non-WS client)
O_{IGN}
O_{INWS}
Application
Application service (non WS)
Resources of service providers
Resources in mobile network operator
SecMan(11)_F04

Figure 4 – Security architecture for mobile Web Services

The mobile web services security architecture consists of the following components:

- Mobile terminals, that are clients of the mobile Web Services;
- A Mobile Web Services Security Gateway (MWSSG). All requests from mobile clients are sent to the MWSSG which also enforces access control;
- The Policy Server, which manages security policies related to the secure processing of the messages and access control policies for messages;
- The Application Service, which provides various value-added services to the clients;
- The Discovery Service, which stores the interface information for application services and related security policies for access to the application services by the clients; and

Pre-published

- The Registry Server, which resides in the internal domain of the mobile operator and manages the interface information for application services, related security policies for access to the application services by the clients, and access control policies related to the target services.

A mobility security framework for the NGN transport stratum is defined in Recommendation ITU-T Y.2760 which addresses the security requirements, security mechanisms and procedures for mobility management and control in NGN.

4.6 Architecture for external relationships

The relationships between an IP-based telecommunication network security system (TNSS) and various groups of external objects are described in Recommendation ITU-T X.1032.This standard provides:

- TNSS interrelationships with security systems of information systems and information structure;
- TNSS interrelationships with telecommunication system objects;
- TNSS interrelationships with external organizations; and
- TNSS interrelationships with security threats sources

Figure 5 illustrates the ITU-T X.1032 function of external objects and their effort on TNSS.

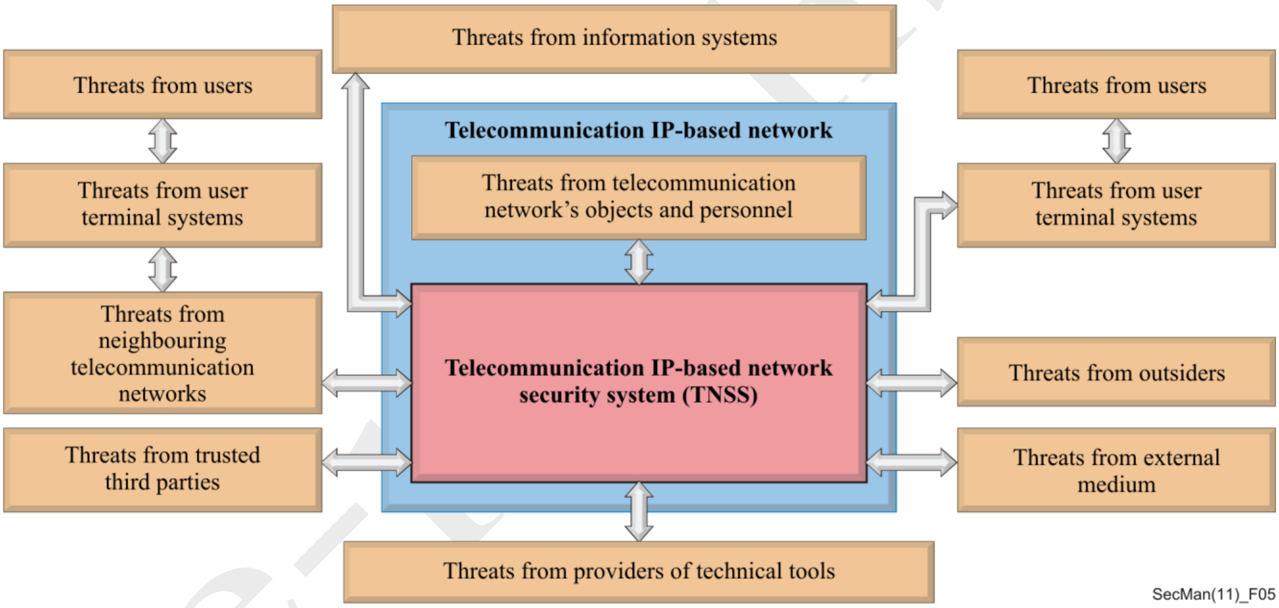

Threats from information systems
Threats from users
Threats from user terminal systems
Threats from neighbouring telecommunication networks
Threats from trusted third parties
Telecommunication IP-based network
Threats from telecommunication network's objects and personnel
Telecommunication IP-based network security system (TNSS)
Threats from users
Threats from user terminal systems
Threats from outsiders
Threats from external medium
Threats from providers of technical tools
SecMan(11)_F05

Figure 5 – Model of TNSS interrelationships with security threat sources

Threats are classified under five types as given in ITU-T X.800 and ITU-T X.805:

- destruction of information and other resources;
- corruption or modification of information;
- theft, removal or loss of information and other resources;
- disclosure of information; and
- interruption of services.

Security policy in a telecommunication network may be used either to counteract all threats or to counteract some of these threats. Correspondingly, required security dimensions are selected in the course of TNSS elaboration. External interrelationships of TNSS with security threat sources may be:

Pre-published

- electrical interfaces;
- actions of people;
- technical attacks via the telecommunication network and external technical attacks;
- external environmental influences;
- technical measures for counteracting attacks; and
- organizational measures for counteracting attacks.

4.7 Other network security architectures and models

Additional aspects of network security architectures are covered later in the text. In particular, please see clauses: 9.2, Network management architecture; 10.1, Next Generation Network security; 10.4, IPCablecom architecture; 10.5, IPCablecom2 architecture; and 12.2, IPTV.

In addition, two Recommendations cover the security architecture and framework specific to the NGN mobile networks. Recommendation ITU-T Y.2741, *Architecture of secure mobile financial transactions in next generation networks*, specifies the general architecture for a security solution for mobile commerce and mobile banking in the context of NGN. It describes the key participants, their roles, and the operational scenarios of the mobile commerce and mobile banking systems. It also provides examples of the implementation models of mobile commerce and mobile banking systems. Recommendation ITU-T Y.2760, *Mobility security framework in NGN*, specifies the mobility security framework in the NGN transport stratum. It addresses the security requirements, mechanisms and procedures for mobility management and control in NGN.

4.8 Security architectures and models for digital financial services and fintech services

This Recommendation X.1150 provides the security assurance framework for digital financial services (DFS). It also specifies a systematic security risk management process for identifying and assessing threats and vulnerabilities and identifies appropriate security controls to address vulnerabilities and mitigate risks, which needs to be implemented by the DFS provider and mobile network operator. It can be used to implement security controls for protecting the user, mobile device, mobile network operator and DFS provider.

Pre-published

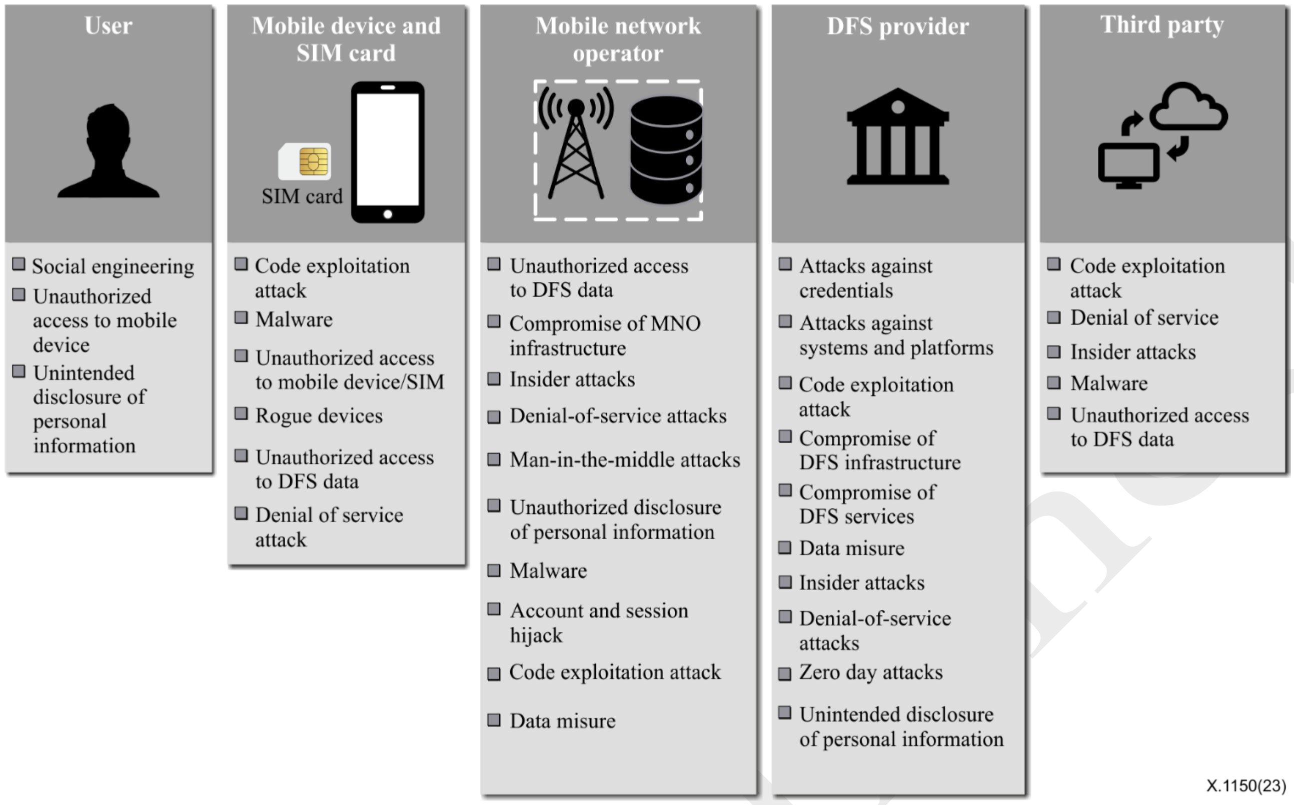

User
Mobile device and SIM card
SIM card
Mobile network operator
DFS provider
Third party
□ Social engineering
□ Unauthorized access to mobile device
□ Unintended disclosure of personal information
□ Code exploitation attack
□ Malware
□ Unauthorized access to mobile device/SIM
□ Rogue devices
□ Unauthorized access to DFS data
□ Denial of service attack
□ Unauthorized access to DFS data
□ Compromise of MNO infrastructure
□ Insider attacks
□ Denial-of-service attacks
□ Man-in-the-middle attacks
□ Unauthorized disclosure of personal information
□ Malware
□ Account and session hijack
□ Code exploitation attack
□ Data misure
□ Attacks against credentials
□ Attacks against systems and platforms
□ Code exploitation attack
□ Compromise of DFS infrastructure
□ Compromise of DFS services
□ Data misure
□ Insider attacks
□ Denial-of-service attacks
□ Zero day attacks
□ Unintended disclosure of personal information
□ Code exploitation attack
□ Denial of service
□ Insider attacks
□ Malware
□ Unauthorized access to DFS data
X.1150(23)

Figure 6 – Threats to DFS systems using USSD, SMS, IVR and NSDT

This Recommendation X.1149 provides a security framework for an open platform that supports financial technology (FinTech) services. This Recommendation demonstrates the evolution of the FinTech service platform to an open platform, analyses threats and vulnerabilities of open platform and open application programming interface (API), describes an open platform architecture and an open API usage procedure for FinTech services, and specifies detailed security requirements for FinTech services. Appendix I of this Recommendation describes use cases of the open platform API.

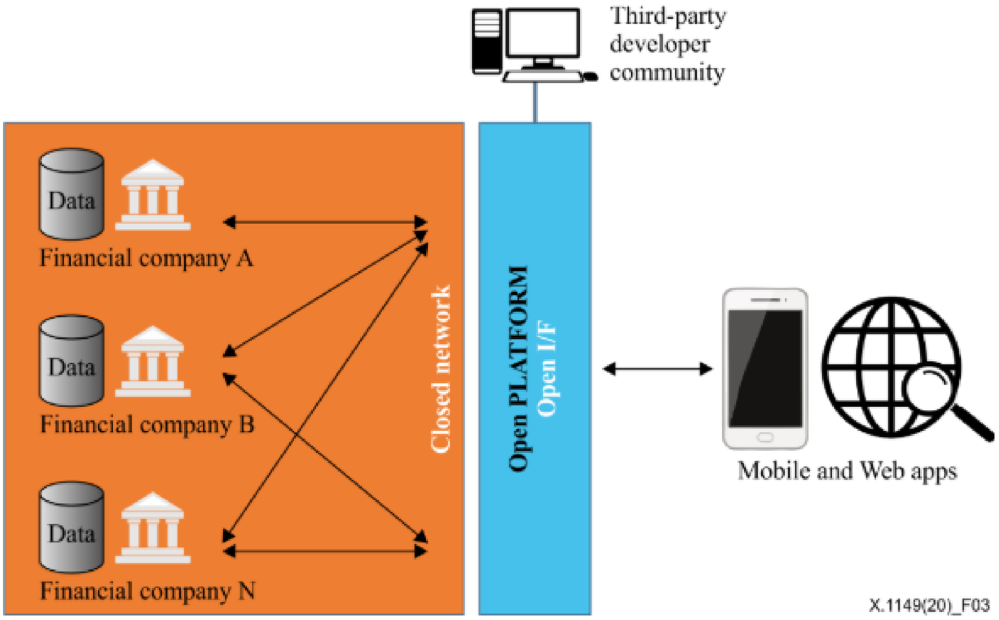


Figure 7 – Open platform architecture for FinTech services

5. Aspects of security management

Pre-published

5 Aspects of security management

Security management is a broad topic that embraces many activities associated with controlling and protecting access to system and network resources, event monitoring, reporting, policy and auditing, as well as managing the information related to these functions and activities. In this section, some of the generic security management activities are considered. Security management activities associated with securing the network infrastructure are discussed in section 9.

5.1 Information security management

Information, like other assets, is an essential contributor to an organization's business. Information can be printed, stored electronically, transmitted by mail, communicated electronically, displayed on film, spoken in conversation or conveyed in other ways. Regardless of the form or functionality of the information, or the means by which the information is shared or stored, information should always be appropriately protected.

Organizations whose facilities are used by subscribers to process information that may include personal information, confidential data and sensitive business data, need to ensure an appropriate level of protection to prevent compromise of the information.

Once information security is violated, for example by unauthorized access to an organization's information processing system, the organization may suffer significant damage. Therefore, it is essential for an organization to protect its information effectively by implementing a structured security management process. This is achieved by implementing and enforcing a suitable set of controls. These controls, which apply to data, telecommunications facilities, services and applications, need to be established, applied, monitored, reviewed and continuously improved. Failure to deploy effective security controls successfully can result in an organization failing to meet its security and business objectives.

The most widely-recognized ISMS specification is that defined in the ISO/IEC 27000 series of standards which includes standards on ISMS fundamentals, requirements, a code of practice, implementation guidance and related topics. ITU-T and ISO/IEC have jointly developed Recommendation ITU-T X.1051 | International Standard ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002.*

Recommendation ITU-T X.1051 establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in telecommunications organizations and provides an implementation baseline for information security management to help ensure the confidentiality, integrity and availability of telecommunications facilities and services. Specific guidance for the telecommunication sector is included on the following topics:

- information security policies;
- organization of information security;
- human resources security;
- asset management;
- access control;
- cryptography;
- physical and environmental security;
- operations security;
- communications security;
- systems acquisition, development and maintenance;
- supplier relationships;

Pre-published

- information security incident management;
- information security aspects of business continuity management; and
- compliance.

In addition to the application of security objectives and controls described in Recommendation ITU-T X.1051, telecommunications organizations also have to take into account the following particular security concerns:

- information should be protected from unauthorized disclosure. This implies non-disclosure of communicated information in terms of the existence, content, source, destination, date and time;
- the installation and use of telecommunication facilities should be controlled to ensure the authenticity, accuracy and completeness of information transmitted, relayed or received by wire, radio or any other methods; and
- only authorized access should be provided when necessary to telecommunications information, facilities and the medium used for the provision of communication services, whether it might be provided by wire, radio or any other methods. As an extension of the availability provisions, organizations should give priority to essential communications in case of emergency, and should comply with regulatory requirements.

To reduce risk, properly-implemented information security management is required in telecommunication organizations regardless of the medium or the mode of transmission.

Telecommunication organizations provide their services by acting as an intermediary in the transfer of data by other organizational and individual users. Therefore, account must be taken of the fact that information processing facilities within the organization are accessed and utilized not only by its own employees and contractors, but also various users outside the organization.

Bearing in mind that telecommunication services and facilities may be shared and/or interconnected with other service providers, management of information security in telecommunication organizations must extend to any and all areas of network infrastructure, services applications and facilities.

5.2 Information security management processes

Recommendation ITU-T X.1051 defines categories of telecommunication security controls. Recommendation ITU-T X.1052 provides best practices for information security management for telecommunication organizations to support Recommendation ITU-T X.1051 based on a process approach to describe a set of security management areas, which gives guidelines to telecommunication organizations to fulfil the control objectives defined in Recommendation ITU-T X.1051. The management areas include the areas defined by other Recommendations such as Recommendations ITU-T X.1055, ITU-T X.1056 and ITU-T X.1057.

It is necessary for telecommunications organizations to confirm the scope of their ISMS, which includes information assets. This confirmation, together with the establishment of guidelines for the implementation of information security management, should be undertaken before assessing the risks to the information assets and subsequent control of the risk. In addition, it is necessary to establish the structure and form of the information security organization as the basis for implementation risk control. The risk-controlling activities of the organizations should not be isolated from the operations of the organizations. The operations of the organization are generally described in a series of procedures. The risk-control activities should be regarded as an integral part of the relevant procedures.

According to the best practice and experience of the telecommunication organizations' security management work, combined with the PDCA management cycle, the information security management of telecommunication organizations should include seven main processes as provided below (Figure 8).

Pre-published

1) Conduct risk assessment for information security

2) Establish security management policy

3) Define information security controls

4) Implement information security controls

5) Operation and maintenance for the information security controls

6) Monitoring and auditing on the information security controls

7) Improve information security processes and controls

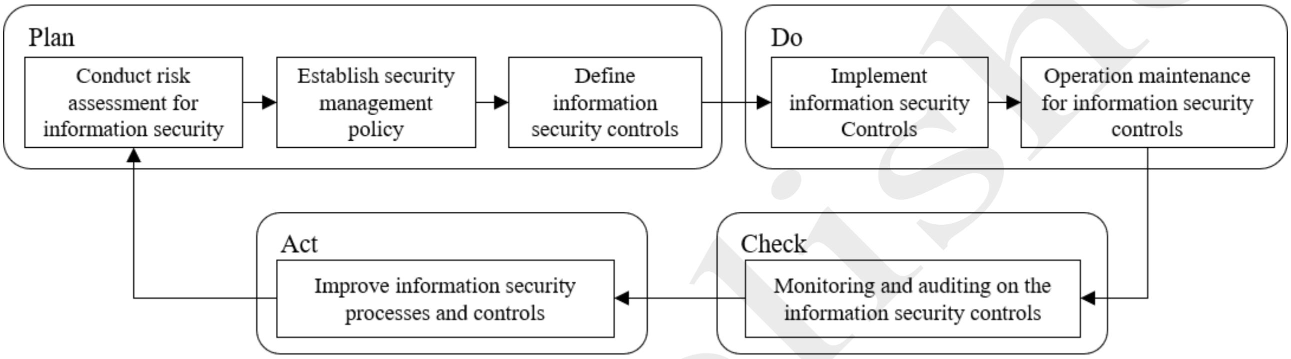

Plan
Conduct risk assessment for information security
Establish security management policy
Define information security controls
Do
Implement information security Controls
Operation maintenance for information security controls
Act
Improve information security processes and controls
Check
Monitoring and auditing on the information security controls

Figure 8 - Organization information security management processes

5.3 Risk management

Risk management is the process of assessing and quantifying risk and taking action to ensure that residual risk is below a pre-determined acceptable level. This topic is introduced in Recommendation ITU-T X.1205. More detailed risk management guidelines are contained in Recommendation ITU-T X.1055, which identifies processes and techniques that can be used to assess telecommunications security requirements and risks, and to help to select, implement and update appropriate controls to maintain the required level of security.

A number of risk management methodologies exist. Recommendation ITU-T X.1055 provides the criteria for assessing and selecting appropriate methodologies for a telecommunication organization. However, it does not propose any specific risk management methodology.

The risk management process is illustrated in Figure 9.

Pre-published

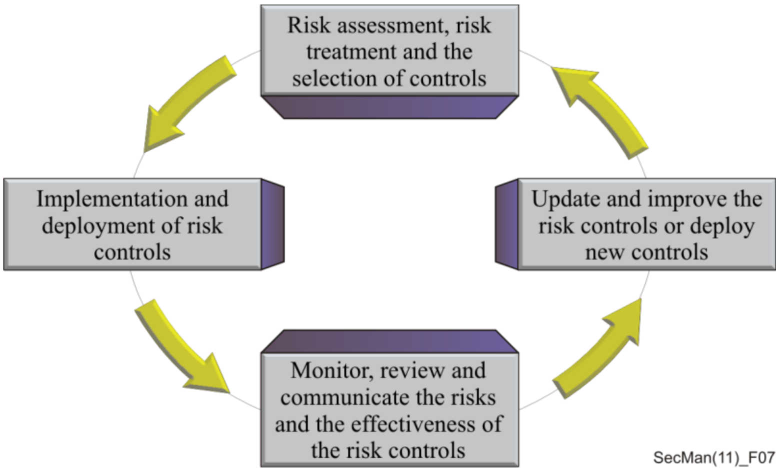

Risk assessment, risk treatment and the selection of controls
Update and improve the risk controls or deploy new controls
Monitor, review and communicate the risks and the effectiveness of the risk controls
Implementation and deployment of risk controls
SecMan(11)_F07

Figure 9 – ITU-T X.1055 risk management process

Risk profiles are used to guide the overall process of risk management. Specifically, they are used to assist the decision-making process and to help prioritize risks in terms of their criticality as well as helping to determine allocation of resources and countermeasures. They can also assist in the development of suitable metrics and be used alongside other tools such as gap analysis methodologies. Recommendation ITU-T X.1055 provides guidance in developing risk profiles and includes a template and some risk profile examples. Risk analysis in Next Generation Networks is addressed in supplement Y.Sup19 to the ITU-T Y.2200-series - *Supplement on the risk analysis service in next generation networks*.

5.4 Asset management

An asset is a component or entity to which an organization directly assigns value. An organization’s assets have their own unique values from the various viewpoints of business, financial affairs, reliability and so on. The information and communication facilities within the scope of the ISMS may be considered to have higher values than those of other assets. Incidents that involve such assets can negatively affect not only users, but the business of the organization. Therefore, the assets must be considered to have high protection priorities. Most organizations strive to find the best methods to identify assets which have high protection priorities. The goal of asset management is to identify and protect the most critical components of the organization so as to minimize the risk of problems. In determining the importance of assets, the principle services and the value of the business should be considered taking into account:

- the potential impact on service and the scope of the services which each asset affects;
- the potential loss of profit and the degree of potential financial loss;
- the potential impact of loss of customer(s); and
- the potential damage to the image of the organization.

Telecommunication organizations should have particularly high goals for operating and managing their various assets, for providing customer services and for directly or indirectly supporting their business. To protect those assets, it is critical that telecommunication organizations ensure that the operations and services of the business are not compromised.

Recommendation ITU-T X.1057 provides an overview of processes and methods that need to be addressed to identify, classify, evaluate and maintain the assets which telecommunication organizations own.

Information security asset management refers to the appropriate handling and protection measures considering the asset value as determined by the organization. In order to manage an organization’s various assets systematically and securely, a process of life cycle asset management should be adopted which covers

Pre-Published

acquisition or generation of the asset as well as modification and disposal or destruction of the asset according to pre-determined rules and standards. The asset management process is illustrated in Figure 10.

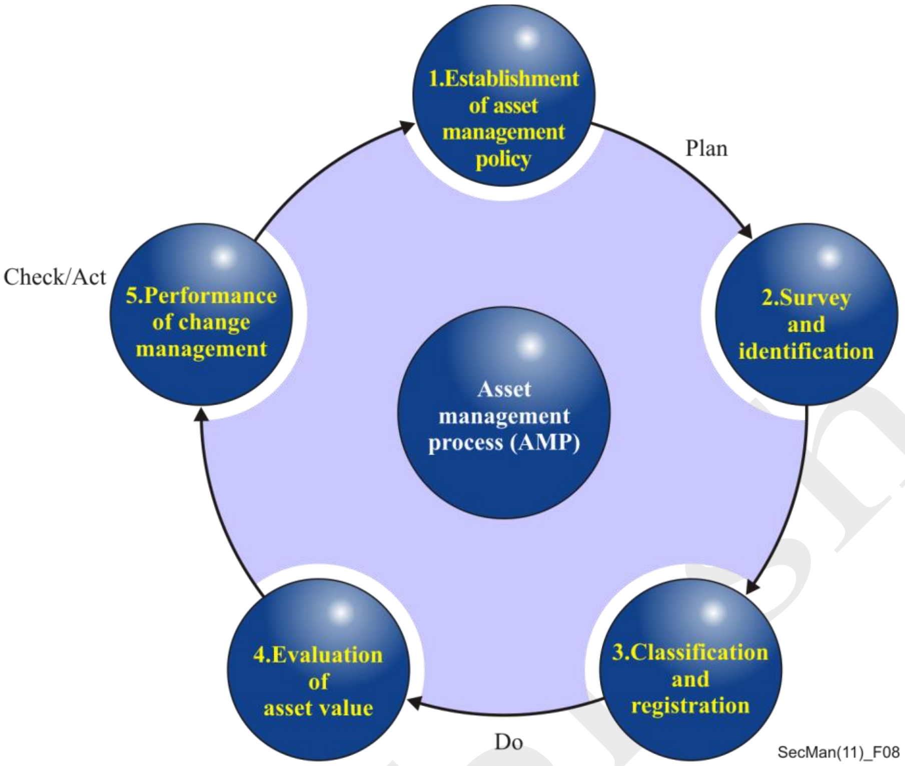

1.Establishment of asset management policy
Plan
2.Survey and identification
3.Classification and registration
Do
4.Evaluation of asset value
5.Performance of change management
Check/Act
Asset management process (AMP)
SecMan(11)_F08

Figure 10 –The concept of the asset management process

Recommendation ITU-T X.1057 provides guidelines of detailed activities in each process which cover: establishment of asset management policy; survey and identification; classification and registration; evaluation of asset value; and performance of change management. ITU-T X.1057 also describes the telecommunication-specific assets with examples as shown in Table 4.

Pre-published

Table 4 – Examples of general and telecommunication-specific assets

Asset type	Description	Examples	
		Telecommunication-Specific	General
Electronic information	Information stored in electronic format	Telecommunication service customer information (database), network session and access log, network configuration files, service use and access policies, etc.	Database (office DB, etc.), data files (office policy and guidelines, CCTV log, etc.), system files (configuration files, log files, etc.), etc.
Paper	Paper-held information: documents or records to be produced and used in tasks	Contracts and agreements including SLA, network architecture diagrams, IP address list, cabling diagrams, server system diagrams, network operating system manuals, etc.	Contracts and agreements; system documents (network configuration diagrams, user manuals, etc).
Software	Software developed commercially or for the organization itself	Network operating system, network scanner, early warning detection tools and utilities, audit trail software, etc.	Application software (e.g. office applications); system software (e.g. OS, DBMS, vulnerability scanner); development tools and utilities.
Hardware	Server and network devices used for internal and external services or businesses	Servers (e.g. DNS Server, DHCP server, log server, authentication server, NTP server, NMS server, monitoring server); network and communications equipment (e.g. backbone router, switch, CMTS, NAS/RAS, AP, modem); security equipment (e.g. ESM, firewall, IPS, IDS, VPN, virus wall, vaccine); mobile systems; satellite systems (stations); microwave systems; transmission system; etc.	Server (e.g. Web server, DB server, WAS, log server, backup server, storage); mainframes, network and communications equipment (e.g. switches); security equipment; desktops; workstations; laptops; handhelds; etc.
Facility	The place in which systems are installed and operated, which include physical spaces and various supporting equipment rooms	Cabling facilities; network management and monitoring facilities; telecommunication equipment room; Internet data centre; etc.	Office building; server room; paper room; electrical equipment room; etc.
Supporting utility system and equipment	Equipment used for supporting information system operation, which includes power supply, air-conditioning equipment and so on	Mobile, satellite and fixed network supporting utilities (generator, UPS, etc.), etc.	Electrical equipment; air-conditioning equipment; fire extinguishing equipment; CCTV; etc.

5.5 Risk management of their assets globally accessible in IP-based networks

Telecommunications organizations have become more progressive to leverage the benefits of both legacy and Internet services. Some of these organizations have transferred their legacy services to the Internet, such as using IP technology to provide voice services instead of using circuit-switched technology and even integrating voice services such as voice over long-term evolution (VoLTE) with ordinary voice over IP (VoIP). Some organizations have merged Internet flexibility into legacy services, for example, by providing customers to use web portals to send messages out to the mobile terminals or to check messages and missed calls. Some organizations also utilize the Internet to provide customer self-service experiences, for example, by allowing customers to update their contracts and make transactions online.

During this transformation process, a large number of assets are deployed by telecommunication organizations to bridge the physical network boundary between IP-based networks and telecommunication networks capabilities. Securing these assets globally accessible in IP-based networks has become one of the most obvious challenges for security management teams and the risk management of these assets could be a priority or primary concern for telecommunications organizations.

Recommendation ITU-T X.1059 identifies threats and challenges that could arise when telecommunication network assets are globally accessible in IP-based networks and provides guidance of risk management for a specified category of assets which are globally accessible in IP-based network (AGIT). AGIT is defined as hardware and software assets that can be reached or connected by an IP, an URL address or a certain client, etc. through the infrastructure of public IP networks.

The main risk management process for AGIT and detailed phase and steps in AGIT risk management are illustrated in Figure 11 and Figure 12.

Pre-published

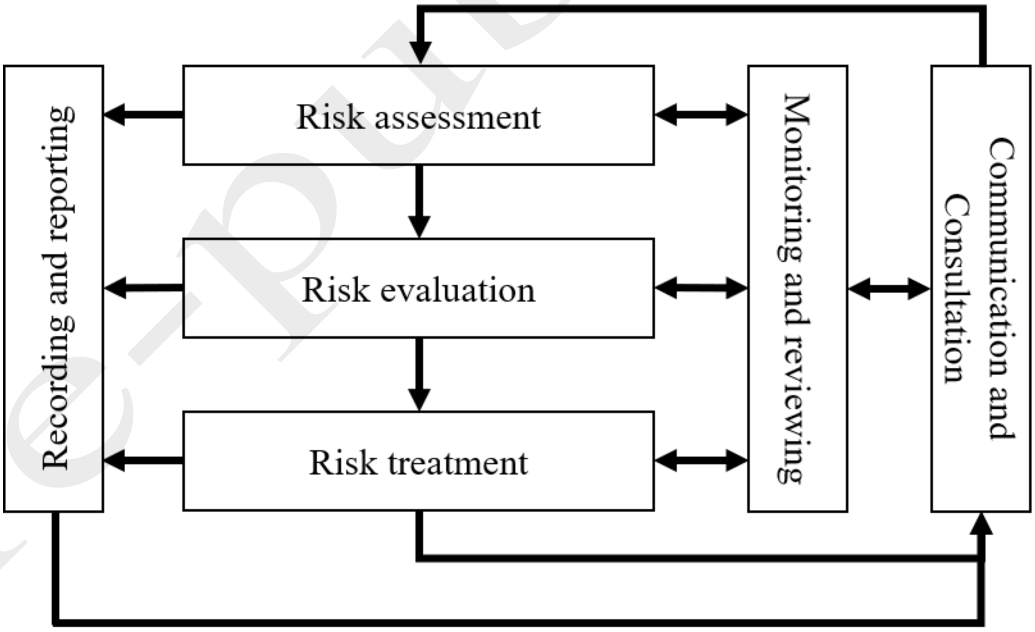


Figure 11 - AGIT risk management process model

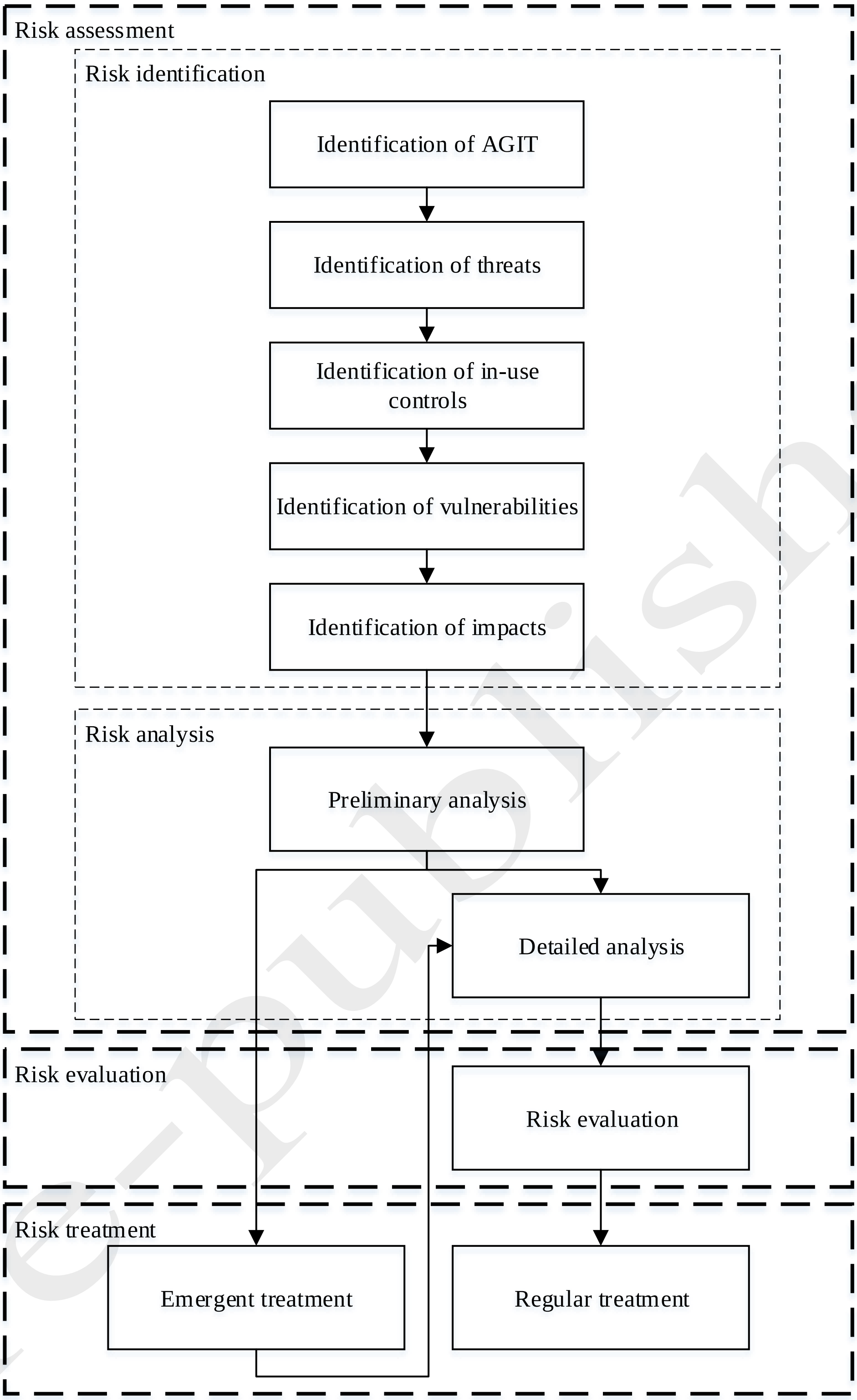


Figure 12 - Phases and steps in AGIT risk management process model

5.6 Governance of information security

One additional important aspect of security management is governance. Governance responsibilities involve the oversight of information security to ensure that the objectives of the organization are achieved.

Pre-published

Recommendation ITU-T X.1054 | International Standard ISO/IEC 27014 provides guidance on the governance of information security.

Governance of information security needs to align objectives and strategies for information security with business objectives and strategies, and requires compliance with legislation, regulations and contracts. It should be assessed, analysed and implemented through a risk management approach, supported by an internal control system.

The governing body (i.e. the part of an organization assigned responsibility for governance) is ultimately accountable for an organization's decisions and the performance of the organization. With respect to information security, the key focus of the governing body is to ensure that the organization's approach to information security is efficient, effective and acceptable, and in line with business objectives and strategies giving due regard to stakeholder expectations. Various stakeholders can have different values and needs.

The governing body performs the "evaluate", "direct", "monitor" and "communicate" processes that govern information security. In addition, the "assure" process provides an independent and objective opinion about the governance of information security and the level attained. Figure 13 shows the relationship between these processes.

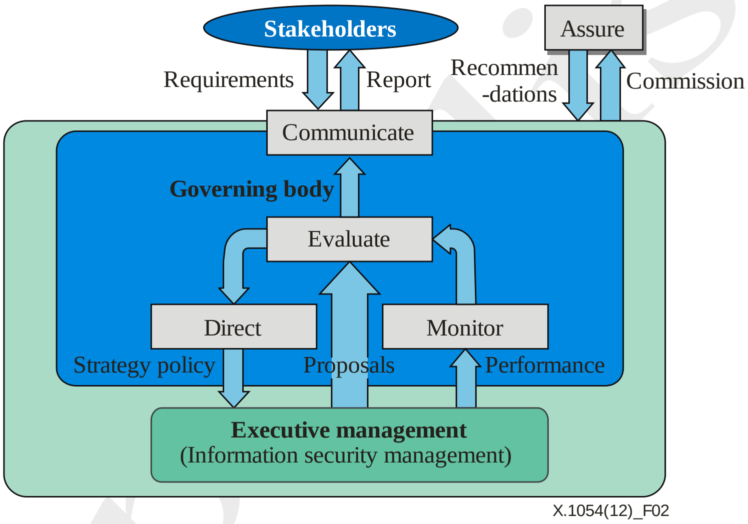


Figure 13 - Implementation of the governance model for information security

Pre-published

5.7 Personally identifiable information protection management

The number of organizations processing personally identifiable information (PII) is increasing, as is the amount of PII that these organizations deal with. At the same time, societal expectations for the protection of PII and the security of data relating to individuals are also increasing. A number of countries are augmenting their laws to address the increased number of high profile data breaches.

As the number of PII breaches increases, organizations collecting or processing PII will increasingly need guidance on how they should protect PII in order to reduce the risk of privacy breaches occurring, and to reduce the impact of breaches on the organization and on the individuals concerned. Recommendation ITU-T X.1058 | International Standard ISO/IEC 29151 provides the guidance for the organizations.

This Recommendation contains implementation guides and other information for PII protection within the same structure as ISO/IEC 27002. The normative annex provides new controls and associated guidance for PII protection corresponding the privacy principles of ISO/IEC 29100. These new PII protection controls are: consent and choice; purpose, legitimacy and specification; collection limitation; data minimization; use, retention and disclosure limitation; accuracy and quality; openness, transparency and notice; individual participation and access; accountability; information security; and privacy compliance.

Figure 14 compares the structure of ISO/IEC 27002 and this Recommendation.

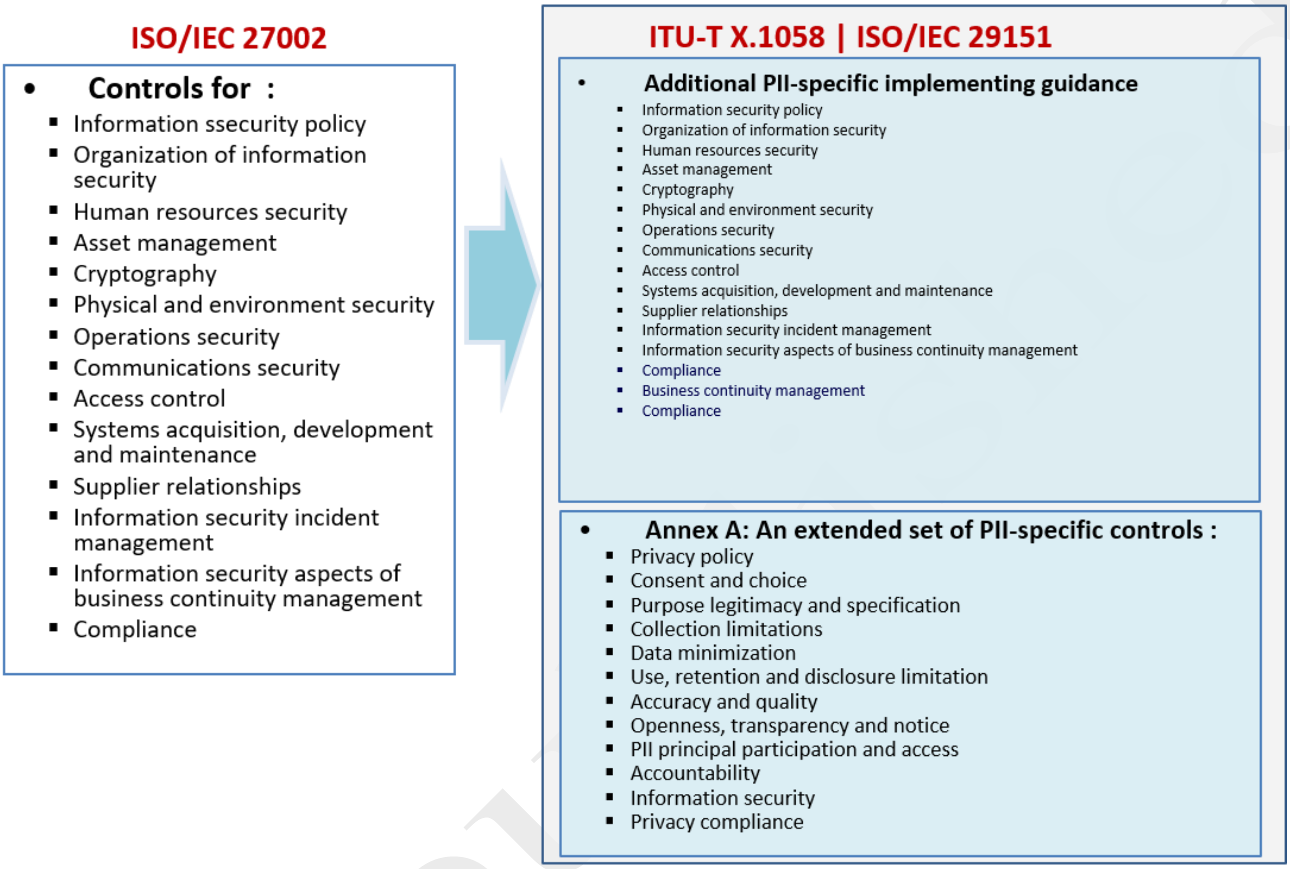

ISO/IEC 27002
Controls for :
Information ssecurity policy
Organization of information security
Human resources security
Asset management
Cryptography
Physical and environment security
Operations security
Communications security
Access control
Systems acquisition, development and maintenance
Supplier relationships
Information security incident management
Information security aspects of business continuity management
Compliance
ITU-T X.1058 | ISO/IEC 29151
Additional PII-specific implementing guidance
Information security policy
Organization of information security
Human resources security
Asset management
Cryptography
Physical and environment security
Operations security
Communications security
Access control
Systems acquisition, development and maintenance
Supplier relationships
Information security incident management
Information security aspects of business continuity management
Compliance
Business continuity management
Compliance
Annex A: An extended set of PII-specific controls :
Privacy policy
Consent and choice
Purpose legitimacy and specification
Collection limitations
Data minimization
Use, retention and disclosure limitation
Accuracy and quality
Openness, transparency and notice
PII principal participation and access
Accountability
Information security
Privacy compliance

Figure 14 – The comparison of the structure of ISO/IEC 27002 and X.1058

5.8 Security management for cyber defence centre

The Recommendation ITU-T X.1060 establishes a framework for organizations to build and manage a cyber defence centre (CDC), and to evaluate its effectiveness. The framework indicates how a CDC should determine and implement security services to enable the security of an organization. This Recommendation is intended for those responsible for security at the top management level of an organization, such as the chief security officer (CSO) or chief information security officer (CISO) and security supervisors who assist them.

Organizations act to make their businesses successful. In order to manage risks to business activities, the CISO formulates security policies, especially from a cybersecurity perspective. A CDC is an entity that implements security policies specifically as CDC services, which consist of security activities that are performed by teams responsible for security. CDC services may specify security functions as capabilities of a system to perform security-related processing. Figure x shows stakeholders and their roles for CDC operation.

Pre-published

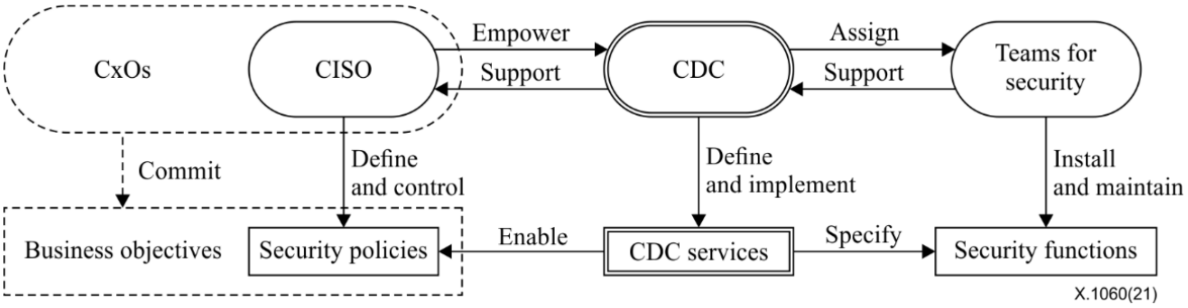


Figure 15 - Stakeholders and their roles for CDC operation

Pre-published

6. The role of the Directory and the importance of the ITU-T X.500 series of Recommendations

Pre-published

6 The role of the Directory and the importance of the ITU-T X.500 series of Recommendations

The ITU-T X.500 series of Recommendations provides specifications for establishment of a directory (referred to below as an ITU-T X.500 directory).

A directory is a term for an organized collection of information that can be queried to obtain specific information. Within the ITU-T and within the context of security and telecommunications standardization, the term *X.500 directory* refers to a repository of information based on the ITU-T X.500 series of Recommendations that were developed jointly with ISO/IEC. The directory specification is introduced in Recommendation ITU-T X.500 and elaborated in Recommendation ITU-T X.501, Recommendation ITU-T X.511 specifies the service provided by an X.500 directory. Recommendation ITU-T X.518 specifies the procedure for a distributed directory. Recommendation ITU-T X.519 provides directory protocols to facilitate communication and information exchange between entities. Recommendation ITU-T X.525 specifies how directory information may be replicated. The Recommendations ITU-T X.520 and ITU-T X.521 provide metadata for directory information.

Recommendation ITU-T X.509 is part of the ITU-T X.500 series of Recommendation, but is widely used outside a directory context. It provides a framework for both public-key infrastructure (PKI) and for privilege management infrastructure (PMI). An X.500 directory may store PKI-related and PMI-related information objects to support those infrastructures, and an X.500 directory may use PKI and PMI capabilities to protect directory information. Recommendation ITU-T X.510 completes ITU-T X.509 by providing protocol specifications for secure operations.

This section begins with a review of the cryptographic concepts relevant to Recommendation ITU-T X.509. This is followed by a discussion of Recommendation ITU-T X.509 and its support of PKI and PMI. The security of an ITU-T X.500 directory itself and the need to protect directory information is discussed later.

6.1 Cryptographic concepts relevant to Recommendation ITU-T X.509

Cryptography is a key component of both PKI and PMI. Three aspects of cryptography are considered here:

- algorithms using both symmetric and asymmetric keys;
- hash functions; and
- digital signature generation and verification.

These three areas are described briefly below.

6.1.1 Symmetric and asymmetric key cryptographic algorithms

Symmetric (or *secret key*) cryptography refers to a cryptographic system in which the same key is used for both encryption and decryption, as illustrated in Figure 16(a). In a symmetric cryptosystem, communicating entities share a unique secret key. The key must be distributed to the entities by secure means.

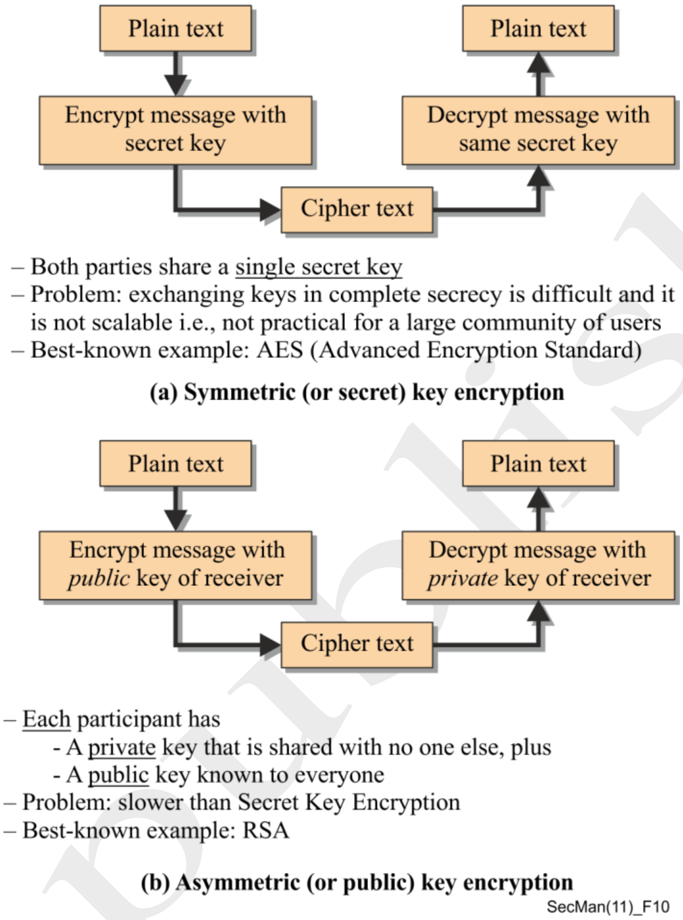
An *asymmetric* (or *public key*) cryptography system involves a pair of keys – a public key and a private key. The public key can be widely distributed but the private key must always be kept secret by the owning entity. The private key is usually held on a smart card or on a token. The public key and the private key are mathematically related, but there is no feasible way to derive the private key from the public key.

There are different types of asymmetric key pairs. Some technologies (such as RSA) allow encryption and decryption of data, while other technologies allow only generation and validation of digital signatures.

Pre-published

RSA technology, named after the inventors Ron Rivest, Adi Shamir and Len Adleman, allows or encryption and decryption as illustrated in Figure 16(b). Data encrypted by one of the keys of a key pair can be decrypted only by the other key. To send confidential data securely to someone, the sender encrypts the data with the recipient's public key. The recipient then decrypts it with their corresponding private key.

If the private key is used for encryption, anyone in passion of the public key may decrypt the message. This does not provide for confidentiality, but for authentication of the sender, as only the owner of the corresponding private key could have encrypted the data.


Plain text
Encrypt message with secret key
Cipher text
Decrypt message with same secret key
Plain text
Plain text
Encrypt message with *public* key of receiver
Cipher text
Decrypt message with *private* key of receiver
Plain text
SecMan(11)_F10

– Both parties share a single secret key
– Problem: exchanging keys in complete secrecy is difficult and it is not scalable i.e., not practical for a large community of users
– Best-known example: AES (Advanced Encryption Standard)

(a) Symmetric (or secret) key encryption

– Each participant has
  - A private key that is shared with no one else, plus
  - A public key known to everyone
– Problem: slower than Secret Key Encryption
– Best-known example: RSA

(b) Asymmetric (or public) key encryption

Figure 16 – Illustration of secret key and public-key encryption processes

Figure 16 illustrates confidentiality using the two modes of encryption. With symmetric encryption, each pair of entities must have different keys and these must be distributed and held securely. With RSA asymmetric encryption, on the other hand, the public encryption keys can be published in a directory and everyone can use the same (public) encryption key to send data to a particular entity securely. This makes asymmetric encryption much more scalable than symmetric encryption. However, asymmetric encryption is costly in terms of computing time, so it is not efficient to encrypt entire messages using asymmetric encryption. A way around this problem is to have one of the entities in an exchange create a symmetric key, encrypt it using a designated peer entity's public key and then transmit the encrypted symmetric key to that peer entity. The symmetric key is then used to encrypt the body of the messages exchanged between the two entities. Another method to generate symmetric keys is the so-called Diffie-Hellman Key Exchange, as defined in IETF RFC 2631.

Pre-published

Pre-published

6.1.2 Hashing

A *hash function or hashing algorithm* is a mathematical function that specifies how to take an arbitrary message (bit string) and produce a (much smaller) fixed-length hash value called a *digest*. A good hash algorithm is designed to satisfy the following properties:

– It is a one-way algorithm, meaning it is infeasible to find a message that maps to a specific given digest.

– It is infeasible to modify a message without changing the digest.

– It is collision resistant, meaning it is infeasible to find any two distinct messages that map to the same digest.

Many different hashing algorithms of different quality have been defined. A hashing algorithm can be broken either by brute force or by finding some ingenious way to break the algorithm without excessive use of computing power. Some popular hashing algorithms, like MD2 and MD5 are now considered unsafe and should not be used. The US National Institute of Standards and Technology (NIST) has published a number of *secure hashing algorithms* (SHAs) in a series of NIST FIPS PUB 180 standards. One of the first algorithms, SHA-1, is now considered unsafe, while SHA 224, 256, etc. are considered safe for many years to come. However, there is always the risk that some organization will break a secure hash algorithm without announcing it.

Hashing can be used to assure integrity of data. If both the sender and the recipient of data generate a digest of the data, and the two digests are identical, it is safe to assume that the data has not been modified during transfer (unless the hashing algorithm has been broken).

6.1.3 Digital signature generation and validation

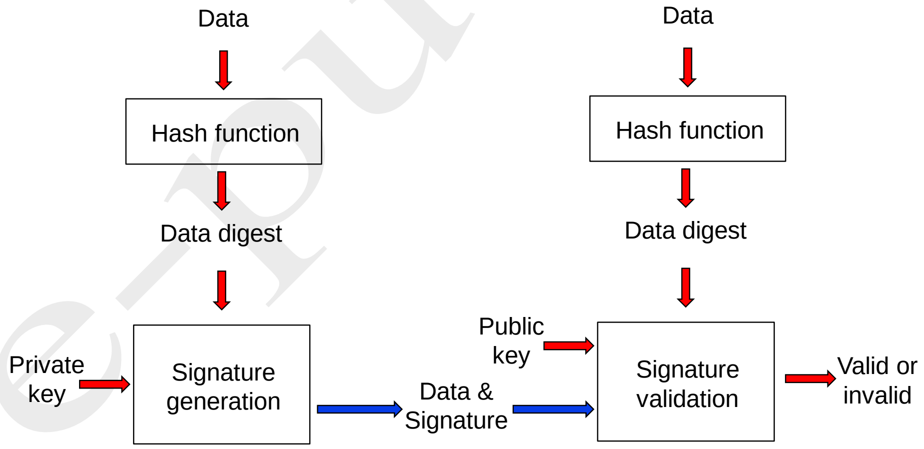


Figure 17 – Generation and validation of digital signature

Figure 17 illustrates the principle of digital signature generation and validation. The signer creates a digest of the data to be transmitted. The digest, along with the private key of the signer, is input to the algorithm used to generate the signature. The signature is then added to the data to be transmitted. The verifier having received the data with the digital signature calculates its own digest using the same hashing algorithm as the signer. This digest together with the public key of the signer is input to another function that will indicate whether the signature is valid or invalid. If the data has been changed in any way, or if the private key used for signature generation is not the one expected, the signature will be flagged as invalid.

This procedure works only if the two partners use the same hashing algorithm and the same asymmetric key algorithm. The combination of a hashing algorithm and an asymmetric key algorithm is called a signature algorithm. The signature algorithm used is typically identified and transmitted along with the data and the digital signature.

In case of the RSA asymmetric key algorithm, the signer uses its private key to encrypt the digest and to generate the signature while the verifier decrypts the signature using the corresponding public key to retrieve the original digest and then compares it with its own calculated digest. This technique has been predominant during recent years, but other techniques based on elliptic curve digital signature algorithms are gaining momentum.

6.2 Public-key infrastructure (PKI)

In order to trust digitally-signed data, it is crucial to know the identity of the entity to which the corresponding asymmetric key pair belongs. There is no point in trying to verify a digital signature if you are not sure who created it. The binding of a key pair to an identity is documented in a *public-key certificate* which must be trusted. A *public-key infrastructure* (PKI) is a mechanism for establishing trust in the key pairs and the public key certificates. Recommendation ITU-T X.509 provides the framework for public-key certificates and PKI. This section describes public-key certificates and provides an introduction to PKI.

6.2.1 Public-key certificates

A *public-key certificate* is the standard way to bind a public key, and thereby the corresponding private key, to the identity of the owner of the key pair. A trusted authority, called *certification authority (CA)*, attests to this binding by digitally signing the public-key certificate. Recommendation ITU-T X.509 defines the structure of a public-key certificate.

A public-key certificate consists of:

- the version of the public-certificate structure. (Version 3 indicates the latest version and the one that is mostly required);
- a unique serial number within the scope of the issuing CA;
- the signature algorithm used for signing the public-key certificate;
- the name of the issuing CA;
- the time period during which the public-key certificate is valid;
- the subject, i.e., name of the entity to which this public-key is issued;
- the public key associated with this public-key certificate;
- two components that give alternative unique identifiers of the issuer and the subject. (These components are deprecated and should normally be absent);
- an optional list of extensions allowing additional information to be included in the public-key certificate; and
- the CA signature, which certifies the public-key certificate and ensures that it cannot be modified without detection.

A public-key certificate can be widely published, for example on a web site or in a directory.

Pre-published

6.2.2 Elements of a public-key infrastructure

A public-key certificate has to be validated before it is accepted. For example: it might have expired; it might have been revoked; it may not be acceptable for a particular use; or some constraints may not be fulfilled. This validation is done via a public key infrastructure.

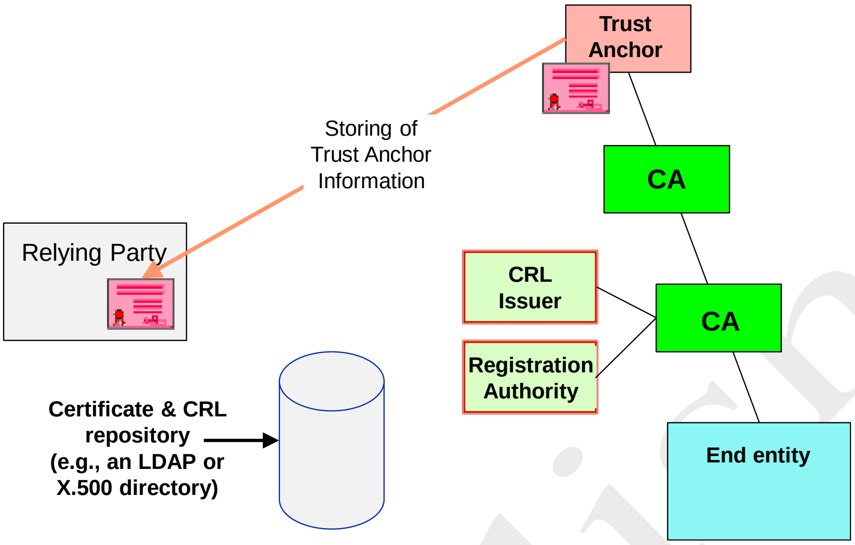

Trust Anchor
Storing of Trust Anchor Information
CA
Relying Party
CRL Issuer
CA
Registration Authority
Certificate & CRL repository (e.g., an LDAP or X.500 directory)
End entity

Figure 18 – Components of a PKI

Figure 18 illustrates the components of a PKI as defined by Recommendation X.509:

- An *end entity* is an entity to which a public-key certificate has been issued. An end entity cannot issue public-key certificates to other entities.
- A certification authority (CA) is an entity that may issue public-key certificates to other CAs and to end entities. A public-key certificate issued to a CA is also called a CA certificate. A public-key issued to an end entity is called an end-entity public-key certificate. A CA has responsibilities beyond just issuing the certificate. It must verify that the information included in public-key certificate to be issued is correct. This may be delegated to a separate function, called a registration authority, which then is responsible for doing all the checking. The CA is also responsible for maintaining the status of the public-key certificates it has issued. A public-key certificate may be revoked for several reasons. For example, the private key might have been revealed (compromised) or responsibilities of those involved may have changed. Revoked public-key certificates may be added to a *certificate revocation list (CRL)*. The CA may delegate the maintenance and publication of CRLs to a CRL issuer.
- A *relying party* is an entity that makes a decision based on the content of a public-key certificate issued to some other entity and therefore needs to validate the public-key certificate.
- It is an inherent part of PKI that somewhere there is a point of absolute trust. Such a point is called a *trust anchor*. There may, in fact, be many trust anchors. A relying party may identify one or more trust anchors from locally-stored information about recognized trust anchors. This information is typically in the form of a public-key certificate. A trust anchor functions as a CA by issuing CA certificates to other CAs and may in principle also issue end-entity public-key certificates.

Each CA will operate according to a set of policies. Recommendation ITU-T X.509 provides mechanisms for distributing some of this policy information in extensions of public-key certificates issued by the CA. The policy rules and procedures followed by a CA are usually documented in a *certificate policy* (CP) and a

Pre-published

certification practice statement (CPS), which are published by the CA. These documents help to ensure a common basis for evaluating the trust that can be placed in the public-key certificates issued by a CA, both internationally and across sectors. They also provide part of the legal framework necessary for building up inter-organizational trust, as well as specifying limitations on the use of the issued public-key certificates.

When a relying party needs to validate a public-key certificate, it must establish a *certification path*. A certification path is a chain of public-key certificates where the subject in one public-key certificate is the issuer in a subsequent public-key certificate. The top public-key certificate (typically a CA certificate) must be issued by a trust anchor recognized by the relying party. This is illustrated in Figure 19.

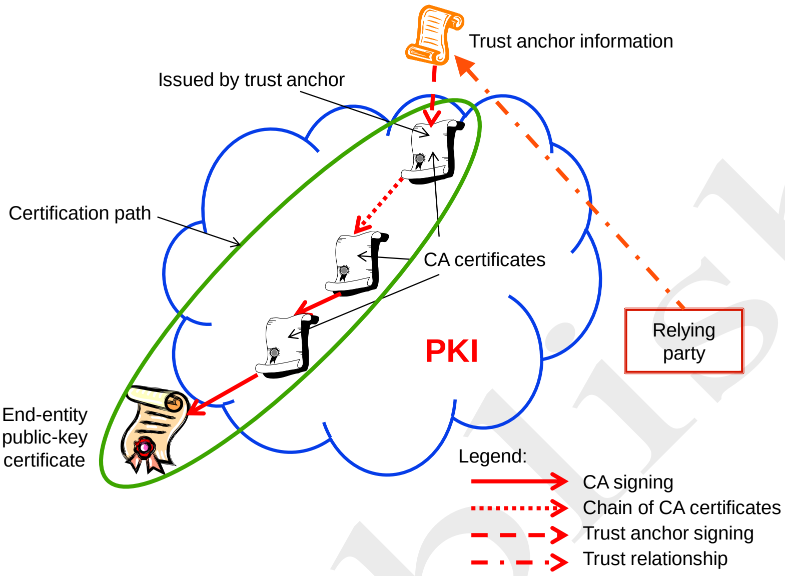


Figure 19 – Certification path

Each public-key certificate on the certification path needs to be validated. In principle, the certificate policy related to each public-key certificate must be observed. However, certificate policies are provided in non-machine readable format leaving it to a human user to make the judgement. However, human users may not be capable of judging the policy requirements and, in many situations, there may be non-human users involved.

The next edition of Recommendation ITU-T X.509, expected to be completed in 2016, will include significant enhancement to ensure efficient and secure validation of public-key certificates:

– A new type of PKI component, called *trust broker*, provides a service for relying parties when validating public-key certificates. A trust broker keeps track of a set of CAs and the policies under which they issue public-key certificates. When validating a public-key certificate, a relying party may consult the appropriate trust broker to check its validity.

– Some relying parties may communicate only with a limited set of other entities and they may be required to observe restrictions on the communications, e.g., to accept only communications over a limited set of communications protocols. The necessary information is supplied to a relying party in an *authorization and validation list (AVL)*. This list is supplied and maintained by a new PKI component called the *authorization and validation manager (AVM)*. Some relying parties may be constrained with respect to processing power, storage, bandwidth and time and cannot afford to go to a third party to validate public-key certificates. In such an environment the AVL may be extended to provide up-to-date validation information. It is the responsibility of the AVM to keep such an AVL up-to-date.

Pre-published

6.3 Privilege management infrastructure (PMI)

A privilege management infrastructure (PMI) manages privileges to support a comprehensive authorization service in relationship with a PKI. The mechanisms defined allow for setting user access privileges in a multi-vendor and multi-application environment. The concepts of PMI and PKI are similar, but PMI deals with authorization while PKI concentrates on authentication. Table 5 illustrates the similarities between the two infrastructures.

Table 5 – Comparison of privilege management and public-key infrastructure features

Privilege management infrastructure	Public-key infrastructure
Source of Authority (SoA)	Root Certification Authority (Trust Anchor)
Attribute Authority	Certification Authority
Attribute certificate	Public-key certificate
Attribute certificate revocation list	Certificate revocation list
Authority revocation list for PMI	Authority revocation list for PKI

The purpose of assigning privileges to users is to ensure that they follow a prescribed security policy established by the Source of Authority. Policy-related information is bound to a user's name within the attribute certificate and comprises a number of elements illustrated in Table 6.

Table 6 – Structure of an ITU-T X.509 attribute certificate

Version
Holder
Issuer
Signature (Algorithm ID)
Certificate Serial Number
Validity Period
Attributes
Issuer Unique ID
Extensions

Attribute certificates are also used in telebiometrics to create biometric certificates to bind a user to his/her biometric information. Biometric device certificates define capabilities and limitations of biometric devices. Biometric policy certificates define the relationship between a security level and biometric algorithm parameters.

Five components for the control of a PMI are described in Recommendation ITU-T X.509: the privilege asserter; the privilege verifier; the object method; the privilege policy; and environmental variables (see Figure 20). The privilege verifier can control access to the object method by the privilege asserter, in accordance with the privilege policy.

Prepublished

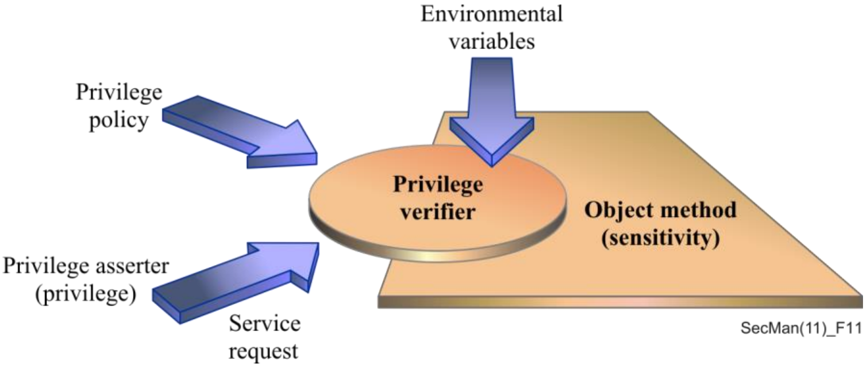


Figure 20 - ITU-T X.509 PMI control model

Where delegation of privilege is necessary for an implementation, four components of the delegation model for PMI are considered in Recommendation ITU-T X.509: the privilege verifier; the source of authority; other attribute authorities; and the privilege asserter (see Figure 21).

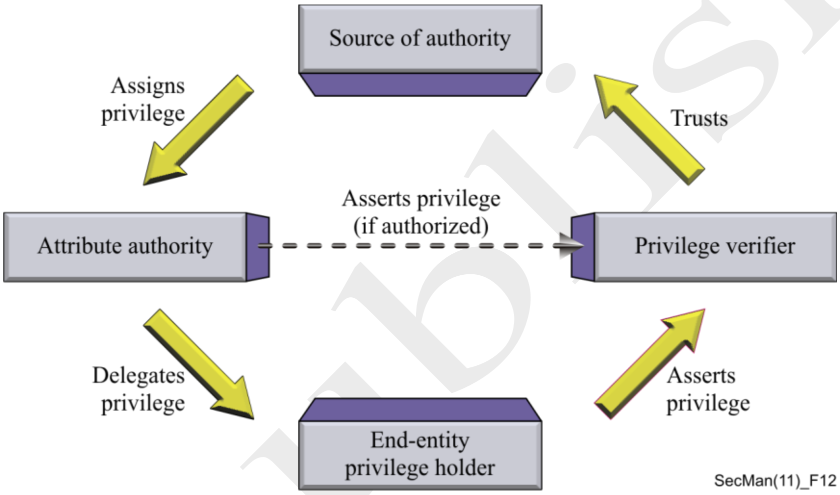


Figure 21 - ITU-T X.509 PMI delegation model

Recent implementations of authorization schemes following the Role-Based Access Control (RBAC) model consider that the user is given a role. The authorization policy associates a set of permissions with that role. When accessing a resource, the user has his or her role checked against the policy to enable any subsequent action.

The early versions of Recommendation ITU-T X.509 (1988, 1993 and 1997) specified the basic elements needed for PKIs, including the definition of public-key certificates. The revised Recommendation ITU-T X.509 approved in 2001 (and updated in 2005, 2008 and 2012) contains a significant enhancement on attribute certificates and a framework for privilege management infrastructure (PMI).

6.4 Protection of directory information

Directory data protection is primarily a privacy issue (i.e., protecting against unauthorized disclosure of sensitive personal information), but it also involves ensuring integrity of the data and protecting the assets represented by the data.

A directory holds information about entities which may be sensitive and should be revealed only to those having both a *right* and a *need-to-know*.

Pre-published

Pre-published

There are three aspects of data protection:

- authentication of the user who seeks to access the information;
- access control to protect data against unauthorized access. (Note: access control is dependent on proper authentication); and
- data privacy protection, which is dependent on proper access control.

Data privacy protection features have always been a key part of Recommendation ITU-T X.500, which is the only directory specification that has these important features.

6.4.1 Authentication of Directory users

An ITU-T X.500 directory may allow anonymous access to some of its non-sensitive information. However, for access to more sensitive data, some level of authentication of users is necessary. Recommendation ITU-T X.500 allows four levels of authentication including:

a) name only;

b) name plus unprotected password: the password is transmitted in clear text on the connection (which, when using the TCP/IP stack, can be encrypted with TLS). Password policy provides mechanisms to ensure that users change their passwords periodically and those passwords meet quality requirements and cannot be re-used before some set period. A user can also be locked out after a certain number of authentication failures;

c) name and protected password (i.e., a password that is hashed together with some additional information to ensure that any attempt to access the Directory by replaying the hashed value will be detected); and

d) strong authentication, where the sender digitally signs certain information. The signed information consists of the name of the recipient and some additional information that allows detection of attempted replay.

Different levels of data protection are required for different types of accessing users. The user's authentication level is also used to determine the user's access rights.

6.4.2 Directory access control

Access control is used to permit or deny operations on pieces of directory information. Recommendation ITU-T X.500 is very flexible in how directory information is accessed and users can be subdivided for access control purposes. A piece of information that is protected is called a protected item. Protected items may be grouped for common access control properties. Users may likewise be grouped according to access permissions or denials.

The access rights of a user or a group of users depends on the level of authentication. Retrieving sensitive information or updating entries will normally require a higher level of authentication than retrieving less sensitive information.

Access control also takes the type of data access into account, e.g., read, add, delete, update, and change of names. In some cases, users may not even be aware of the existence of certain pieces of information.

Access control is about the right-to-know. However, the need-to-know goes beyond access control. Having a *right-to-know* does not allow a user to retrieve information if a *need-to-know* is not established. If *need-to-know* is not established, disclosure of information could be a privacy violation.

There are several other examples when a *right-to-know* is not sufficient. For instance:

- even if a user has the right to retrieve the individual postal addresses of some entities, it may not be appropriate to permit bulk retrieval of postal addresses; and
- if a user has access rights to some information, it may not be relevant to the particular application for which the retrieval is performed, in which case there is no *need-to-know* and the information should not be revealed.

6.4.3 Privacy protection

Data privacy protection in Recommendation ITU-T X.500 is unique and very powerful. Data privacy measures include protection against unwarranted searches that return a substantial amount of information. (Such searches are sometimes called *data trawling*.)

Recommendation ITU-T X.500 uses a table-driven service administration concept which, in addition to administration of general services, also provides data privacy protection capabilities. The administrator creates one or more tables for each combination of service type and group of users. For data retrieval to succeed, there must be a table that exactly matches the type of service and the type of user group when a user searches the Directory by supplying general search criteria. However, this is not enough. The table is protected by access control so the user must also have permission to access the relevant table.

A table, also called a search rule, may hold information such as:

- the required search criteria to ensure that the search is targeted to result in the return of information about one, or very few, entities. This prevents searches that return substantial information and protects against data trawling;
- a list of pieces of information relevant to the type of service; and
- control information for individual entities represented in the directory. The table being used interacts with the control information of an entity to restrict the information returned for that entity. This allows data to be tailored to the privacy protection criteria for each individual entity. An entity may have special requirements, such as not to disclose the postal address and possibly instead return a fake address. Other entities may not want their e-mail addresses revealed to some groups of users.

Protection of sensitive personal information is of concern for a number of reasons. Several security standards, particularly those relating to authentication of individuals and identity management, involve the collection and storage of sensitive, personally-identifiable information. An increasing number of jurisdictions have legal requirements relating to the collection and use of such information. Security services and mechanisms, many of which are based on ITU-T standards, serve as mechanisms to protect information that is sensitive from a privacy standpoint. Privacy is being addressed in a number of Recommendations, some of which directly address the privacy impact of certain technologies. Examples include Recommendation ITU-T X.1171, which is discussed in more detail in section 12.6 on Tag-based Services, and the guideline on protection for personally-identifiable information in RFID application that is now in development by SG17 as part of the IDM work (please see section 7.1.2).

6.5 Cryptographic concepts relevant to Recommendation ITU-T X.510

Recommendation ITU-T X.510 defines the wrapper protocol specification which can be used for:

- maintaining authorization and validation lists (AVLs)
- subscribing public-key certificate status information from certification authorities (Cas)
- accessing a trust broker

Pre-published

6.5.1 General concepts for securing protocols

The intention of Recommendation ITU-T X.510 is to separate the cybersecurity aspects from the protocol requiring cybersecurity. The wrapper protocol is used to embed a protocol, called the protected protocol, to supply cybersecurity to this protocol.

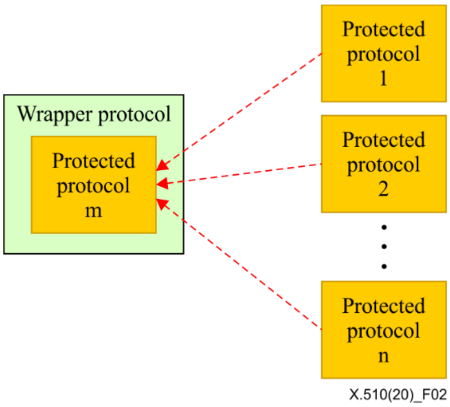


Figure 22 - ITU-T X.510 Protected protocol plug-in

The Figure 23 depicts the communication between two entities running the wrapper protocol protecting an instance of the same protocol.

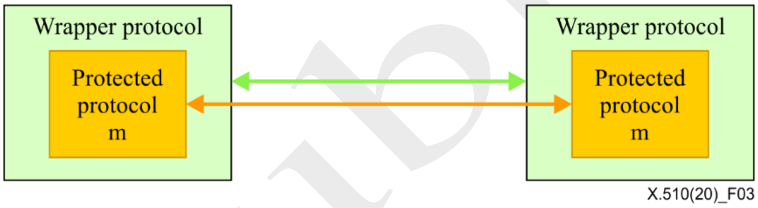


Figure 23 - ITU-T X.510 Embedded communication

6.5.2 X.510 Wrapper protocol general concepts

Two entities communicating with the wrapper protocol use an association with the following steps:

- establishment of an association by exchange of handshake PDUs
- transfer of data
- release of the association

6.6 Protected protocols

Two protected protocols are defined in X.510

- the authorization and validation manage protocol (AVMP) is designed to be protected by the wrapper
- transfer of data.
- the certification authority subscription protocol (CASP) is used by an authorizer to maintain AVL status information by subscribing to the necessary information from relevant Cas

Pre-published

7. Identity management and telebiometric

Pre-published

7 Identity management and telebiometrics

The previous chapter demonstrated the important role played by the Directory in supporting a number of security services and some of the key security mechanisms including the use of public key techniques that can be used to support authentication, encryption, integrity and non-repudiation services. In this chapter two distinct, but not unrelated topics are discussed. First of all, the work on managing digital identity is reviewed. The issue of ensuring that a digital identity (whether of an individual or a device) can be trusted is critical not only to security services such as authentication, authorization and access control but also to services that depend on identity in order to establish trust and prevent fraud and identity theft. The second topic, telebiometrics, is very much concerned with personal identification, authentication and the interface between humans and the digital environment.

7.1 Identity management

7.1.1 Overview of identity management

Identity management (IdM) is the process of securely managing and controlling identity information (e.g., credentials, identifiers, attributes, and reputations) that is used to represent entities (such as service providers, end-user organizations, people, network devices, software applications and services) in a communications process. A single entity may have multiple digital identities in order to access various services with differing requirements, and these may exist in multiple locations. IdM supports authentication of an entity. For ITU-T purposes, the identity asserted by an entity represents the uniqueness of that entity in a specific context.

IdM is a key component of cybersecurity because it provides the capability to establish and maintain trusted communications among entities and enables nomadic, on-demand access to networks and e-services. It also enables the authorization of a range of privileges (rather than all-or-nothing privileges) and makes it easier to change privileges if an entity's role changes. IdM improves an organization's ability to apply its security policies by enabling an entity's activity on the network to be monitored and audited. IdM also facilitates access to entities both inside and outside an organization.

IdM provides assurance of identity information in a manner that supports secure, trusted access control. This is achieved through single-sign-on/single sign-off, user control of personally-identifiable information, and the ability of a user to select an identity provider that can provide verification and delegation functions on their behalf, as opposed to providing credentials to every service provider. IdM also supports a multitude of identity-based services including: targeted advertising; personalized services based on geo-location and interest; and authenticated services to decrease fraud and identity theft.

IdM is a complex technology that includes:

- establishing, modifying, suspending, archiving and terminating identity information;
- recognizing partial identities that represent entities in a specific context or role;
- establishing and assessing trust between entities; and
- locating an entity's identity information (e.g., via an authoritative identity provider that is legally responsible for maintaining identifiers, credentials and some or all of the entity's attributes).

Supplement 7 to the ITU-T X-series of Recommendations provides a brief introduction to the topic of identity management.

7.1.2 Key ITU-T identity management standards

Within ITU-T, IdM work is primarily concentrated in two Study Groups, SG13 and SG17.

Study Group 17, the Lead SG on IdM, is responsible for studies relating to the development of a generic identity management model that is independent of network technologies and that supports the secure exchange

Pre-published

of identity information between entities. This work also includes: studying the process for discovery of authoritative sources of identity information; generic mechanisms for the bridging/interoperability of a diverse set of identity information formats; identity management threats and the mechanisms to counter them; the protection of personally identifiable information (PII); and the development of mechanisms to ensure that access to PII is authorized only when appropriate.

Identity management Recommendations approved to date include: Recommendations ITU-T X.1250, *Baseline capabilities for enhanced global identity management and interoperability*, ITU-T X.1251, *A framework for user control of digital identity*, ITU-T X.1253, *Security guidelines for identity management systems*, and ITU-T X.1275, *Guidelines on protection of personally identifiable information in the application of RFID technology*. Recommendation ITU-T X.1252, *Baseline identity management terms and definitions* provides a set of IdM-related definitions to help ensure uniform and consistent terminology in IdM standards. Recommendation ITU-T X.1254, *Entity authentication assurance framework*, defines four levels of entity authentication assurance and the criteria and threats for each of the four levels. It provides guidance concerning control technologies to be used to mitigate authentication threats as well as guidance for mapping the four levels of assurance to other authentication assurance schemas and for exchanging the results of authentication based on the four levels of assurance. Recommendation ITU-T X.1255, *Framework for discovery of identity management information*, specifies an open architecture framework in which identity management information can be discovered. This framework will enable entities operating within the context of one IdM system to have identifiers from other IdM systems accurately resolved.

Study Group 17 is working closely with the OASIS Trust Elevation Technical Committee to deliver advanced authentication solutions based on X.1254 for step-up authentication. In order to enable a relying party to enhance its trust in the identity of a party, attributes might be aggregated from multiple authorities. The aggregation can be regarded as having to deal with a collection of globally unique identifiers, which is common across all attribute authorities. Recommendation ITU-T X.1258, *Enhanced entity authentication based on aggregated attributes*, introduces the concept of attribute aggregation and provides the architecture and flows for attribute aggregation methods.

Recommendation ITU-T X.1277, *Universal authentication framework*, describes the FIDO universal authentication framework (UAF) that enables online services and websites, whether on the open Internet or within enterprises, to transparently leverage native security features of end-user computing devices for strong user authentication and to reduce the problems associated with creating and remembering many online credentials. Recommendation ITU-T X.1277.2, *Universal authentication framework (UAF) protocol specification*, describes the architecture in detail, it defines the flow and content of all UAF protocol messages and presents the rationale behind the design choices. The goal of the UAF is to provide a unified and extensible authentication mechanism that supplants passwords while avoiding the shortcomings of current alternative authentication approaches. This approach is designed to allow the relying party to choose the best available authentication mechanism for a particular end user or interaction, while preserving the option to leverage emerging device security capabilities in the future without requiring additional integration effort.

Recommendation ITU-T X.1278, *Client to authenticator protocol/Universal 2 factor framework*, describes an application layer protocol for communication between an external authenticator and another client/platform, as well as bindings of this application protocol to a variety of transport protocols using different physical media. Recommendation ITU-T X.1278.2, *Client to authenticator protocol*, describes an application layer protocol for communication between a roaming authenticator and another client/platform, as well as bindings of this application protocol to a variety of transport protocols using different physical media. The application layer protocol defines requirements for such transport protocols. Each transport binding defines the details of how such transport layer connections should be set up, in a manner that meets the requirements of the application layer protocol.

Recommendation ITU-T X.1280, *Framework for out-of-band server authentication using mobile devices*, provides a framework for out-of-band server authentication using mobile devices including the following: 1) defines the out-of-band server authentication model and authentication procedure; 2) defines security threats

Prepublished

and security requirements in the out-of-band server authentication model; 3) defines criteria and guidelines for generating server verification information using mobile devices; and 4) describes use cases of the out-of-band server authentication model. This Recommendation does not address issues related to user authentication, regulation, and privacy considerations.

Study Group 13 (*Future networks including cloud computing, mobile and next generation networks (NGN))* is responsible for NGN-specific IdM functional architecture that supports value-added identity services, the secure exchange of identity information and the application of bridging/interoperability between a diverse set of identity information formats. SG13 is also responsible for identifying any identity management threats within the NGN and the mechanisms to counter them. Recommendation ITU-T Y.2720, *NGN identity management framework*, describes a structured approach for designing, defining, and implementing IdM solutions and facilitating interoperability in heterogeneous environments. SG13 has developed two further IdM Recommendations based on this framework: Recommendation ITU-T Y.2721, *NGN identity management use cases*, which provides an analysis of use case examples relevant to NGN, and Recommendation ITU-T Y.2722, *NGN identity management mechanisms*, which specifies the mechanisms that can be used to meet IdM requirements and deployment needs of NGN.

A Joint Coordination Activity for Identity Management (JCA-IdM) has been operational since 2007. The purpose of the JCA IdM is to coordinate the IdM work within ITU-T and with external organizations. The JCA has established an IdM information resource web page that identifies identity management-related documents of ITU-T and other standards organizations classified by categories, organizations and the status of their work. The IdM Lead Study Group web page provides extensive information on IdM activities, approved and developing IdM recommendations and other information related to the IdM work. This IdM “landscape” is available at http://groups.itu.int/itu-t/StudyGroups/SG17/IdmRoadmap.aspx.

7.2 Telebiometrics

Telebiometrics focuses on two aspects: personal identification and authentication using biometric devices; and quantifiable metrics of interaction between humans and telecommunication environment. In particular, it focuses on how safety and security of identification or authentication of users can be improved by the use of telebiometric methods. The work of ITU-T on this topic is being done in close cooperation with other standards development organizations. The results to date include: interaction between a human being and the environment; telebiometrics in e-health and telemedicine; biometric digital keys; biometric extensions for ITU-T X.509 certificates; and biometric authentication in an open network.

7.2.1 Telebiometric authentication

Biometrics is able to support highly-secure authentication services, but the standardization of biometric authentication on an open network faces a number of challenges:

- service providers may not have any information regarding what biometric devices are in use in the end-user's environment, the security level/setting of such devices, or how they are operated;
- the accuracy (as determined by the rate of false acceptances or false rejections) differs between biometric products. Therefore, the service provider cannot claim to maintain a uniform accuracy level; and
- the accuracy of biometric verification is influenced by both environmental factors (e.g., illumination and weather) and human factors (e.g., pose, make-up, lens characteristics and aging).

General biometric authentication protocols and profiles for telecommunication systems in an open network are specified in Recommendation ITU-T X.1084.

Figure 24 illustrates the authentication of an end user via a non-face-to-face open network.

Pre-published

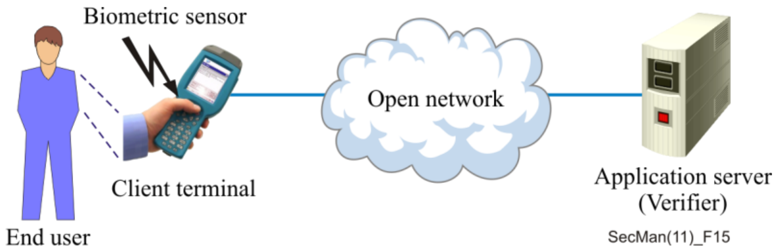


Figure 24 – Telebiometric authentication of an end user

7.2.2 Telebiometric digital key generation and protection

A framework for biometric digital key generation and protection has been defined in Recommendation ITU-T X.1088. This framework defines protection using a biometric template with a public-key certificate and biometric certificate in order to provide cryptographically-secure authentication and secure communications on open networks. Security requirements for biometric digital key generation and protection are also defined. The framework can be applied to biometric encryption and digital signature. Two methods are proposed:

- biometric-key generation, in which the key is created from a biometric template (Figure 25); and
- biometric-key binding/restoring, in which the key is stored in a database and can be extracted by biometric authentication (Figure 26).

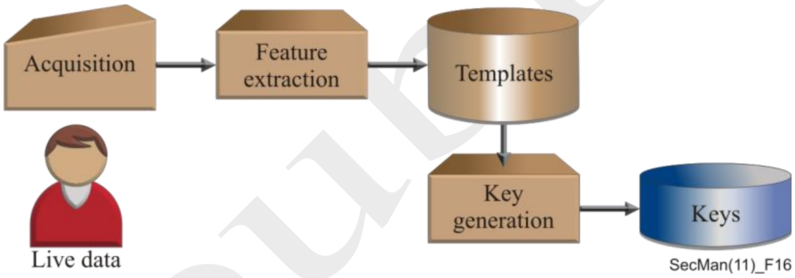


Figure 25 – Biometric-key generation

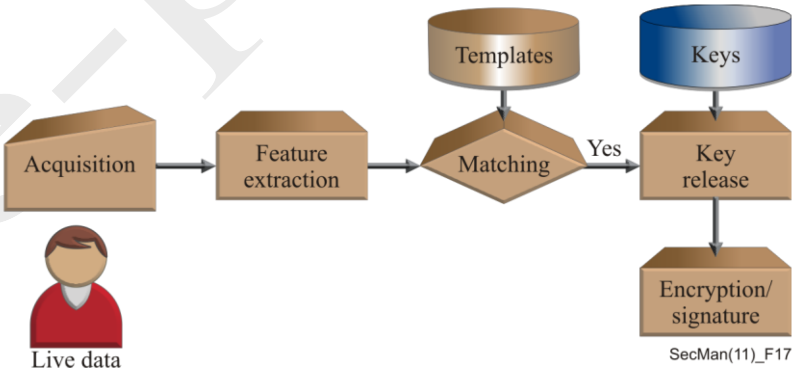


Figure 26 – Biometric-key binding/restoring

7.2.3 Security and safety aspects of telebiometrics

A framework for the security and safety aspects of telebiometrics has been defined in the telebiometric multimodal model (Recommendation ITU-T X.1081), which defines the interactions between a human being and the environment and also the quantities and units used to measure these interactions. This model is not

Pre-published

limited to consideration of purely physical interactions, but also recognizes behavioural interactions which are currently not quantified by standard units.

Recommendation ITU-T X.1086 not only defines the vulnerabilities and threats associated with operating telebiometric systems but also describes countermeasures for protecting biometric devices during their installation, removal, and delivery phases. The specified countermeasures include technical protection schemes of the biometric system in operational procedures as well as the roles and responsibilities of authorized personnel in system supervision.

7.2.4 Telebiometrics related to human physiology

Security and safety aspects of telebiometrics are also addressed in Recommendation ITU-T X.1082, which defines quantities and units for physiological, biological or behavioural characteristics that might provide input or output to telebiometric identification or verification systems (recognition systems), including any known detection or safety thresholds. It gives names, definitions and symbols for quantities and units for telebiometrics related to human physiology (i.e., human characteristics and emissions that can be detected by a sensor). It also includes quantities and units concerned with effects on a human being caused by the use of telebiometric devices.

7.2.5 Telebiometrics authentication using biosignals

Personal identification can be achieved by using biosignals, such as those obtained from a ballistocardiogram (BCG), electroencephalogram (EEG), electrocardiogram (ECG), and photoplethysmogram (PPG) for telebiometric applications of wearable and mobile devices. Recommendation ITU-T X.1094 identifies the requirements and the data exchange format for biosignal sensor, the architecture of telebiometric authentication platform and the biosignal transmission protocol.

7.2.6 One-time telebiometric template

A user-authentication framework using biometric one-time templates has been specified in Recommendation ITU-T X.1090. The framework provides secure user-authentication and protection mechanisms for biometric templates transmitted over open networks by generating a new disposable template for each instance of authentication. An additional Recommendation ITU-T X.1091 describes a general guideline for testing and reporting the performance of biometric template protection techniques based on biometric cryptosystem or cancellable biometrics. This guideline specifies two reference models for evaluation, which use biometric template protection techniques in telebiometric systems. It then defines the metrics, procedures and requirements for testing and evaluating the performance of the biometric template protection techniques.

7.2.7 Telebiometrics in e-health and telemedicine

Recommendation ITU-T X.1080.1 defines a generic telecommunication protocol that supports interactions between a patient at a local medical station and a remote medical centre that can offer greater expertise. This work relates to generic protocols that provide safety, security, privacy protection and consent for manipulating biometric data in any application of telebiometrics such as e-health, tele-medicine and tele-health.

There are two aspects of this work. This part defines a set of messages, with authentication, integrity and privacy (specified using ASN.1) that provide the telebiometric communications between an operator and a remote telemedicine device. The other part relates to the adequate instances taken from the tables of quantities and units that need to be transmitted in support of the communication. These are related to both measurement (out modalities) and interaction with (in modalities) the human body. These parts of the ITU-T X.1080 series of Recommendations give names and symbols for quantities and units concerned with emissions from the human body that can be detected by a sensor and relayed to a remote clinic, and with effects on the human

Pre-published

body that can be produced by the telebiometric medical devices and robots in its environment, or by human medical staff under advice from a remote clinic.

Additionally Recommendation ITU-T X.1092 provides an integrated framework to protect biometric data and private information in e-health and telemedicine. It defines a model of health services using telebiometrics for user identification and authentication. It identifies threats in transmitting various sensory data related to human health and provides countermeasures for secure transmission when applying the integrated framework.

7.2.8 Telebiometrics countermeasures in mobile devices

Biometric technology in mobile devices is frequently used in various areas which require a high level of reliability such as e-banking, and procurement services. It is necessary to make efforts to develop a security system that can pre-emptively cope with potential security threats for the purpose of ensuring mobile biometric data security. Since biometric technology handles sensitive personally identifiable information (PII), some of the privacy issues for biometric in mobile devices should be considered.

Recommendation ITU-T X.1087 specifies the implementation model and threats in the operating telebiometric systems in mobile devices. It provides a general guideline for security countermeasures from both the technical and operational perspectives in order to establish a safe mobile environment for the use of telebiometric systems.

7.2.9 Telebiometrics in access control with Smart ID Cards and for data protection

Recommendation ITU-T X.1080.0, Access control for telebiometrics data protection, is a specification for how to protect telebiometrics information against unauthorized access. It does so by taking a service-oriented view, where only information necessary for a particular purpose is provided, i.e., access is given not only on a right-to-know basis, but also on a need-to-know basis. The heart of this Recommendation is an attribute specification included in an attribute certificate or public-key certificate that specifies in detail what privileges a particular entity has for one or more service types. Security is provided by using a profile of the cryptographic message syntax (CMS). The CMS profile provides authentication, integrity and, when required, confidentiality (encryption).

The biometrics-on-card can be classified into three types such as store-on-card, which is a form in which biometric information is stored in a smart card, compare-on-card in which biometric information is compared in a smart card, and sensor-on-card in which a biometric sensor is embedded in a smart card to acquire, store and compare the biometric information within the card. The application scheme is also divided into two types depending on whether or not the digital signature function is provided by embedding the ITU-T X.509 certificate. X.1093 describes the general scheme for logical and/or physical access control using the biometrics-on-card. This Recommendation can be applied to the recent emerging area of requiring secure physical and also logical access control management.

7.2.10 Telebiometrics in entity authentication service pet animals

Recommendation ITU-T X.1095, *Entity authentication service for pet animals using telebiometrics*, defines an entity authentication infrastructure for pet animals using telebiometrics. It specifies multimodal telebiometrics which uses nose patterns and faces of pet animals. This Recommendation is applicable in various pet animal services such as registration, insurance, and e-healthcare for pet animals. The entity authentication for pet animals is always performed in a non-cooperative environment, therefore it is necessary to define criteria for acquiring suitable multimodal telebiometrics for pet entity authentication. And there are requirements for devices that acquire multimodal telebiometrics, and architecture in the operating platform for stable multimodal telebiometric applications for pet animals. This Recommendation specifies functional requirements on biometric capture devices and data acquisition of biometrics for pet entity authentication. A platform architecture, performance testing methodology, and privacy issues are also defined. The following

Pre-published

topics are addressed in the scope of this Recommendation: Pet animals cover dogs and cats; Multimodal telebiometrics cover nose patterns and faces; Biometric capture devices cover digital cameras, mobile cameras, specific cameras such as infrared cameras, high-speed cameras, and optical scanners.

7.2. 11 Other developments in telebiometric standards

Extensions have been defined for ITU-T X.509 certificates used in public-key infrastructures or privilege management infrastructures to produce biometric certificates. These are specified in Recommendation ITU-T X.1089. Recommendation ITU-T X.1083 specifies the syntax (using ASN.1), semantics, and encodings of messages that enable a BioAPI-conforming application to request biometric operations from BioAPI-conforming biometric service providers (BSPs) across node or process boundaries, and to be notified of events originating in those remote BSPs.

Pre-published

8. Examples of approaches to authentication, non-repudiation, and data de-identification

Pre-published

Pre-published

8 Examples of approaches to authentication, non-repudiation, and data de-identification

A number of standards and guidelines have been published that use a variety of techniques (cryptographic and non-cryptographic) to support security services. Some examples are provided below to illustrate how these techniques are being used to support authentication and non-repudiation services.

8.1 Secure password-based authentication protocol with key exchange

The secure password-based authentication protocol with key exchange (SPAK) is a simple authentication protocol in which use of a human-memorable password between client and server results in mutual authentication and a shared secret that can be used as session keys for the next session.

Requirements for SPAK, together with guidelines for selecting the most suitable SPAK from various secure password authentication protocols, are defined in Recommendation ITU-T X.1151. This protocol is very simple. It is easy to implement and use and, unlike PKI, it requires no other infrastructure. It is expected to be of growing importance to many applications in the future. SPAK provides both user authentication and strong key exchange with a simple password so that a subsequent communication session can be protected by a secret that is shared during the authentication procedure (see Figure 27).

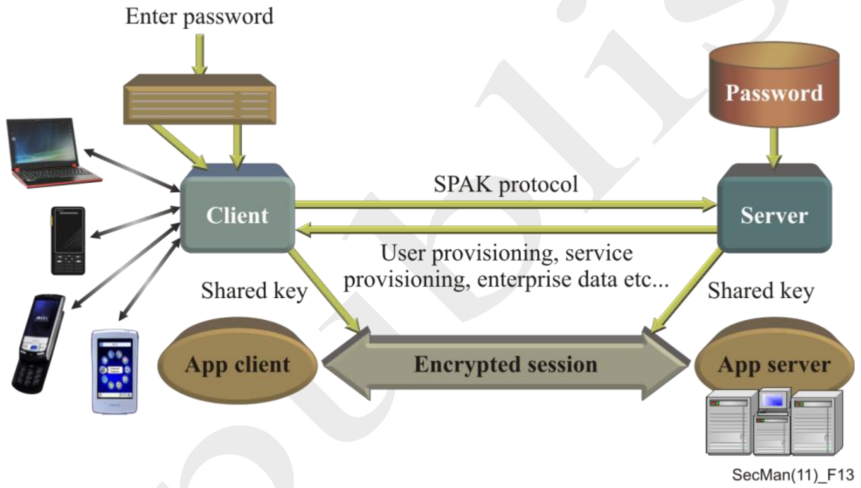


Figure 27 – Typical operation for SPAK protocol

8.2 Extensible Authentication Protocol

The Extensible Authentication Protocol (EAP) supports multiple authentication mechanisms between a supplicant and an authentication server in a data communication network. EAP can be used as a basic tool for enabling user authentication and distributing session keys. It can perform device authentication to establish a secure point-to-point connection and prevent access by an unauthorized device.

Recommendation ITU-T X.1034 describes a framework for EAP-based authentication and key management for securing the lower layers in a communication network. It provides guidance on the selection of EAP methods and describes the mechanism for key management for the lower layers of a data communication network. The framework is applicable to both wireless access networks and wired access networks with a shared medium.

Three entities are required for authentication and key management: a supplicant (or peer); an authenticator; and an authentication server as shown in Figure 28. The supplicant functions as an end-user, accessing the network from an end-user station. The authenticator acts as policy enforcement point, mediating EAP messages between the supplicant and the authentication server. The authentication server authenticates the supplicant, optionally shares a secret that can be used to derive cryptographic keys, posts the result of authentication to the authenticator, and forwards the shared secret to the authenticator. This shared secret can be used to derive cryptographic keys between the authenticator and the supplicant to ensure confidentiality and integrity and enable message authentication.

Authentication and key management generally comprise four operational phases: security capability discovery; EAP authentication; key distribution and key management (see Figure 28). In the security capability phase, a supplicant negotiates the security capabilities and the various parameters of the protocol to be used with the authenticator. In the EAP phase, the authentication server authenticates a supplicant and derives a master secret shared with the supplicant. In the key distribution phase, the authentication server transports the master secret to an authenticator to allow authentication to derive cryptographic keys for a subsequent session between a supplicant and an authenticator. (Fresh cryptographic keys should be used in every session.) Finally, in the key management phase, the authenticator exchanges random numbers with the supplicant to obtain a fresh cryptographic key, resulting in perfect forward secrecy.

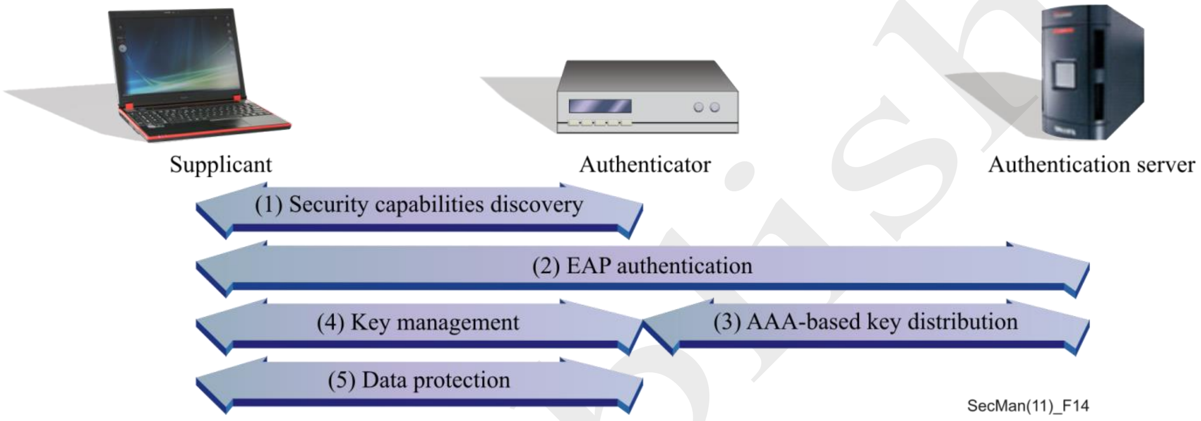


Figure 28 – Operational phases for the authentication and key management of the lower layer

8.3 One-time password authentication

The use of a one-time password (OTP) improves security, preventing the risk of guessing and reusing a password. OTP-based authentication can be used together with other authentication mechanisms (e.g. PKI, static password) to support multi-factor authentication. Recommendation ITU-T X.1153 defines a management framework for one-time-password-based authentication and offers an interoperable management framework that allows sharing of a single one-time password token among different service providers.

8.4 Delegated non-repudiation

Non-repudiation service protects against an entity falsely claiming to have participated in all or part of a communication (e.g. denying having sent or received a message). Recommendation ITU-T X.813 defines six non-repudiation mechanisms: a TTP security token, security tokens and tamper-resistant modules, a digital signature, time stamping, an in-line TTP and a notary. Recommendation ITU-T X.1159 provides a delegated non-repudiation architecture based on Recommendation ITU-T X.813 to generate and verify non-repudiation evidence by a trusted third party (TTP) instead of by a user. In this Recommendation, a right and/or a user's signing key for non-repudiation evidence generation is delegated to a TTP, which acts as a central signing authority that generates and verifies non-repudiation evidence. This delegated non-repudiation model can protect against key loss or theft and is safe in an open network, such as a mobile and cloud network.

A non-repudiation service involves the generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes. The evidence generation requestor requests the evidence generator to generate evidence for an event or action. In this Recommendation, the evidence generation requestor is a user, and the evidence generator is a central signing authority.

Pre-published

The delegated non-repudiation service provides non-repudiation of origin (NRO) and/or non-repudiation of delivery (NRD).

Figure 29 illustrates the concept of the delegated non-repudiation architecture, which shows the interactions of the different entities for the delegated non-repudiation service.

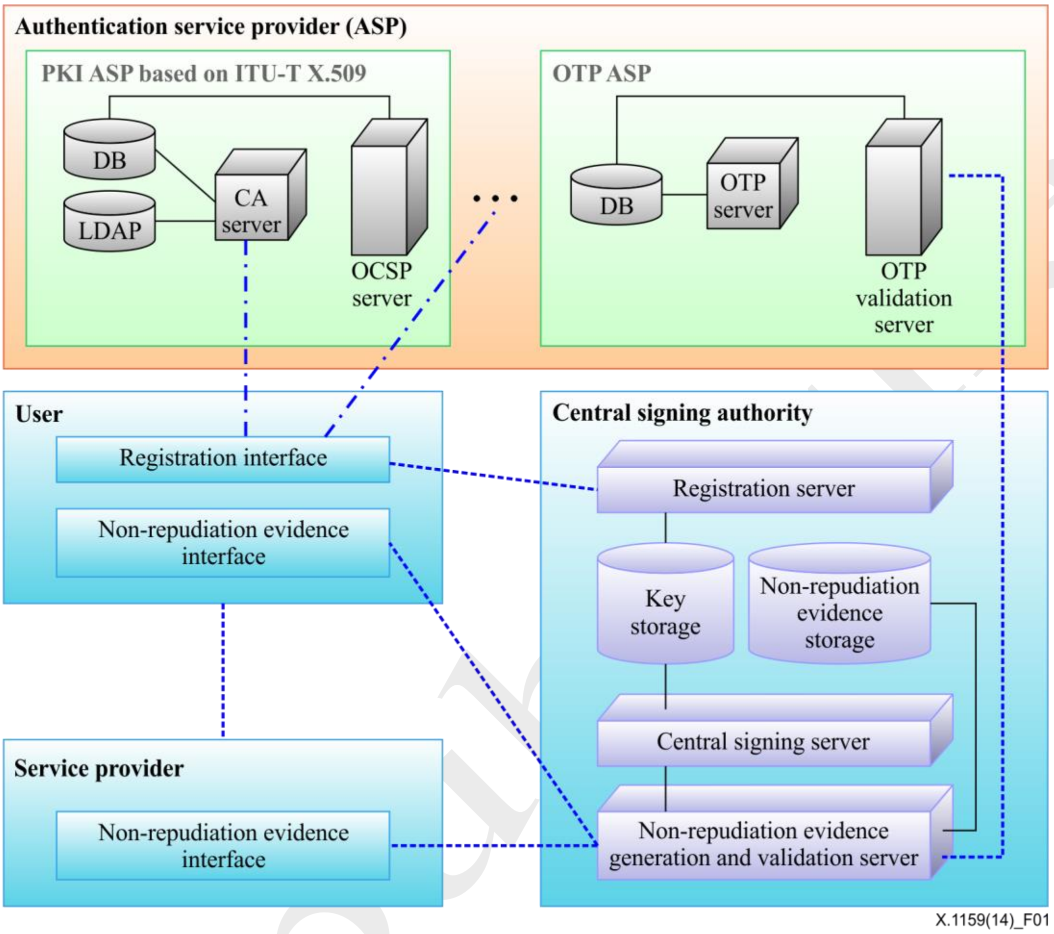

Authentication service provider (ASP)
PKI ASP based on ITU-T X.509
DB
LDAP
CA server
OCSP server
• • •
OTP ASP
DB
OTP server
OTP validation server
User
Registration interface
Non-repudiation evidence interface
Central signing authority
Registration server
Key storage
Non-repudiation evidence storage
Central signing server
Non-repudiation evidence generation and validation server
Service provider
Non-repudiation evidence interface
X.1159(14)_F01

Figure 29 - Concept of delegated non-repudiation architecture

For the delegated non-repudiation service, the user pre-issues a signing key and/or an authentication token through the authentication service provider (ASP). Using the registration interface, the user can register the non-repudiation service to a central signing authority. In this operation, a central signing authority verifies the user's identification and registers a pre-issued authentication token to access a central signing authority. If necessary, the user can register the delegated signing key to a central signing authority in this operation. Using the registration server, a central signing authority registers the user's delegated signing key and stores it securely in the key storage. If the user or the service provider needs to provide the non-repudiation service, they may request from a central signing authority to generate the non-repudiation evidence through the non-repudiation evidence interface. A central signing authority validates the user's transaction-based authentication data before the generation of non-repudiation evidence. The non-repudiation evidence, concatenated with the result of validation, is stored securely in a non-repudiation token storage. In a non-repudiation evidence generation and validation server, the central signing authority can generate and validate the non-repudiation evidence. For the generation of the non-repudiation evidence, a signature is generated by a central signing server which is used only for the access to a key storage. The central signing authority generates the non-repudiation evidence and sends it to the requestor and may also store it in a non-repudiation evidence storage location.

Pre-published

In general, when a non-repudiation service is provided through delegation of a user's signing key to a TTP, the user and the TTP share the same signing key. This limits the non-repudiation service between the objects. Because the delegated signing key is the same as the user's original signing key, the non-repudiation evidence generated by a central signing authority is indistinguishable from the non-repudiation evidence generated by the user. Consequently, in this case, the service cannot provide the non-repudiation between the user and a central signing authority. If the user fully trusts the TTP, the service may be applicable. Otherwise, a delegated signing key for a non-repudiation generation is required to be distinguishable from the user's original signing key. In the delegated non-repudiation service model, the requestor derives the delegated information from the requestor's signing key and then sends the delegated information to a central signing authority. A central signing authority derives the requestor's delegated signing key from the received delegated information by the requestor and from a central signing authority's secret key

8.5 Non-repudiation framework based on a one time password

Recommendation ITU-T X.1156 provides a non-repudiation framework based on a one-time password (OTP) to enhance trust between transaction entities. The non-repudiation framework based on an OTP is to prevent entities from denying that they have sent or received electronic transaction data in the telecommunication network using an OTP. The framework defines entities, non-repudiation tokens and non-repudiation processes. Also, this framework provides security requirements of an OTP-based non-repudiation service, as well as mechanisms for generating non-repudiation tokens. The non-repudiation process is composed of four distinct phases: evidence generation, evidence transfer, evidence verification, and dispute resolution (please see Recommendation ITU-T X.813).

An originator of electronic transaction data generates an OTP using an OTP generation key in conjunction with the data, and sends the TTP (either directly or through a recipient) a request for some evidence of origin. Furthermore, a recipient may ask the TTP to generate the evidence of delivery. Both pieces of evidence of the transaction data are called non-repudiation tokens. After the transaction, both the originator and the recipient may request the TTP to verify the non-repudiation tokens.8.6 De-identification techniques

Recommendation ITU-T X.1148 provides an overview of de-identification process based on data lifecycle model, specifies a de-identification process framework with operational steps and roles of stakeholders in the de-identification process. It further discusses data release models and data stages in a de-identification process and includes various de-identification approaches and examples in its annexes and appendices.

Pre-published

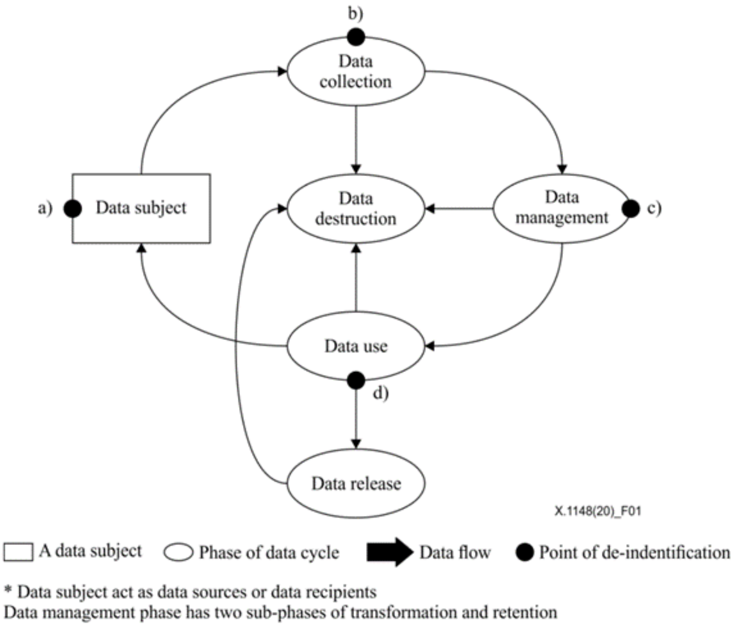

b)
Data collection
a)
Data subject
Data destruction
Data management
c)
Data use
d)
Data release
X.1148(20)_F01
A data subject
Phase of data cycle
Data flow
Point of de-indentification
* Data subject act as data sources or data recipients
Data management phase has two sub-phases of transformation and retention

Figure 30- De-identification process in data lifecycle model

Recommendation ITU-T X.1771 provides security guidelines for information and communication technology (ICT) service providers acting as data controllers and for trusted third parties fulfilling the role of combining de-identified datasets. The purpose of these security guidelines is to reduce data protection risks and promote the utility of the dataset.

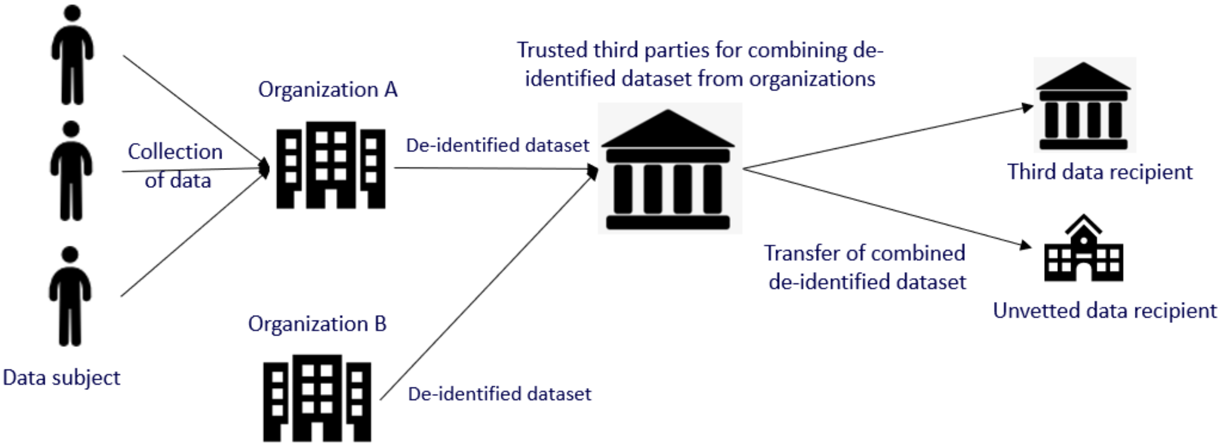


Figure 31 - Extended use case for combining de-identified datasets submitted from different organizations

9. Securing the network infrastructure

Pre-published

9 Securing the network infrastructure

The data used to monitor and control the telecommunications network is often transmitted on a separate network that carries only the network management traffic (i.e., no user traffic). This network is often referred to as the telecommunication management network (TMN) as described in Recommendation ITU-T M.3010. It is imperative that this traffic be secured. The management traffic is usually categorized in terms of information required to perform fault, configuration, performance, accounting and security management functions. Network security management deals with setting up a secure management network as well as managing the security of information related to the three security planes of the ITU-T X.805 security architecture.

Management activity relating to infrastructure elements of a network must always be undertaken in a secure manner. For example, network activities must be performed only by an authorized user. To provide a secure end-to-end solution, security measures (e.g., access control, authentication) should be applied to each type of network activity for the network infrastructure, network services, and network applications. A number of ITU-T Recommendations focus specifically on the security aspect of the management plane for network elements and management systems that are part of the network infrastructure.

Other network management applications include those related to environments where different service providers need to interact to offer end-to-end services. Examples include communications facilities provided to regulatory or government institutions in support of disaster recovery, and situations where leased lines provided to customers cross geographical boundaries.

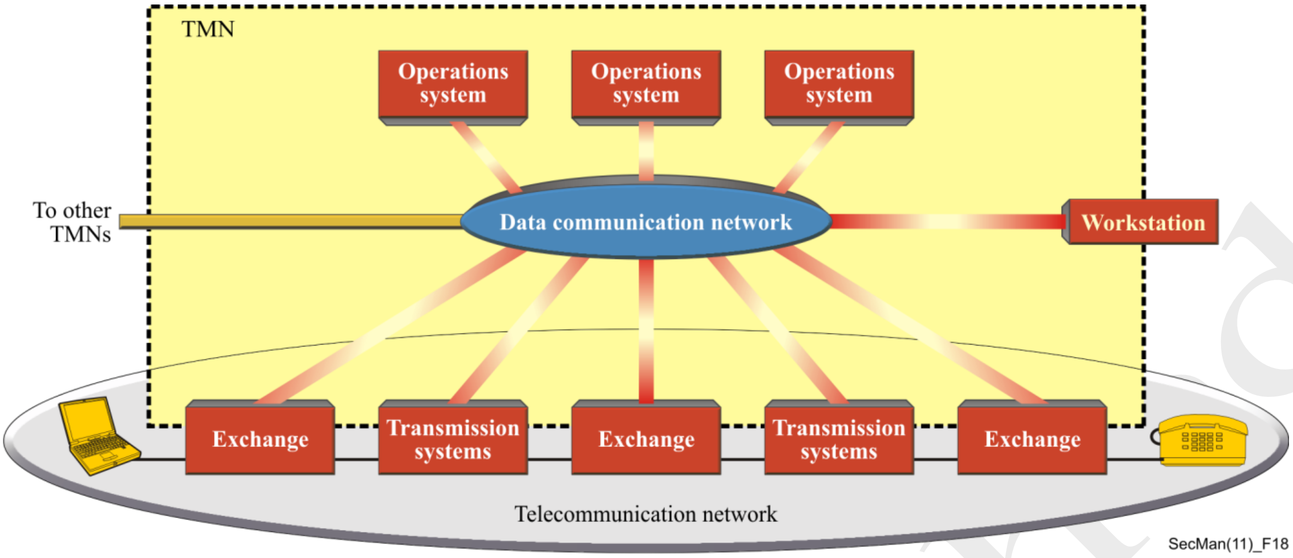
9.1 The telecommunications management network (TMN)

The TMN is separate and isolated from the public network infrastructure so that any disruptions due to security threats in the end-user plane of the public network do not spread to the TMN. As a result of this separation, it is relatively easy to secure the management network traffic because access to this plane is restricted to authorized network administrators and traffic is restricted to valid management activities. With the introduction of next generation networks, traffic for an end-user application may sometimes be combined with management traffic. While this approach minimizes costs by requiring only a single integrated network infrastructure, it introduces many new security challenges. Threats in the end-user plane now become threats to the management and control planes as the management plane now becomes accessible to a multitude of end-users, introducing the possibility of many additional types of malicious activity which must be countered.

9.2 Network management architecture

The architecture for defining the network management of a telecommunications network is defined in Recommendation ITU-T M.3010. The relationship of a TMN to a telecommunication network is shown in Figure 32. The management network architecture defines interfaces that determine the exchanges required to perform the operations, administration, maintenance, and provisioning functions.

Pre-published



NOTE – The TMN boundary represented by the dotted line may extend to and manage customer/user services and equipment.

Figure 32 – Relationship of a TMN to a telecommunication network

An overview and framework that identifies security threats to a TMN is provided in Recommendation ITU-T M.3016.0. Within the ITU-T M.3016-series Recommendations, ITU-T M.3016.1 defines detailed requirements, ITU-T M.3016.2 outlines security services, and ITU-T M.3016.3 defines mechanisms that can counter the threats within the context of the TMN functional architecture defined in Recommendation ITU-T M.3010. Because not all requirements need to be supported by all organizations, Recommendation ITU-T M.3016.4 provides a pro-forma for creating profiles based on individual security requirements, services and mechanisms. This allows the development of profiles that conform to an organization's unique security policy.

There are two facets to consider when discussing network security management. One relates to the management plane for user end-to-end activity (e.g., VoIP services) where the administration of users must be performed in a secure manner. This is referred to as *security of management information* exchanged over the network to support an end-to-end application. The second facet is *management of security information*, which applies irrespective of the application. For example, trouble-reporting activity between two service providers must be conducted securely. This may require the exchanges to be encrypted, in which case there must be provision for management of the encryption keys.

Several Recommendations that address security management functions of the ITU-T X.805 architecture are available for the three layers of the management plane (please see Figure 1). In addition, as discussed in the subsections below, other Recommendations define generic or common services such as the reporting of alarms when there is a security violation, audit functions, and information models that define levels of protection for different targets.

9.3 Securing the infrastructure elements of a network

End-to-end connectivity may be considered in terms of access networks and core networks. Different technologies may be used in these networks. Recommendations have been developed to address both access and core networks. The Broadband Passive Optical Network is used here as an example. Administering the user privileges for such an access network is defined using unified modelling methodology defined in Recommendation ITU-T Q.834.3. Management exchange using Common Object Request Broker Architecture (CORBA) is specified in Recommendation ITU-T Q.834.4. The interface described in these Recommendations is applied between the element management system and the network management system. The former is used to manage individual network elements and thus is aware of the internal details of the hardware and software architectures of the elements from one or more suppliers, whereas the latter performs the activities at the end-to-end network level and spans multiple supplier management systems. Figure 33 shows the various objects

Pre-published

used for creating, deleting, assigning, and using access control information for users of the element management system. The user permission list contains the list of management activities that are permitted for each authorized user. The access control manager verifies the user ID and password of the user of the management activity and grants access according to the functionality allowed in the permission list.

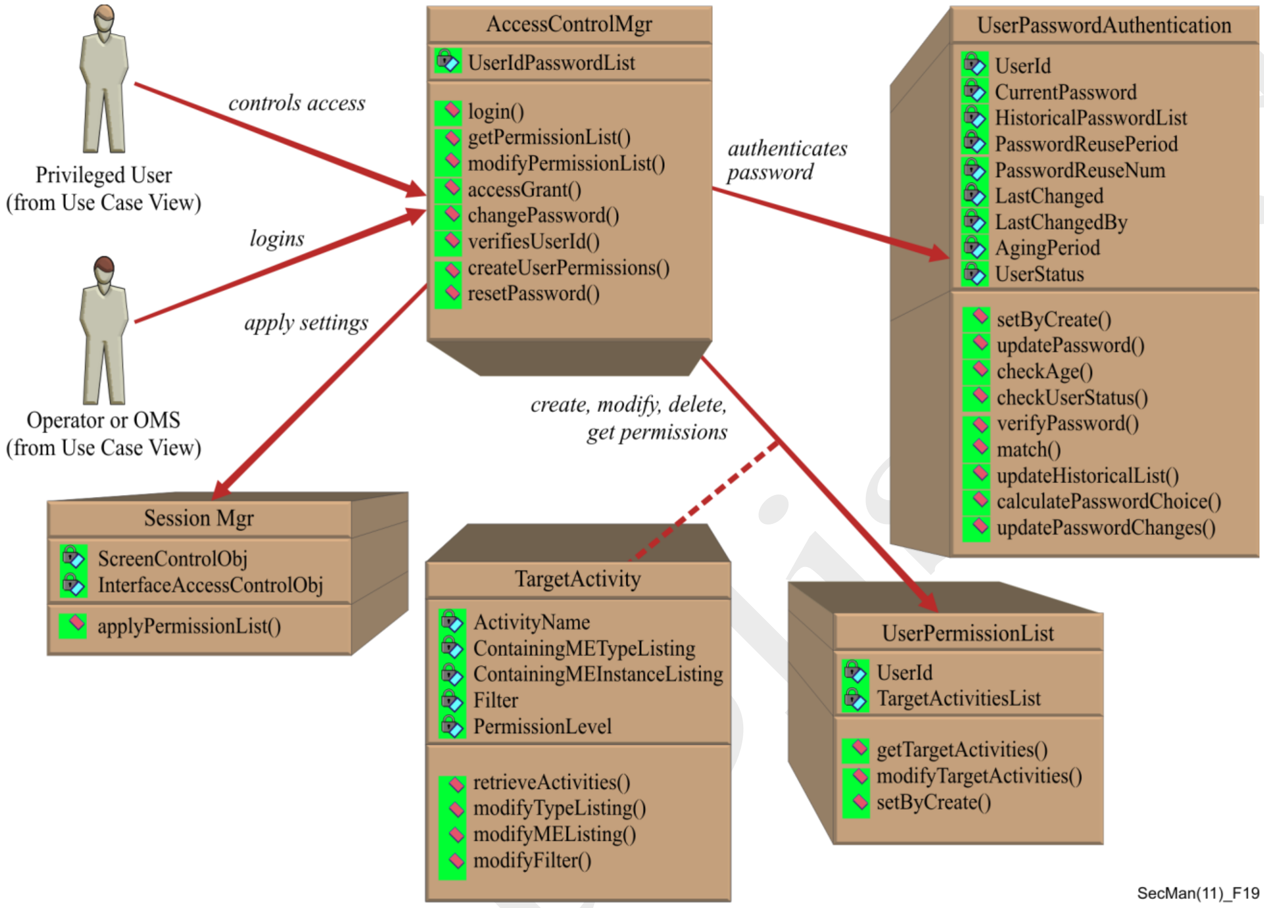


Figure 33 – Administering user privileges in ITU-T Q.834.3

9.4 Securing monitoring and control activities

Two aspects of security are relevant at the intersection between the management plane and the services layer. One aspect is ensuring that appropriate security measures are available for services provided in the network. For example, ensuring that only valid users are allowed to perform the operations associated with provisioning a service. The second aspect is defining which administrative and management exchanges are valid in order to help to detect security violations.

Recommendation ITU-T M.3208.2 addresses the first aspect, management activity of a service. This connection management service allows a subscriber to create/activate, modify and delete the leased circuits within the limits of the pre-provisioned resources. Because the user provisions the end-to-end connectivity, it is necessary to ensure that only authorized users are allowed to perform these operations. The ITU-T X.805 security dimensions associated with this service are: peer entity authentication; data integrity control (to prevent unauthorized modification of data in transit); and access control (to ensure a subscriber does not gain access maliciously or accidentally to another subscriber's data).

Recommendation ITU-T M.3210.1, which defines the administrative activities associated with the management plane for wireless services, is an example of a standard that addresses the second aspect. In a wireless network, as the users roam from the home network to the visited network, they may traverse different administrative domains. The services defined in ITU-T M.3210.1 describe how the fraud management domain

Pre-published

in the home location collects appropriate information about a subscriber who is registered on the visited network. Scenarios a) and b) in Figure 34 show initiation of the fraud monitoring activity, by either the home network or the visited network. The fraud detection system in the home network requests information on the activities when a subscriber registers with a visited network and remains active until the subscriber deregisters from the network. Profiles may then be developed related to usage based on analysis of call records, either at the service level, or for a subscriber. The fraud detection system can analyze and generate appropriate alarms when fraudulent behaviour is detected.

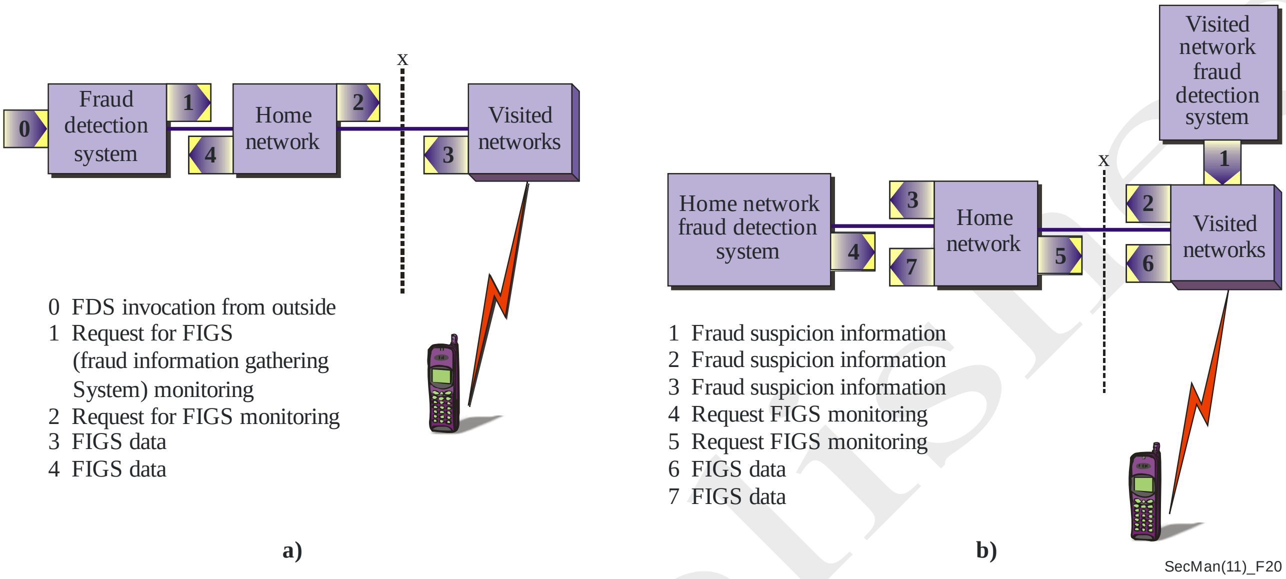

Fraud detection system
Home network
Visited networks
0
1
2
3
4
x
0 FDS invocation from outside
1 Request for FIGS (fraud information gathering System) monitoring
2 Request for FIGS monitoring
3 FIGS data
4 FIGS data
a)
Visited network fraud detection system
Home network fraud detection system
Home network
Visited networks
1
2
3
4
5
6
7
x
1 Fraud suspicion information
2 Fraud suspicion information
3 Fraud suspicion information
4 Request FIGS monitoring
5 Request FIGS monitoring
6 FIGS data
7 FIGS data
b)
SecMan(11)_F20

Figure 34 – Fraud Management for Wireless Services

Recommendation ITU-T X.1157 provides technical capabilities required to support fraud detection and response with high assurance level requirements. Fraud detection and response services support the detection, analytics, and management of fraud across users, accounts, products, processes and channels. It monitors user activities and behaviours and collects event data in near real time to analyze them immediately. To detect more fraud, the fraud detection system needs to integrate the data across use channels to evaluate the risk. The fraud detection system also requires automatic triggering of fraud alerts for incident response. The suspect transactions should be routed to a fraud investigation team and queued for manual or automated additional screening. Figure 35 shows the fraud detection and response capabilities that the fraud detection and response system should provide.

Pre-published

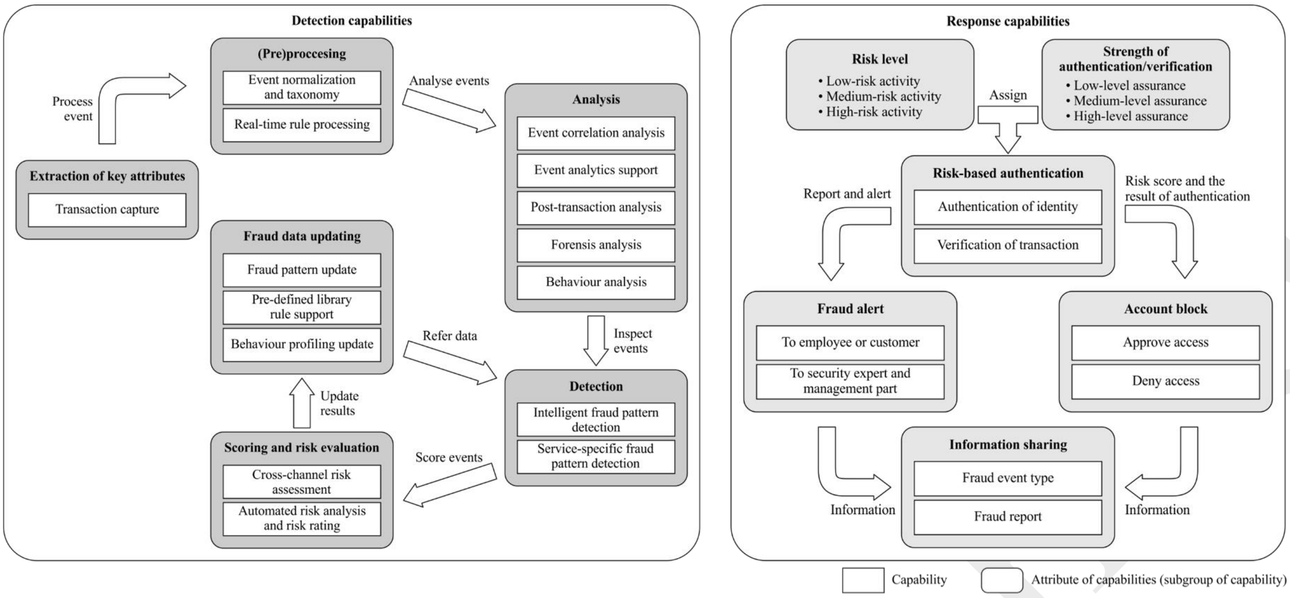

Detection capabilities
Process event
(Pre)proccesing
Event normalization and taxonomy
Real-time rule processing
Analyse events
Analysis
Event correlation analysis
Event analytics support
Post-transaction analysis
Forensis analysis
Behaviour analysis
Extraction of key attributes
Transaction capture
Fraud data updating
Fraud pattern update
Pre-defined library rule support
Behaviour profiling update
Refer data
Inspect events
Detection
Intelligent fraud pattern detection
Service-specific fraud pattern detection
Update results
Scoring and risk evaluation
Cross-channel risk assessment
Automated risk analysis and risk rating
Score events
Response capabilities
Risk level
• Low-risk activity
• Medium-risk activity
• High-risk activity
Assign
Strength of authentication/verification
• Low-level assurance
• Medium-level assurance
• High-level assurance
Report and alert
Risk-based authentication
Authentication of identity
Verification of transaction
Risk score and the result of authentication
Fraud alert
To employee or customer
To security expert and management part
Account block
Approve access
Deny access
Information
Information sharing
Fraud event type
Fraud report
Information
Capability
Attribute of capabilities (subgroup of capability)

Figure 35 – Fraud detection and response capabilities

The fraud detection system is composed of several components that process, store, and transfer data for detecting abnormal activity, described in Figure 36with the operations between the components. The examples of E-finance services, E-healthcare services, and enterprise remote access services are included in Appendix in the Recommendation.

Pre-published

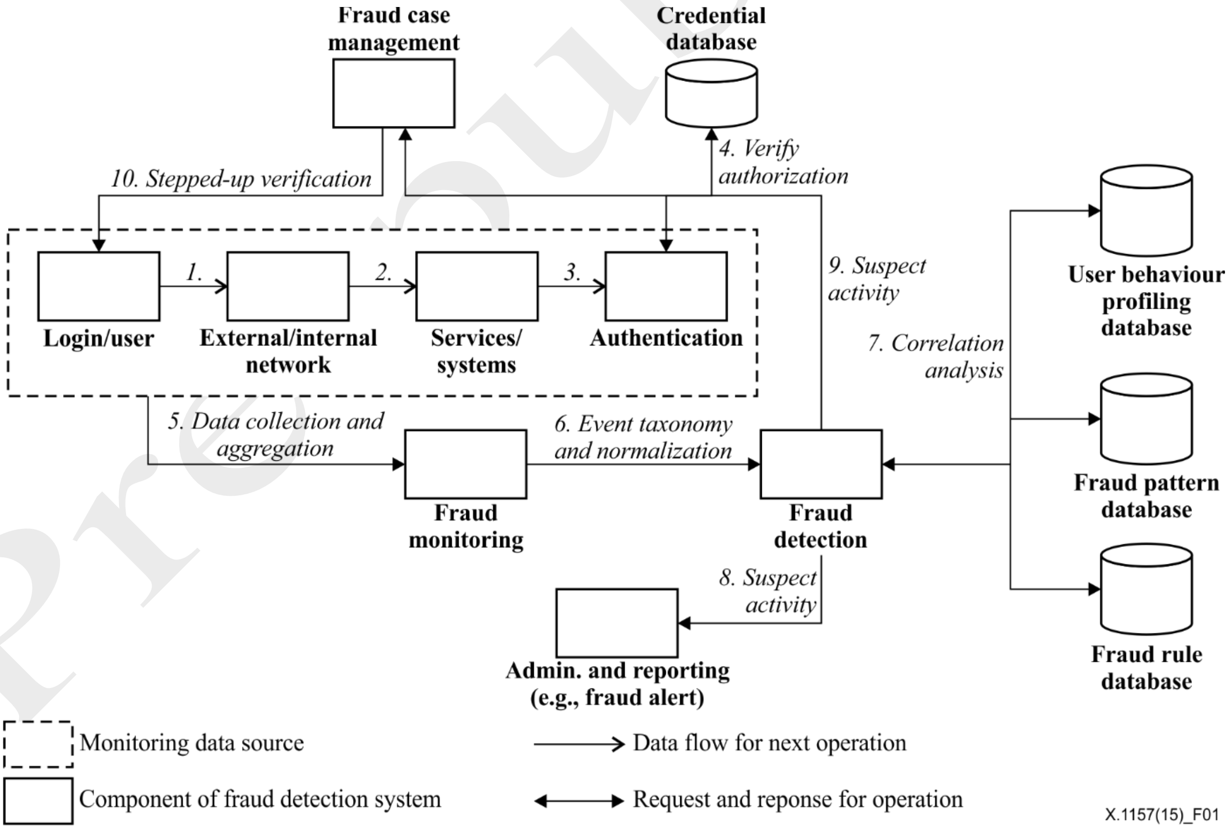

Fraud case management
Credential database
10. Stepped-up verification
4. Verify authorization
1.
2.
3.
Login/user
External/internal network
Services/ systems
Authentication
9. Suspect activity
7. Correlation analysis
User behaviour profiling database
5. Data collection and aggregation
6. Event taxonomy and normalization
Fraud monitoring
Fraud detection
Fraud pattern database
8. Suspect activity
Admin. and reporting (e.g., fraud alert)
Fraud rule database
Monitoring data source
Data flow for next operation
Component of fraud detection system
Request and reponse for operation
X.1157(15)_F01

Figure 36 – Operations and components of a fraud detection system

9.5 Securing network operation activities and management applications

The intersection of the management plane and the application layer in ITU-T X.805 corresponds to securing end-user network-based applications. This includes applications such as messaging and directory. Another class of applications where management activities are to be secured is that of the management applications themselves. This is best explained using examples. The end user for these applications is the service provider's management (operations) personnel. Consider the case where one service provider uses connection services from another provider in order to offer an end-to-end connectivity service. Depending on the regulatory or market environment, some service providers may offer access services: others, referred to as *inter-exchange carriers*, may offer long-distance connectivity. The inter-exchange carriers lease access services from the local provider for end-to-end connectivity across geographically-distributed locations. When a loss of service is encountered, an application called *trouble report administration* is used to report the problem. The user of these systems, as well as the application itself, requires authorization to report problems. Authorized systems and users should perform necessary actions for retrieving the status of the reported problem(s). Figure 37 illustrates the interactions that must be carried out in a secure manner. Access privileges are administered to prevent unauthorized access to trouble reports. A service provider is permitted to report troubles only on the services they lease and not on services leased by a different provider.

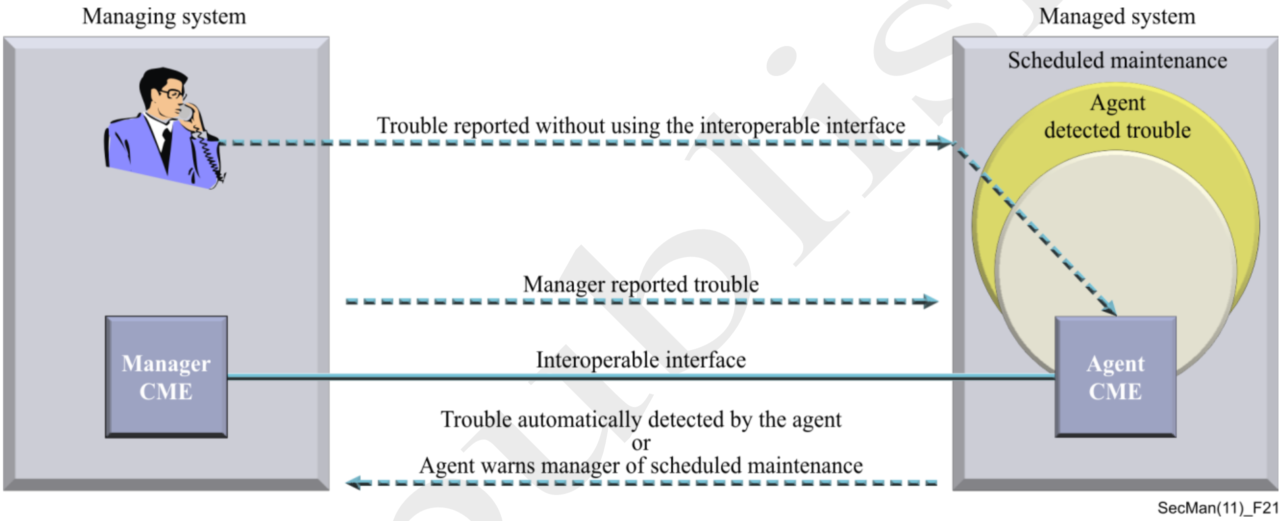


Figure 37 – Trouble management report creation

Recommendation ITU-T X.790, defines this management application and uses mechanisms such as access control lists and two-way authentication to secure the activities.

9.6 Protection against electromagnetic threats

Another important aspect of network infrastructure protection relates to protection of the telecommunication infrastructure against damage, malfunction and leakage of information due to electromagnetic disturbances and influences. In particular, it is important to ensure that the functionality of telecommunication facilities are not compromised by interference related to electromagnetic fields or by interference from other electrical or communications systems. The potential for electromagnetic disruption is particularly relevant given the convergence of telecommunication and IT equipment. It is also a major threat to the efficient and secure operation of home networks.

The risk of leakage of information due to electromagnetic emanation (e.g. from keyboards, display units and unshielded cabling) has long been recognized but there is now increasing focus on the need to protect against electromagnetic interference (both unintentional and deliberate) and electromagnetic attacks. The need for such protection is addressed in Recommendation ITU-T X.1051.

A number of specific Recommendations that address electromagnetic security have been developed by Study Group 5. Recommendation ITU-T K.87, *Guide for the application of electromagnetic security requirements - Overview*, outlines electromagnetic security risks of telecommunication equipment and illustrates how to assess and prevent those risks, in order to manage ISMS in accordance with Recommendation ITU-T X.1051. Recommendation ITU-T K.81, *High-power electromagnetic immunity guide for telecommunication systems* presents guidance on establishing the threat level presented by an intentional high-power electromagnetic attack and the physical security measures that may be used to minimize this threat and also provides information on the vulnerability of equipment. Recommendation ITU-T K.84, *Test methods and guide against information leaks through unintentional electromagnetic emissions* describes threats from information leakage due to unintentional electromagnetic emanations and specifies two approaches to mitigation as well as presenting leakage test methods for conducted and radiated emission.

9.7 Common security management services

There are a number of common services that are considered to be ITU-T X.805 management plane activities. These apply particularly where the *Common Management Information Protocol (CMIP)* (Recommendation ITU-T X.711) is used. A brief description of some of the services included in these recommendations is provided below.

9.7.1 Security alarm reporting function

Alarm reporting is a key function in management interfaces. When a failure is detected, either as a result of operational issues (e.g., a failure of the circuit pack or a violation of the security policy) an alarm is reported to the managing system. The alarm reports include a number of parameters so that the managing system is able to determine the cause of the failure and take corrective action. The parameters for any event include a mandatory field called *event type* and a set of other fields referred to as *event information*. The latter consists of information such as the severity of the alarm, probable causes of the alarm and the detector of the security violation. The alarm causes are associated with event types as shown in Table 7.

These causes are explained further in Recommendation ITU-T X.736.

9.7.2 Security audit trail function

A security audit trail is used to record security-related events and, in particular, security violations. Security-related events can include connections, disconnections, security mechanism utilizations, management operations and usage accounting. The *Security audit trail function* is defined in Recommendation ITU-T X.740.

9.7.3 Access control for managed entities

A very detailed definition of the model associated with assigning access control to various managed entities is described in Recommendation ITU-T X.741. The requirements satisfied by this Recommendation include: protecting management information from unauthorized creation, deletion and modification; ensuring operations are consistent with the access rights for the initiators of the operations; and preventing the transmission of management information to unauthorized recipients. Various levels of access control are defined to meet these requirements. For management operations, access restrictions can be applied at multiple levels. An access control policy may be based on one or more of the schemes defined (e.g., access control lists; capability-based, label-based and context-based access control). In the ITU-T X.741 model, a decision to permit or deny access is based on the access control policy and the access control information (ACI). ACI includes, for example, rules, the identity of the initiator, identities of the targets to which access is requested, and information pertaining to the authentication of the initiator.

Pre-published

Event type	Security alarm causes
integrity violation	duplicate information information missing information modification detected information out of sequence unexpected information
operational violation	denial of service out of service procedural error unspecified reason
physical violation	cable tampering intrusion detection unspecified reason
security service or mechanism violation	authentication failure breach of confidentiality non-repudiation failure unauthorized access attempt unspecified reason
time domain violation	delayed information key expired out of hours activity

9.7.4 CORBA-based security services

While many of the ITU-T X.700 series Recommendations assume the use of the CMIP as the management interface protocol, there have been other trends that are now reflected in these Recommendations, These include the use of the Common Object Request Broker Architecture (CORBA)-based protocol, services and object models for the management interfaces. Of particular note are Recommendations ITU-T X.780, ITU-T X.780.1, ITU-T X.780.2, and ITU-T X.781. In addition, Recommendation ITU-T Q.816 defines a framework for using these services in the context of management interfaces. To support the security requirements for these interfaces, ITU-T Q.816 refers to the object management group (OMG) specification of common services for security. Recommendations ITU-T Q.816.1 and ITU-T Q.816.2 define extensions to ITU-T Q.816 to support coarse-grained interfaces and service-oriented interfaces respectively.

Pre-published

10. Some specific approaches to network security

Pre-published

10 Some specific approaches to network security

In this section, approaches to protect various types of network are reviewed. The section begins with a look at the security requirements for Next Generation Networks. This is followed by a review of mobile communications networks which are in transition from mobility based on a single technology (such as CDMA or GSM) to mobility across heterogeneous platforms using the Internet Protocol (IP). Next, security provisions for home networks and cable television are examined. Lastly, the challenges of security for ubiquitous sensor networks are presented.

10.1 Next Generation Network (NGN) security

A Next Generation Network (NGN) is a packet-based network that is able to provide telecommunication services to users and that is able to make use of multiple broadbands, quality of service (QoS)-enabled transport technologies. In addition, service-related functions are independent of the underlying transport-related technologies. An NGN enables unfettered user access to networks and to competing service providers and services. It supports generalised mobility which will allow consistent and ubiquitous provision of services to users. More details on the general characteristics of an NGN are provided in Recommendation ITU-T Y.2001.

10.1.1 NGN security objectives and requirements

Recognizing that security is one of the defining features of NGN, it is essential to put in place a set of standards that will guarantee, to the maximum degree possible, the security of the NGN. As NGNs evolve and new security vulnerabilities appear for which there is no known immediate automatic remedy, such vulnerabilities must be properly documented so as to enable the network administrators and end users to mitigate them.

Recommendation ITU-T Y.2701, which is based on the principles of Recommendation ITU-T X.805, specifies security requirements for protecting NGNs against security threats and covers some of the technical aspects of identity management.

The following elements must be protected in a multi-network environment:

- network and service provider infrastructure and its assets (e.g., NGN assets and resources such as network elements, systems, components, interfaces, and data and information), its resources, its communications (i.e., signalling, management and data/bearer traffic) and its services;
- NGN services and capabilities (e.g., voice, video, and data services); and
- end-user communication and information (e.g., private information).

The requirements must provide network-based security of end-user communications across multiple-network administrative domains as illustrated in Figure 38.

The requirements specified in ITU-T Y.2701 are regarded as a minimum set of requirements. An NGN provider may need to take additional measures beyond those specified.

Pre-published

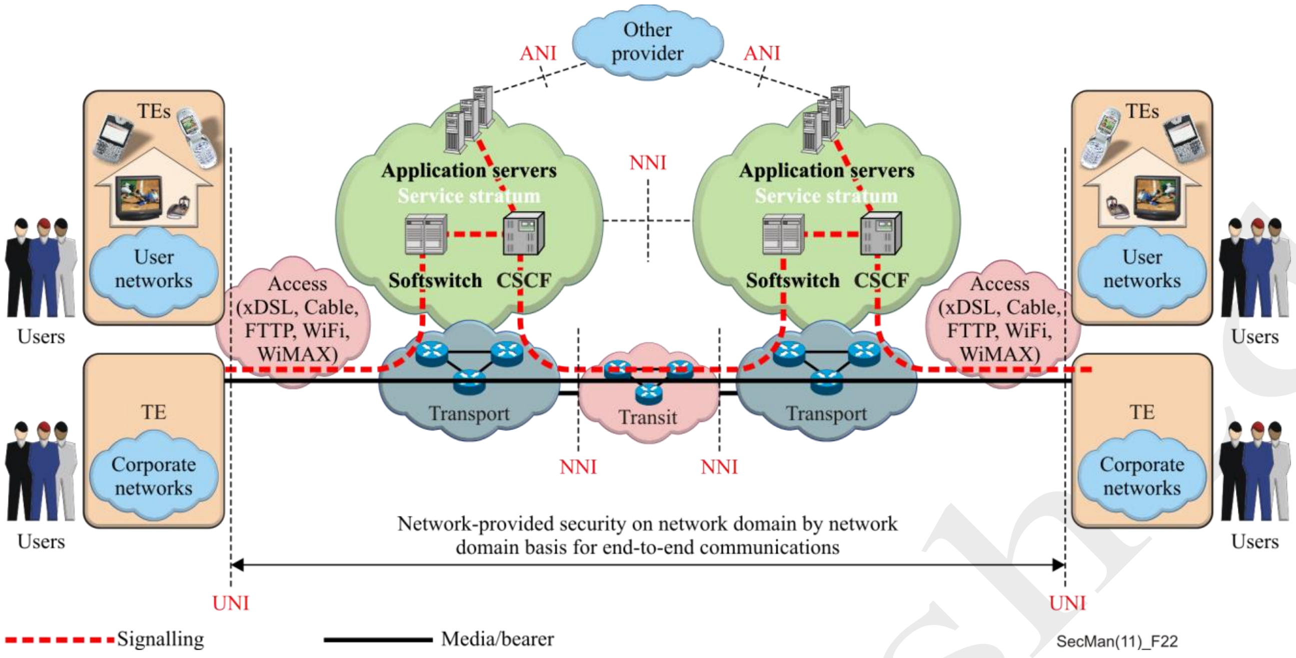


Figure 38 – Security of communications across multiple networks

In addition to the requirements specified in Recommendation ITU-T Y.2701, Recommendation ITU-T Y.2702, provides the detailed requirements for authentication and authorization in NGN Release 1, Recommendation ITU-T Y.2703, provides an application of authentication, authorization and accounting (AAA) for NGN release 1, and Recommendation ITU-T Y.2704, specifies the security mechanisms needed to address the requirements of Recommendation ITU-T Y.2701 and Recommendation ITU-T Y.2702.

A number of specific and generic application areas are also under study as part of the NGN work. For example, Recommendation ITU-T Y.2740, defines security requirements specific to the NGN support for mobile remote financial transactions. Recommendation ITU-T Y.2074 *Requirements for Internet of things devices and operation of Internet of things applications during disasters* also has security relevance.

One additional aspect of the NGN work that merits mention relates to security requirements for emergency telecommunications. A number of standards have been approved including: Recommendation ITU-T Y.1271, *Framework(s) on network requirements and capabilities to support emergency communications over evolving circuit-switched and packed-switched networks*; Recommendation ITU-T Y.2205, *Next Generation Networks - Emergency Telecommunications – Technical Considerations*; and Recommendation ITU-T Y.2705, *Minimum security requirements for interconnection of emergency telecommunications service.*

10.2 Mobile communications security

Mobile communications are evolving from mobility that is limited to a specific technology (e.g., GSM or CDMA) to mobility across heterogeneous networks (e.g., GSM, Wi-Fi, PSTN) with the usage of IP. Future networks will involve an integration of wireless and wireline networks providing a wide range of new services that could not be provided by a single existing network.

With the deployment of true Fixed Mobile Convergence (FMC), a mobile user can roam across heterogeneous networks such as GSM, Wireless LAN and Bluetooth. The security requirements for each type of access will have to be met in different ways but all security requirements must be met to protect users, networks and applications being accessed.

Pre-publishing

Pre-published

Security issues may be broadly categorized as:

- issues arising from the use of IP in mobile wireless; and
- issues arising from the use of multiple multi-technology networks.

Internet attacks and vulnerabilities pose a threat to wireless mobile networks that use IP as their transport protocol. In addition, new threats will arise from the very nature of the wireless networks themselves i.e., their mobility. The security mechanisms already developed for IP networks may not satisfy all security needs of IP-based wireless systems, and thus new or enhanced IP security measures may have to be developed. Also, security must be addressed not only for the radio interface but also for the complete end-to-end service and it must be flexible enough to provide various levels of security appropriate to the service/application being provided. The involvement of multiple networks increases the opportunity for threats such as illegal interception of user profiles, content (e.g., voice or data communication), and authentication information. Thus, deployment of mobile IP services and applications requires that additional security measures be implemented to protect the user, the operator and the service provider.

International Mobile Telecommunications-2000 (IMT-2000) is the global standard for third generation (3G) wireless communications. It is defined by a set of interdependent ITU Recommendations. IMT-2000 provides a framework for worldwide wireless access by linking the diverse systems of terrestrial and/or satellite based networks. It exploits the potential synergy between digital mobile telecommunications technologies and systems for fixed and mobile wireless access systems.

ITU activities on IMT-2000 comprise international standardization that addresses frequency spectrum and technical specifications for radio and network components, tariffs and billing, technical assistance and studies on regulatory and policy aspects.

The broad requirements for security in IMT-2000 networks are covered in Recommendations ITU-T Q.1701, ITU-T Q.1702 and ITU-T Q.1703.

In addition, the 3G specifications contained in the ITU-T Q.1741.x series of Recommendations (for 3GPP) and in the ITU-T Q.1742.x series (for 3GPP2) contain an evaluation of perceived threats and a list of security requirements to address these threats. These Recommendations also contain security objectives and principles for mobile communications, a defined security architecture, cryptographic algorithm requirements, lawful interception requirements, and lawful interception architecture and functions.

10.2.1 Secure mobile end-to-end data communications

Mobile terminals with data communications capability (e.g., Wi-Fi and GSM-enabled mobile phones, notebooks, tablets and e-readers and PDAs) are widely available and are used for an increasing number of applications. Due to the nature of the wireless network and the inherent vulnerabilities of wireless communication technologies, effective security is essential to protect both the applications and the data.

Security must be considered from the standpoint of the mobile network operator, the application service provider and the end user. Security between the mobile terminal and the application server is particularly important. To address mobile end-to-end communications, ITU-T has developed a complete set of security solutions, some of which are discussed below.

10.2.1.1 Framework for secure mobile end-to-end data communications

Recommendation ITU-T X.1121 describes two models of mobile end-to-end data communication between a mobile user and an application service provider (ASP): a General model; and a Gateway model as illustrated in Figure 39 and Figure 40. Service is provided to mobile users through the application server. In the Gateway model, the security gateway relays packets from the mobile terminal to the application server and transforms a mobile network-based communication protocol to an open network-based protocol, and vice versa. Figure

41 depicts the threats in the mobile end-to-end data communication network. Figure 42 shows the places where security features are required for each entity and the relationship between entities.

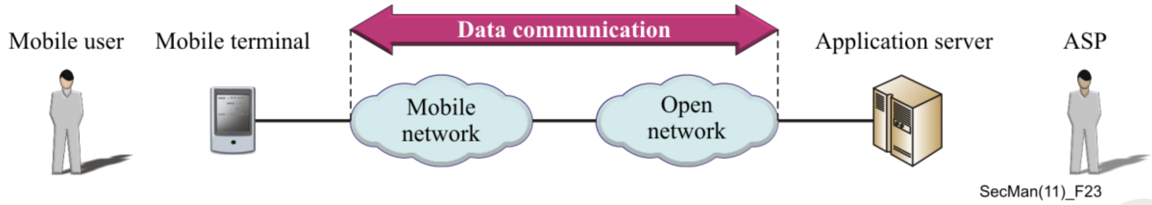


Figure 39 – General model of end-to-end data communication between a user and an ASP

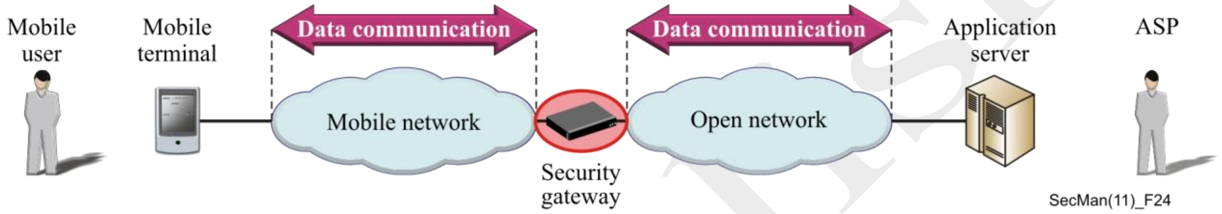


Figure 40 – Gateway model of mobile end-to-end data communication between a mobile user and an ASP

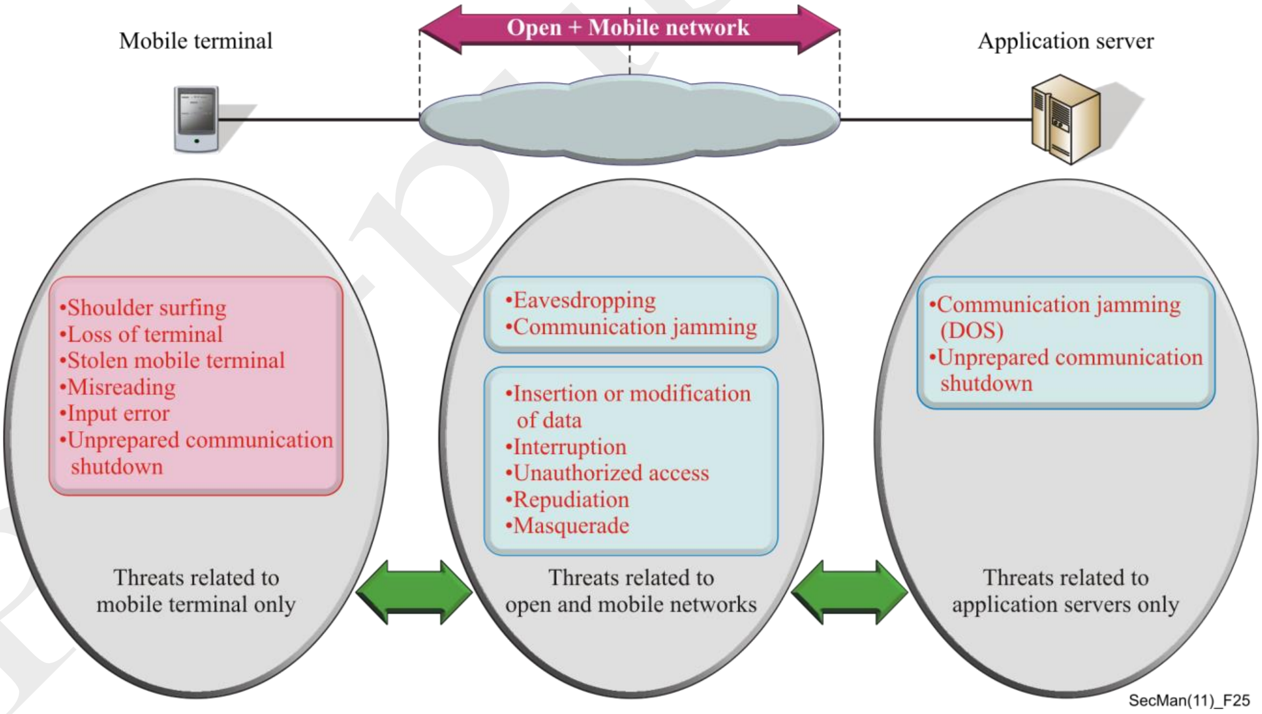

Mobile terminal
Open + Mobile network
Application server
•Shoulder surfing
•Loss of terminal
•Stolen mobile terminal
•Misreading
•Input error
•Unprepared communication shutdown
Threats related to mobile terminal only
•Eavesdropping
•Communication jamming
•Insertion or modification of data
•Interruption
•Unauthorized access
•Repudiation
•Masquerade
Threats related to open and mobile networks
•Communication jamming (DOS)
•Unprepared communication shutdown
Threats related to application servers only
SecMan(11)_F25

Figure 41 – Threats in the mobile end-to-end communications

Republished

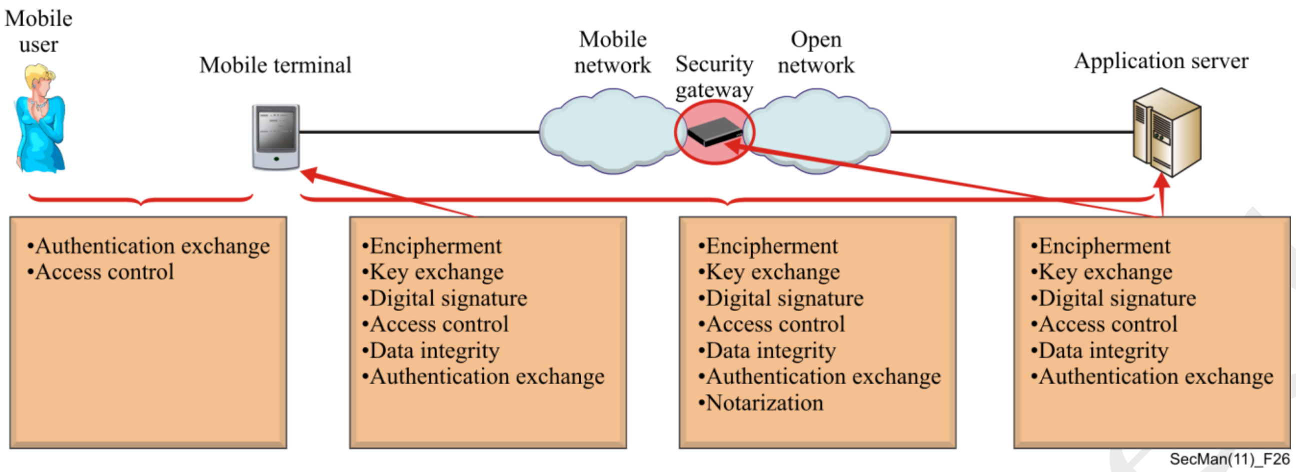


Figure 42 – Security function required for each entity and relation between entities

10.2.1.2 Public key infrastructure (PKI) for secure mobile end-to-end data communications

PKI is very useful for providing some of the security functions (e.g., confidentiality, digital signature, data integrity) needed for mobile end-to-end data communications but, because of the characteristics of mobile data communications, some adaptation is required. Guidance on implementing PKI in a mobile environment is provided in Recommendation ITU-T X.1122, which provides both a general PKI model and a gateway PKI model.

In the general model (shown in Figure 43) a Certification Authority (CA) serves the mobile user by issuing the user's certificate and managing the repository and certificate revocation list (CRL). A validation authority provides an online certificate validation service to the mobile user. The CA used by the ASP issues the ASP's certificate and manages the ASP's repository and CRL. The ASP's validation authority provides an online certificate validation service for ASP certificates.

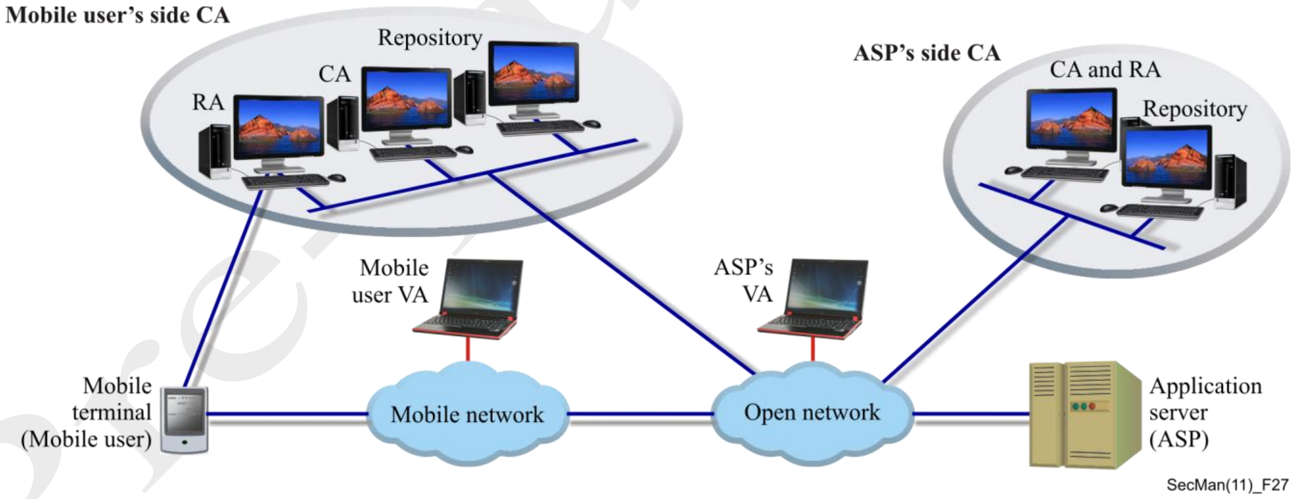


Figure 43 – General PKI model for mobile end-to-end data communications

There are two certificate issuance methods depending on the location at which the public/private key is generated: in one method, the cryptographic key pair is generated and fabricated during production of the mobile-terminal; in the other method, the cryptographic key pair is generated in the mobile terminal or in a tamper-free token attached to the mobile terminal. Figure 44 illustrates the procedure for a mobile terminal to acquire a certificate, where the cryptographic key pair is generated in the mobile terminal.

Pre-published

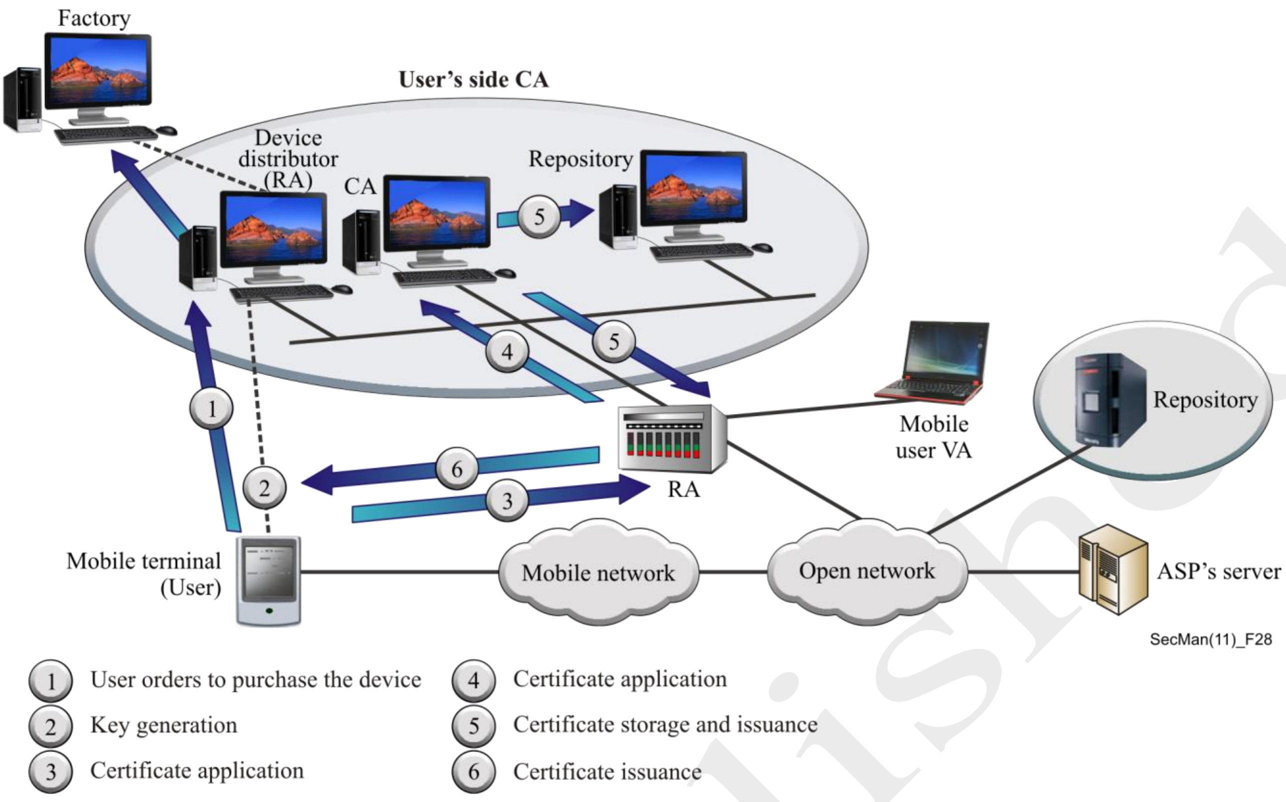


Figure 44 – Certificate issuance procedure for mobile terminal

The mobile terminal often has limited computational power and memory size. As a result, online certificate validation is preferable to off-line validation based on a CRL. Figure 45 depicts the on-line certificate validation procedure for a mobile terminal.

PKI for mobile end-to-end communication can be used either at the session layer, where it can support security services such as client authentication, server authentication, confidentiality and integrity service, or at the application where it can provide non-repudiation and confidentiality services.

10.2.1.3 Correlative reacting system for mobile data communication

The correlative reacting system has been devised to enable mobile terminals or devices and the network to cooperate to defend against security threats. Recommendation ITU-T X.1125 describes the generic architecture of a correlative reactive system in which a mobile network and its user terminals can cooperate interactively to combat various security threats for secure end-to-end data communications. Such threats include, for example, viruses, worms, Trojan-horses or other network threats against both the mobile network and its users.

This architecture provides operator networks with enhanced security capability through mobile station security updates, network access control and application service restrictions. This results in a mechanism that prevents viruses or worms from spreading rapidly through the operator network.

Pre-published

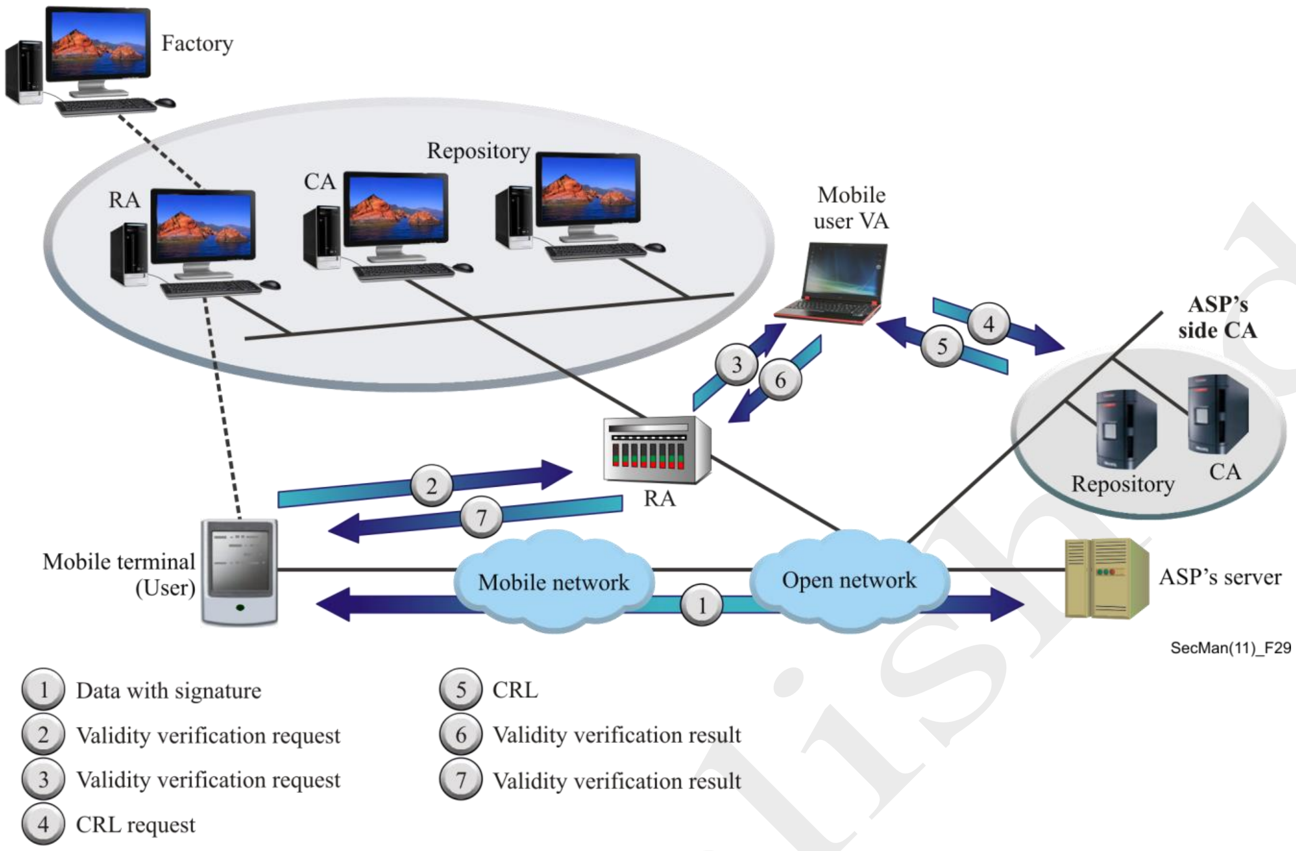


Figure 45 – Certificate validation for mobile end-to-end data communications

10.2.1.4 Secure mobile financial transactions

The general architecture for a security solution for mobile commerce and mobile banking in the context of NGN is specified in Recommendation ITU-T Y.2741 which describes the key participants, their roles, and the operational scenarios of the mobile commerce and mobile banking systems. It also provides examples of the implementation models of mobile commerce and mobile banking systems.

10.3 Home network security

Because a home network uses various wired or wireless transmission techniques, it is exposed to threats similar to those of any other network. ITU-T has developed a comprehensive set of solutions to protect home network services, some of which are discussed below.

10.3.1 Security framework for home network

Recommendation ITU-T X.1111 builds upon the threat model of Recommendation ITU-T X.1121 to establish a security framework for home networking. The characteristics of the home network may be summarized as follows:

- various transmission media can be used in the network;
- the network may comprise wired and/or wireless technologies;
- there are many possible environments to be considered from a security standpoint;
- terminals may be carried around by remote users; and
- the various types of home network device require different levels of security.

Pre-published

The general home network model for security, which is shown in Figure 46, may comprise many devices, such as PDAs, PCs, and TVs/VCRs. In this model, the home devices are classified as one of three types:

- Type A devices, such as remote controllers, PCs or PDAs, which have the capability of controlling a type B or type C device;
- Type B devices: bridges that connect type C devices (which have no communication interface) to the network. A type B device communicates with other devices in the network using a proprietary language or control mechanism; and
- Type C devices, such as security cameras and A/V devices, which provide a service to the rest of the devices.

Some devices combine type A and type C functions.

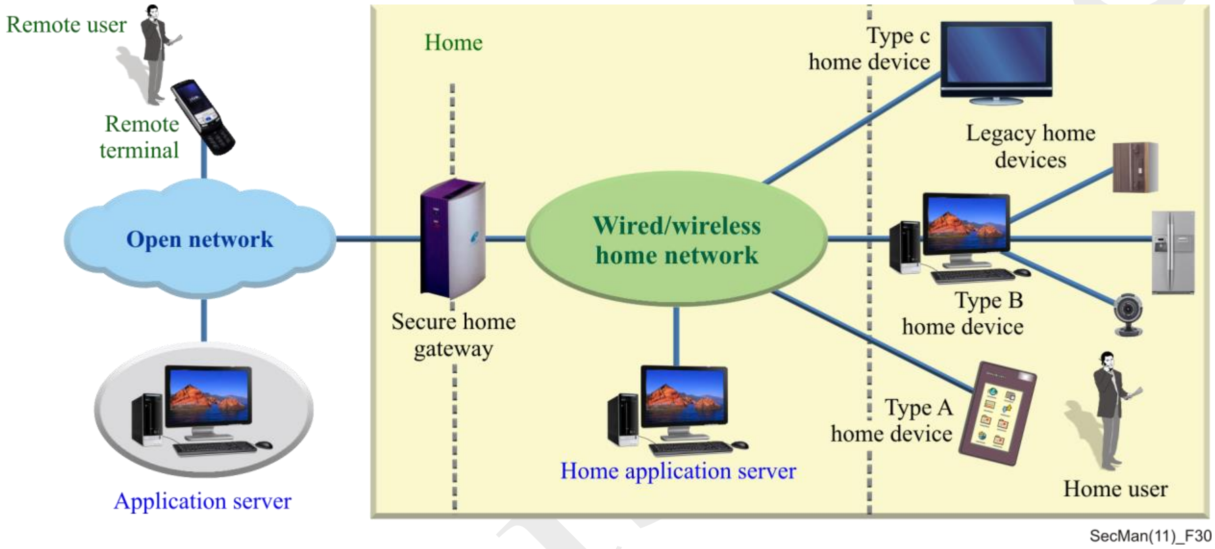


Figure 46 – General home network model for security

Recommendation ITU-T X.1111 describes security threats and security requirements from the standpoint of the home user and the remote user. In addition, it categorizes security technologies in terms of functions that satisfy the security requirements and by the location at which the security technologies must be applied.

10.3.2 Device certificates and authentication in home networks

There are two options for device certification in the home network: the external issuing model wherein all home device certificates are issued by an external CA; and the internal issuing model in which device certificates (including self-signed certificates and end-entity certificates) are issued by an internal CA in the home network. Usually, an internal CA is a secure home gateway with the capability of generating a key pair and issuing a certificate, i.e., the home gateway can issue both a CA certificate and home device certificates. The secure home gateway itself can have a device certificate which is issued by an external certification authority for use in external home services. This externally issued home gateway device certificate can be used for authentication between the home gateway and the network service provider.

Recommendation ITU-T X.1112 describes a framework for the internal model of device certificate issuance, management and usage for home networks. The model is illustrated in Figure 47.

Pre-Published

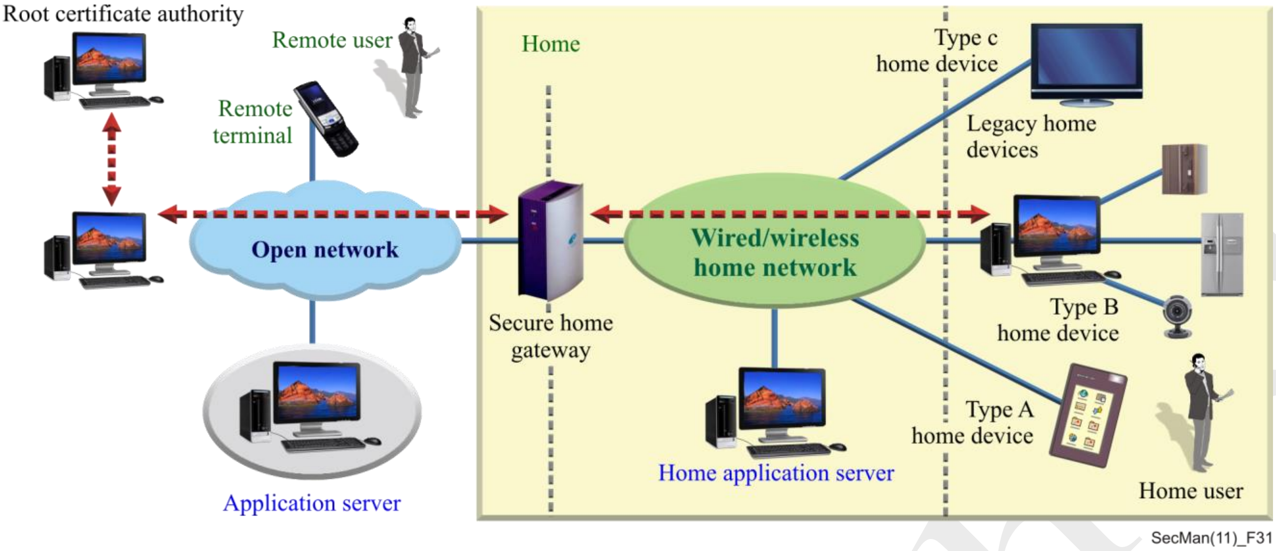


Figure 47 – Device authentication model for the secure home network

For device authentication, a unique identifier is needed for each device in the home network. Specifically, a device certificate will be required as a unique trust element when used in the home network.

Figure 48 shows four typical use cases of a device certificate: 1) between the remote terminal and the secure home gateway; 2) between the application server and the secure home gateway; 3) between home devices and the secure home gateway; and 4) among home devices.

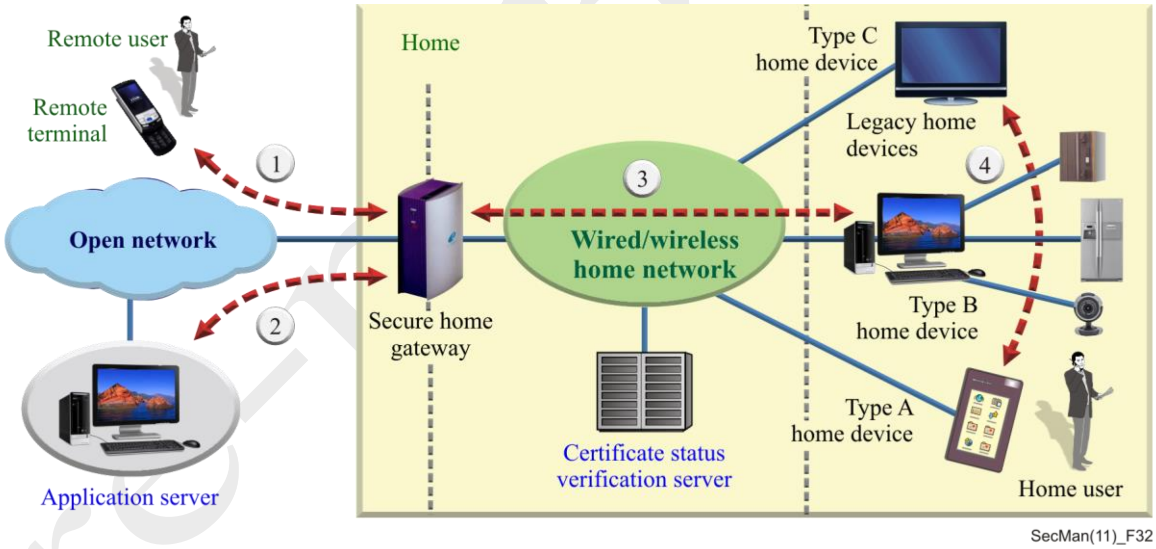


Figure 48 – Device authentication use case based on general home network model for security

For external Internet service from the home device to an external application server, the home device should be authenticated first with the secure home gateway using its own device certificate. The secure home gateway should then be authenticated with the external application server using the home gateway certificate issued by an external CA. These use cases can be applied to various application protocols for supporting secure home network services.

Pre-published

10.3.3 Human user authentication for home network services

Some environments demand authentication of the human user rather than a process or a device. Recommendation ITU-T X.1113 provides guidance on user authentication for the home network to enable use of various authentication techniques such as passwords, certificates and biometrics. It also defines the security assurance level and authentication model according authentication service scenarios. Figure 49 shows authentication service flows based on the general model of home network security defined in Recommendation ITU-T X.1111. In this example, a remote user tries to access entities within the home, while the home user tries to access entities inside and outside the home.

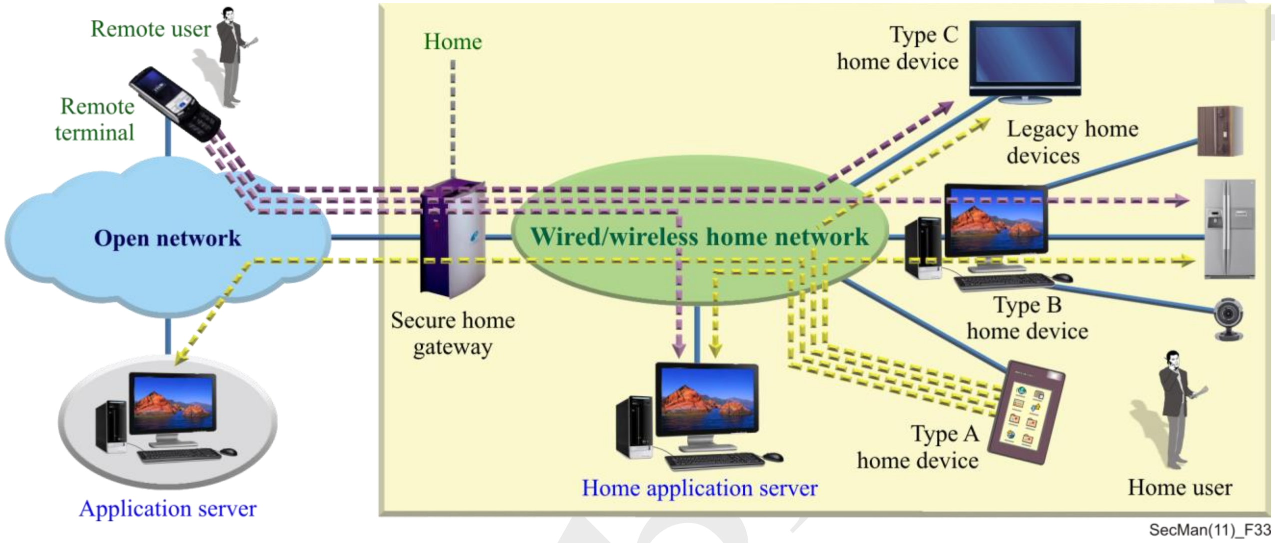


Figure 49 – Authentication service flows for the home network

10.4 IPCablecom security

The IPCablecom system enables cable television operators to provide IP-based real-time services (e.g., voice communications) over networks that have been enhanced to support cable modems.

10.4.1 IPCablecom Architecture

The IPCablecom architecture is defined in Recommendation ITU-T J.160. IPCablecom components are illustrated in Figure 50. The IPCablecom architecture contains both trusted and untrusted network elements. Trusted network elements are typically located within a cable operator's managed backbone network. Untrusted network elements, such as the cable modem and media terminal adapter (MTA), are typically located outside the cable operator's facility within the subscriber's home.

Pre-published

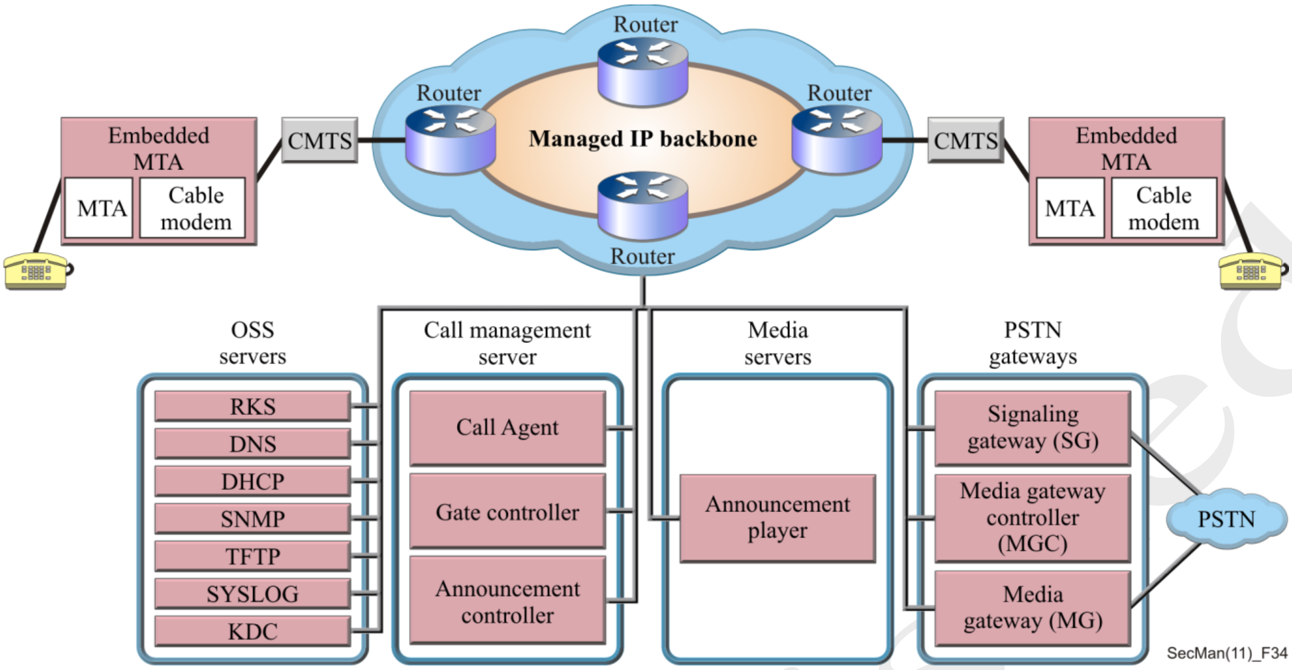


Figure 50 – IPCablecom component reference model

10.4.2 Security requirements for IPCablecom

Each of IPCablecom's protocol interfaces is subject to threats that could affect both the subscriber and the service provider. For example, the media stream path may traverse a large number of potentially unknown Internet service and backbone service providers. As a result, the media stream may be vulnerable to eavesdropping, resulting in a loss of communications privacy. Security design objectives identified in the IP Cablecom architecture are:

- to enable residential voice capabilities with the same or higher level of perceived privacy as the PSTN;
- to provide protection against attacks on the MTA; and
- to protect the cable operator from network disruption, denial-of-service, and theft-of-service attacks.

Design considerations must include confidentiality, authentication, integrity and access control.

Security requirements are specified in Recommendation ITU-T J.170. Threats to be addressed are summarized as follows:

- theft of service, which includes subscription fraud, non-payment for services, MTA clones; (e.g., where an MTA registered under a fraudulent account is cloned), impersonation of a network server and protocol manipulation;
- disclosure of bearer channel information, which includes: simple snooping, MTA clones (e.g., of a publicly-accessible MTA), protocol manipulation, off-line cryptanalysis, and service disruption;
- disclosure of signalling information;
- theft of MTA-based services; and
- illegally registering a leased MTA with a different service provider.

10.4.3 Security services and mechanisms in IPCablecom

Security in IPCablecom is implemented in the lower stack elements and mostly uses mechanisms defined by the IETF. The IPCablecom architecture addresses the threats by specifying, for each defined protocol interface,

Pre-published

the underlying security mechanisms (such as IPsec) that provide the protocol interface with the security services it requires.

The security services available through IPCablecom's core service layer are authentication, access control, integrity, confidentiality and non-repudiation. The security mechanisms include both the security protocol (e.g., IPsec, Real Time Protocol (RTP)-layer security, and SNMPv3 security) and the supporting key management protocol (e.g., IKE, PKINIT/Kerberos). Also, IPCablecom core security services include a mechanism for providing end-to-end encryption of RTP media streams, thus substantially reducing the threat to privacy.

10.5 IPCablecom2 security

IPCablecom2 is a cable industry initiative designed to support the convergence of voice, video, data and mobility technologies.

10.5.1 The IPCablecom2 architecture

IPCablecom2 is based on Release 6 of the IP multimedia subsystem (IMS) as defined by the 3rd generation partnership project (3GPP). The scope of 3GPP includes development of a SIP-based IP-communications architecture for mobile networks. The resulting architecture forms the basis of the IPCablecom2 architecture defined in Recommendation ITU-T J.360.

10.5.2 Security requirements for IPCablecom2

Design goals for the IPCablecom2 security architecture include:

- support for confidentiality, authentication, integrity, and access control mechanisms;
- protection of the network from denial of service, network disruption, theft-of-service attacks;
- protection of the user equipment (UE) (i.e., clients) from denial of service attacks, security vulnerabilities, unauthorized access from the network;
- support for end-user privacy through encryption and mechanisms that control access to subscriber data such as presence information;
- mechanisms for device, UE, and user authentication; secure provisioning, secure signalling, and secure software download; and
- ability to leverage and extend the architecture in furtherance of the previously-stated goals.

The general threats that apply to IPCablecom2 are:

Trust domain threats

A trust domain is a logical grouping of network elements that are trusted to communicate. Threats to trust domains apply to the interfaces connecting network elements within a domain, the interfaces between domains, and the interfaces between UEs and the service provider.

Theft of service

Theft of service can be achieved in many ways including, but not limited to: manipulation of the UE; protocol weakness exploitation; identity spoofing; UE cloning (i.e., the act of imitating a legitimate UE); and subscription fraud and non-payment of services.

Pre-published

Disruption and denial-of-service

This includes general denial-of-service attacks; flooding attacks (i.e., rendering a particular network element unavailable, usually by directing an excessive amount of network traffic at its interfaces); and attacks using zombies (i.e., compromised endpoint systems).

Signalling channel threats

Attacks against signalling threats include: compromise of confidentiality of signalling information; man-in-the-middle attacks resulting from the interception and possible modification of traffic passing between two communication parties; and denial of service attacks in the signalling channel range.

Bearer channel threats

Threats to the bearer channel relate to the media traffic transferred between communicating parties.

Protocol-specific security threats

A variety of threats exist against individual multimedia protocols.

10.5.3 Security services and mechanisms in IPCablecom2

IPCablecom2 makes extensive use of transport layer security and other mechanisms referenced in 3GPP IP Multimedia Subsystem (3GPP 23.002 v6.10.0, *Network Architecture*, December 2005). The following sections summarize the IPCablecom2 enhancements to the IMS security architecture.

10.5.3.1 User and UE authentication

The IPCablecom2 architecture supports the following authentication mechanisms:

- IP multimedia subsystem authentication and key agreement;
- session initiation protocol (SIP) digest authentication; and
- certificate bootstrapping.

The architecture accommodates UEs with multiple authentication credentials. For example, a UE may have a certificate for accessing services while on a cable network, and a universal integrated circuit card (UICC) for accessing services while on a cellular network.

A subscriber may have multiple credentials. A subscriber may have multiple UEs, with different capabilities related to those credentials. For example, a subscriber may have an MTA with a certificate for home use, and a UICC-based UE for travelling.

10.5.3.2 Signalling security

IPCablecom2 adds transport layer security (TLS) as an option for signalling security between the UE and the Proxy Call Session Control Function. The use of TLS (as defined by the IP Multimedia Subsystem (IMS)) is optional for signalling security.

10.6 Ubiquitous sensor network security

A sensor is simply a device that generates an electrical signal that represents a measurable physical property. A ubiquitous sensor network (USN) is a network that uses low cost, low power sensors to develop context

Pre-published

awareness in order to deliver sensed information and knowledge services to anyone, anywhere and at any time. A USN may cover a wide geographical area and may support a variety of applications. Figure 51 illustrates potential USN applications.

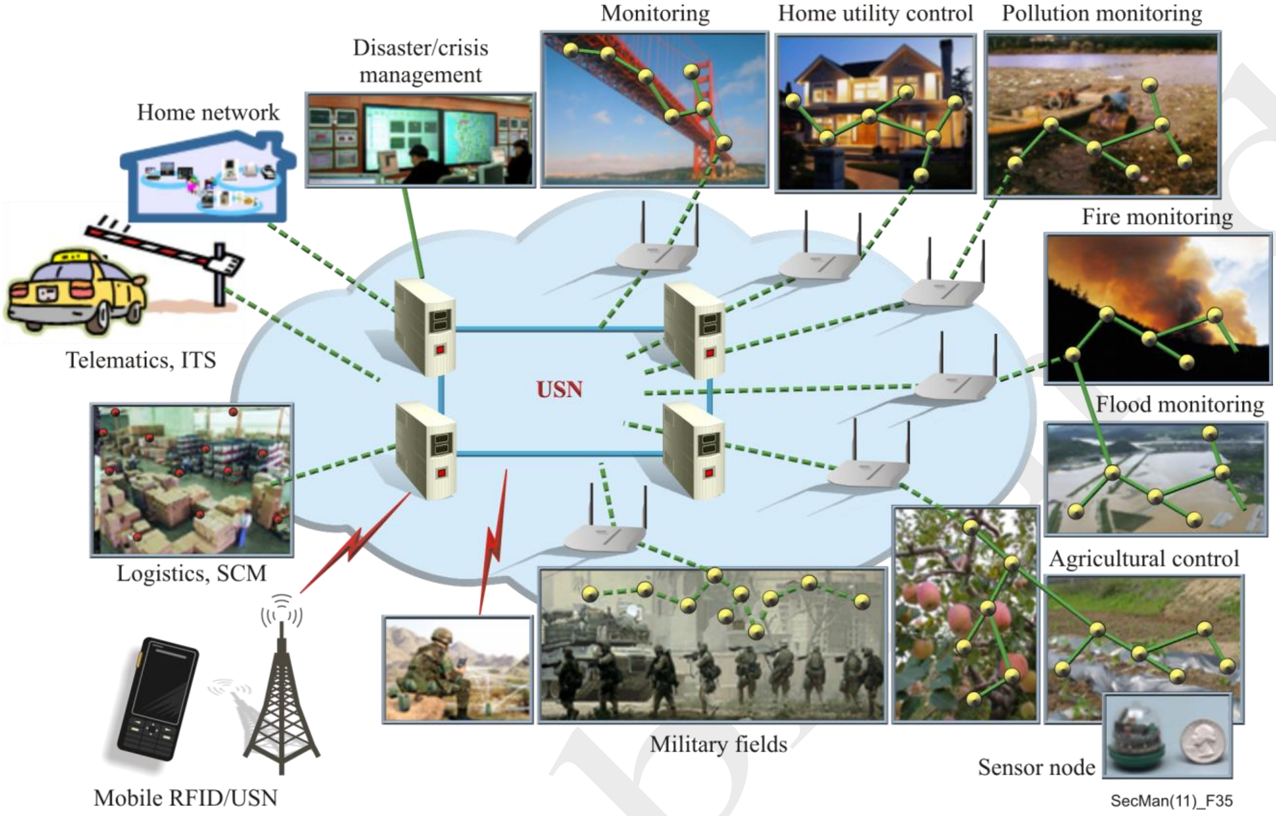


Figure 51 – Potential USN applications

Sensor networks are usually connected to end-user networks and, while the core transmission networks are likely to use the Internet and NGN technologies, a variety of underlying technologies (such as DSL, satellite, GPRS, CDMA, GSM, etc.) will be used.

Since information transfer in a USN faces many potential threats, effective security techniques are needed to counter those threats.

10.6.1 Security framework for ubiquitous sensor network

Recent advances in wireless-based communication technology and electronics have facilitated the implementation of the Ubiquitous Sensor Network (USN). Basically, a USN consists of three parts: a sensor network consisting of a large number of sensor nodes; a base station (also known as gateway) that interfaces between the sensor networks and an application server; and an application server that controls the sensor nodes or collects the sensed information from the sensor nodes.

Recommendation ITU-T X.1311 describes the security threats to, and security requirements of the USN. In addition, this draft Recommendation categorizes the security techniques that satisfy the security requirements and the points of application of the security techniques in the USN security model.

The overall structure of a USN is shown in Figure 52. The sensor networking domain may include both wireless and wire-line sensor networks and many kinds of wired and wireless networking technologies may be used according to the service characteristics and requirements.

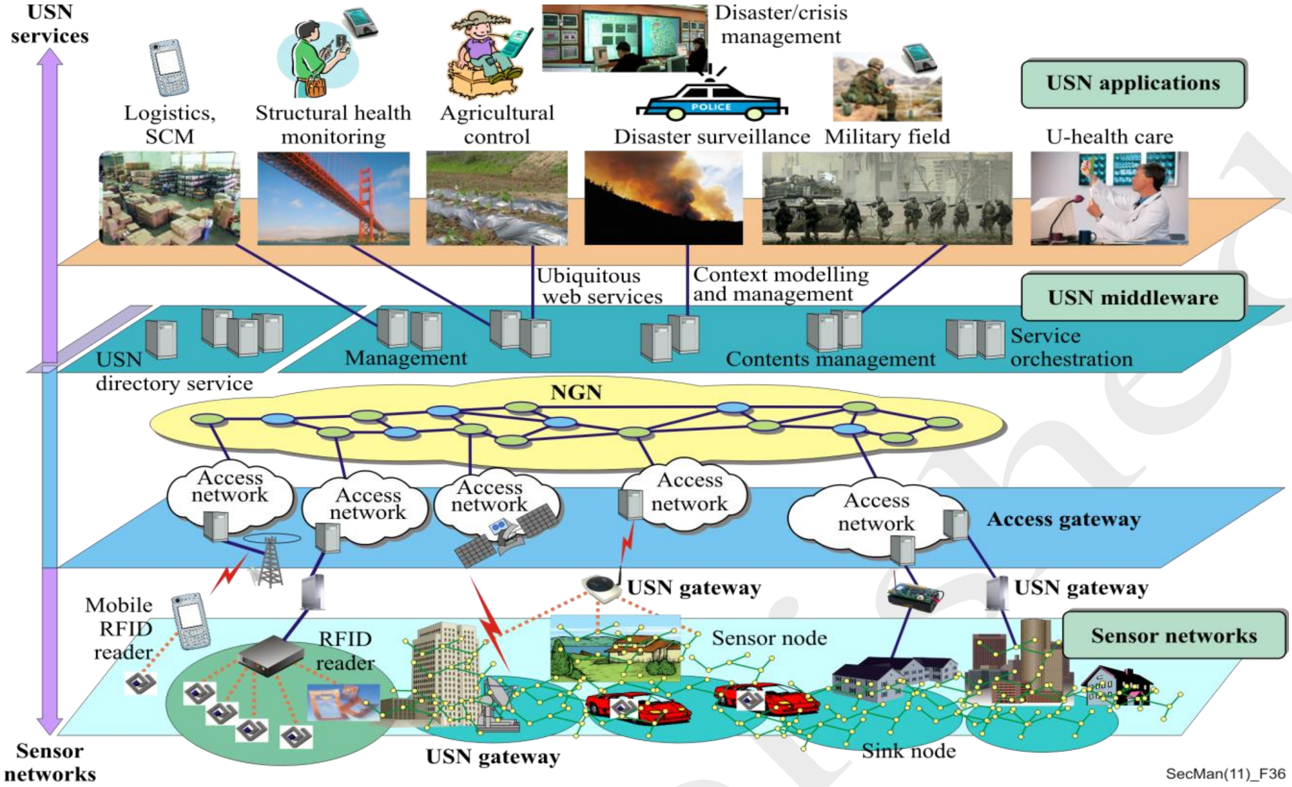


Figure 52 – Overall structure of a USN

The threats to a USN comprise those in the IP network and those in the SN. There are two types of threats to the SN: general threats and routing-related threats. Threats to the IP network, and routing-related threats to message exchange in the SN, are identified in Recs. ITU-T X.800 and ITU-T X.805 (please see Chapter 4 and Figure 1). In addition, there are sensor node-specific threats such as sensor node compromise, eavesdropping, privacy of sensed data, denial of service attack, and malicious use of the commodity network. Lastly, seven additional threats have been identified as follows:

- Spoofed, altered or replayed routing information
- Selective forwarding
- Sinkhole attack
- Sybil attacks
- Wormhole attacks
- HELLO flood attacks and
- Acknowledgment spoofing

The security model shown in Figure 53 illustrates a general framework of USN security based on the application area of USN, the overall structure of USN, and the USN network configuration. The model is based on ISO/IEC 15408-1, *Evaluation criteria for IT*, and is intended to help establish security concepts and relationships to USN security.

Pre-published

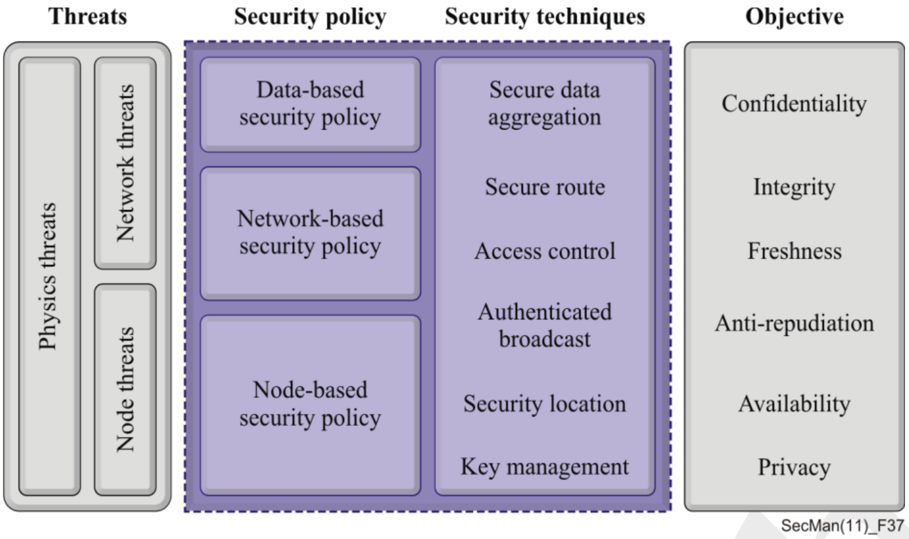


Figure 53 – Security model for USN

10.6.2 Ubiquitous sensor network (USN) middleware

USN middleware is an intermediate entity that provides the functions commonly required by different types of USN applications and services. USN middleware receives requests from USN applications, and delivers those requests to the appropriate sensor networks. Similarly, USN middleware receives sensed data or processed data from sensor networks and delivers them to appropriate USN applications. USN middleware can provide information processing functions such as query processing, context-aware processing, event processing, sensor network monitoring and the like. The service description and requirements for USN middleware are contained in Recommendation ITU-T F.744. Guidelines for middleware security are contained in Recommendation ITU-T X.1312.

USN middleware is located between the USN application and the sensor network in the USN service model. USN middleware security threats can be divided into three groups according to the target: device, data and network.

The system security threats are defined as:

- unauthorized USN middleware access;
- DoS and DDoS attacks against USN middleware;
- malicious or abnormal traffic transfer to USN middleware;
- misuse and abuse of the USN middleware system;
- careless mistakes; and cross-application breach of containment.

The security threats to data are:

- data leakage; and
- data forgery.

The security threats to middleware communication are:

- eavesdropping;
- interruption;
- hijacking; and
- jamming.

The security requirements for USN middleware must address each of these threats. Figure 54 illustrates the security functions of the USN middleware.

Pre-published

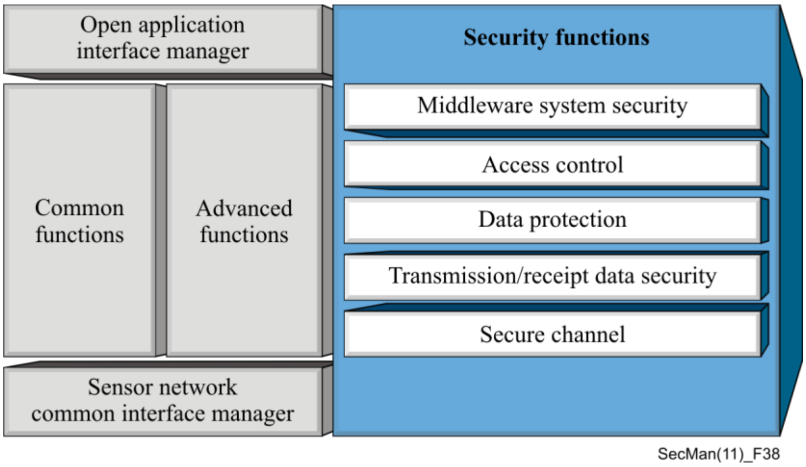
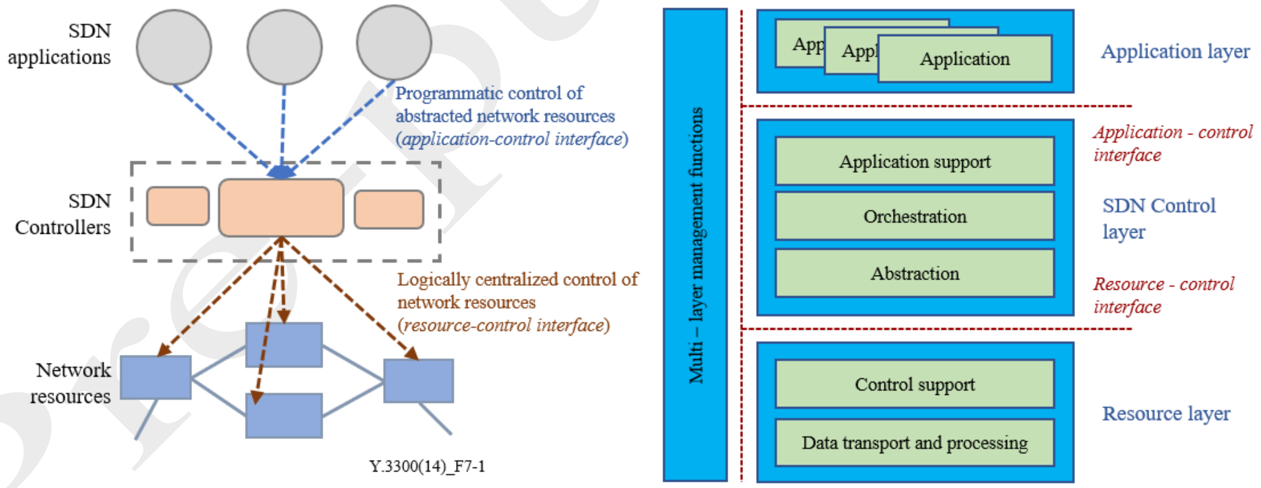

Open application interface manager
Common functions
Advanced functions
Sensor network common interface manager
Security functions
Middleware system security
Access control
Data protection
Transmission/receipt data security
Secure channel
SecMan(11)_F38

Figure 54 – Security functions for USN middleware

10.7 Software-defined networking security

10.7.1 Concepts

Software-defined networking (SDN) is a set of techniques that enables to directly program, orchestrate, control, and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner. SDN enables the administrators to configure network resources very quickly and to adjust network-wide traffic flow to meet changing needs dynamically. SDN controllers serve as a type of operating system for network. By separating the control plane from the network hardware and running the control plane instead as software, the controller facilitates automated network management, as well as integration and administration of applications and network services. The concepts and high-level architecture of SDN described in Recommendation ITU-T Y.3300, Framework of software-defined networking are shown in Figure 55(a) and (b).


SDN applications
Programmatic control of abstracted network resources (application-control interface)
SDN Controllers
Logically centralized control of network resources (resource-control interface)
Network resources
Y.3300(14)_F7-1
Multi – layer management functions
App
Appl
Application
Application layer
Application - control interface
Application support
Orchestration
Abstraction
SDN Control layer
Resource - control interface
Control support
Data transport and processing
Resource layer

(a) Concept of SDN

(b) High-level architecture of SDN

Figure 55 – Framework of SDN

Pre-published

10.7.2 SDN functional architecture

The functional architecture of SDN is provided in Recommendation ITU-T Y.3302, Functional architecture of software-defined networking, which is based on the high-level architecture of SDN.

- SDN application layer (SDN-AL): SDN-AL is composed of the application layer management support and orchestration (AL-MSO) functional component and multiple SDN application functional components [ITU-T Y.3302]. The AL-MSO interacts with the application layer management (ALM) functional component in multi-layer management function (MMF) via the multi-layer management functions application layer (MMFA) reference point in order to support management of SDN applications and to enable joint-operations of management in all SDN sub-layers. SDN applications interact with the SDN-CL via the application control interface (ACI) reference point with requests for the SDN-CL to automatically customize the behaviour and the properties of network resources. SDN applications use the abstracted view and status of the network resources which are provided by the SDN-CL by means of information and data models exposed through the ACI reference point. Depending on the SDN use cases (e.g. intra or inter data centers, mobile networks, access networks), different ACIs can optionally be defined. It is assumed that ACIs use open APIs.

– SDN control layer (SDN-CL): SDN-CL is composed of control layer management support and orchestration (CL-MSO), application support (CL-AS), control layer services (CL-CLS) and resource abstraction (CL-RA). The SDN-CL provides programmable means to control the behaviour of SDN resources (such as data transport and processing resources), according to SDN-AL requests and MMF policies. The SDN-CL operates on resources provided by the SDN resource layer (SDN-RL) and exposes an abstracted view of the network to the SDN-AL. The SDN-CL interacts with SDN-RL using a resource control interfaces (RCI) reference point, with a control layer management (CLM) functional component in MMF using the multi-layer management function control layer (MMFC) reference point. It also interacts with SDN-AL with ACI reference point. The CL-MSO may request the MMF to delegate some management functions. MMF provides functionalities for managing the functionalities of SDN-CL through the MMFC reference point.

– SDN resource layer (SDN-RL): SDN-RL is composed of resource layer management support (RL-MS), resource layer control support, resource layer data processing, and resource layer data transport. SDN-RL is where the physical or virtual network elements perform transport and/or processing of data packets according to SDN-CL decisions. The policy-provisioning information (including configuration information) that result as decisions made by the SDN-CL as well as the information about network resources are exchanged via the RCI reference point. Information exchanged through RCI include control information provided by SDN-CL to SDN-RL (e.g. for configuring a network resource or providing policies) as well as the information that pertains to the notifications sent by SDN-RL whenever a network resource change is detected (if such information is available). The RL-MS provides resource description, i.e. vendor, software version, and their status (e.g. CPU load, used RAM memory or storage). It may include a management agent that performs some local management operations if delegated by MMF. MMF provides functionalities for managing the functionalities of SDN-RL through the MMFR reference point.

Pre-published

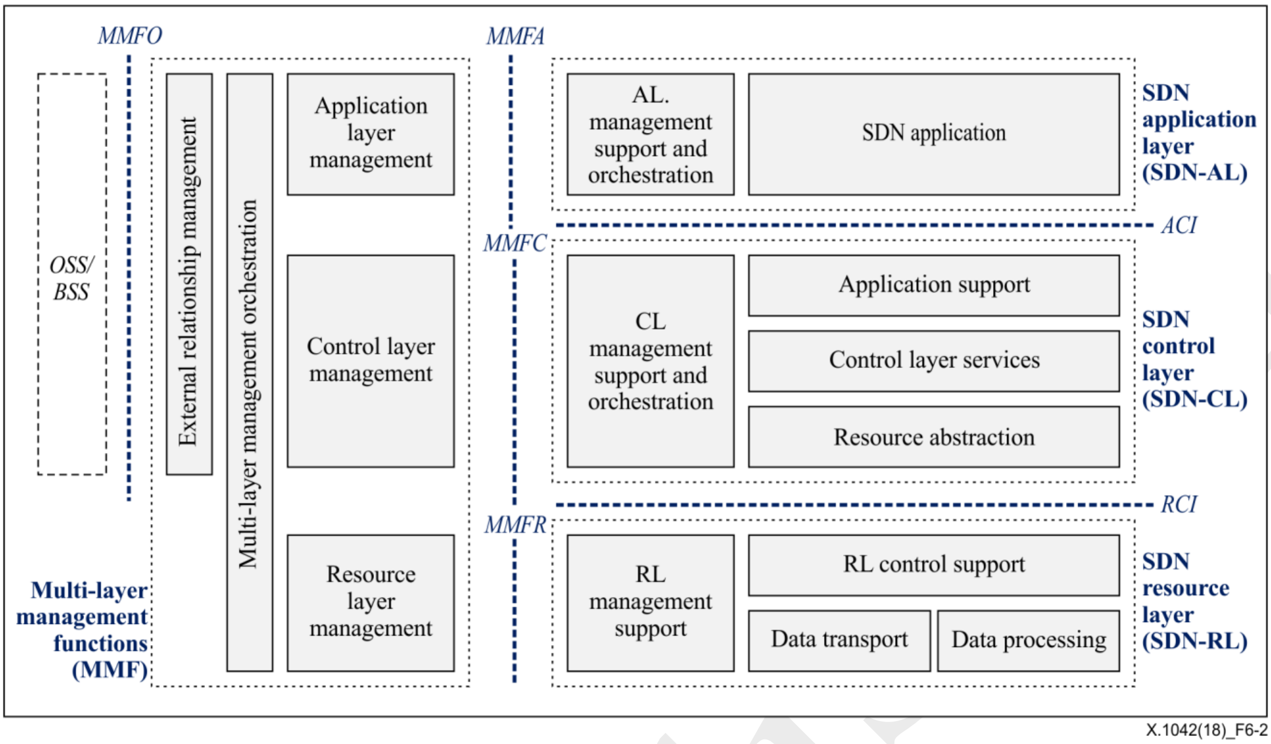

MMFO
MMFA
OSS/ BSS
External relationship management
Multi-layer management orchestration
Application layer management
Control layer management
Resource layer management
Multi-layer management functions (MMF)
AL. management support and orchestration
SDN application
SDN application layer (SDN-AL)
ACI
MMFC
CL management support and orchestration
Application support
Control layer services
Resource abstraction
SDN control layer (SDN-CL)
RCI
MMFR
RL management support
RL control support
Data transport
Data processing
SDN resource layer (SDN-RL)
X.1042(18)_F6-2

Figure 56 - SDN functional architecture

However, there are some challenges for implementing a full-scale carrier SDN. SDN security is one of the most important challenges. Multiple standards have been developed to respond to this challenge.

10.7.3 Security architecture and reference architecture for SDN

The major security threats are spoofing, repudiation, information disclosure, application security vulnerabilities. Those threats are identified based on use cases and security requirements are defined from them.

A security reference architecture including possible security countermeasures shown in Figure 57 is defined in Recommendation ITU-T X.1038, Security requirements and reference architecture for software-defined networking.

Pre-publication

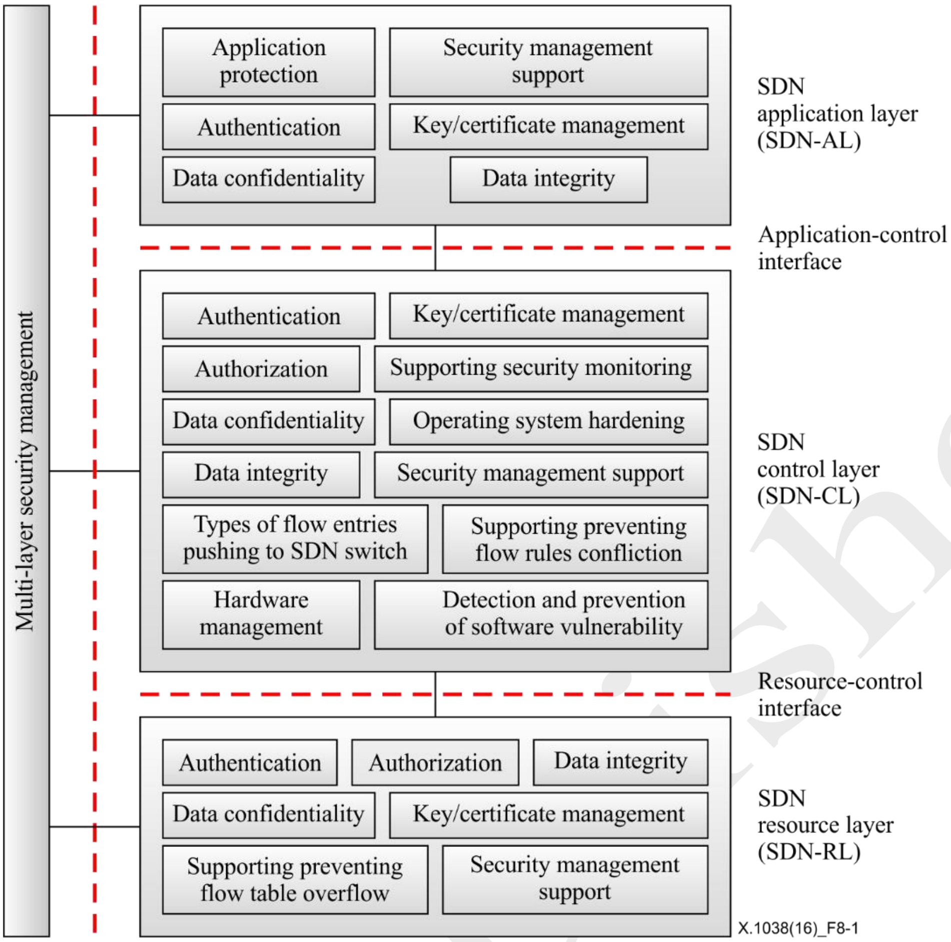

Multi-layer security management
Application protection
Security management support
Authentication
Key/certificate management
Data confidentiality
Data integrity
SDN application layer (SDN-AL)
Application-control interface
Authentication
Key/certificate management
Authorization
Supporting security monitoring
Data confidentiality
Operating system hardening
Data integrity
Security management support
Types of flow entries pushing to SDN switch
Supporting preventing flow rules confliction
Hardware management
Detection and prevention of software vulnerability
SDN control layer (SDN-CL)
Resource-control interface
Authentication
Authorization
Data integrity
Data confidentiality
Key/certificate management
Supporting preventing flow table overflow
Security management support
SDN resource layer (SDN-RL)
X.1038(16)_F8-1

Figure 57 – Security reference architecture for SDN

The logical function multi-layer security management is to provide security configuration and management for the SDN application layer, control layer and resource layer, including:

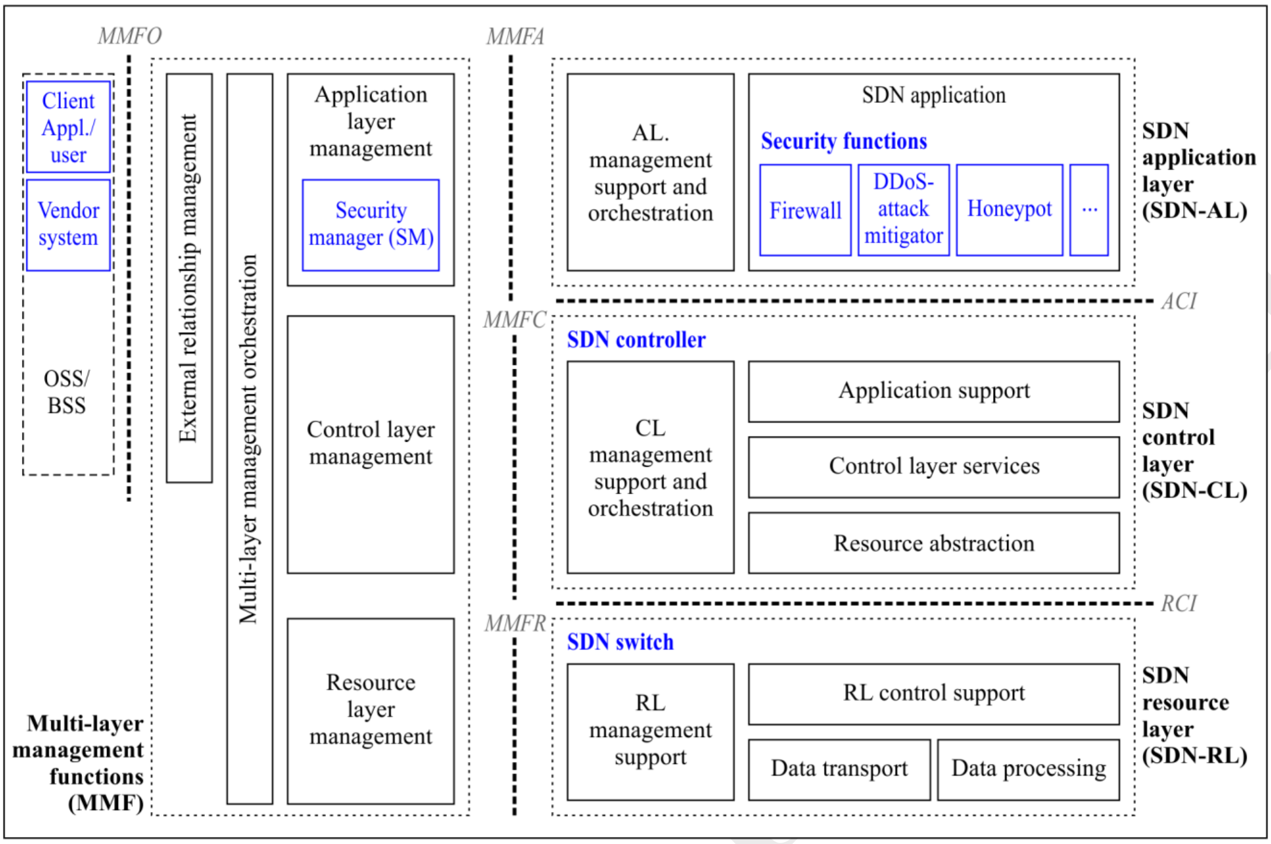
- to control access to platform-specific resources according to security policies so that the platform cannot be sabotaged (intentionally or unintentionally);
- to monitor users logging on to a platform, refusing access to those who enter inappropriate access codes, making a platform-specific minimum configuration, enforcing security policies on operating system and application system;
- to use aggregate information and statistics for the purposes of monitoring attacks on the platform.

10.7.4 Security services using SDN

Software-defined networking needs security, but also, security can be provided by SDN. Recommendation ITU-T X.1042 supports the protection of network resources using security services based on (SDN).

This Recommendation defined four network resources for security services using SDN based on the functional architecture of SDN in Recommendation ITU-T Y.3302. The network resources for SDN-based security services can be classified as three categories: SDN application, SDN controller, SDN switch and security manager (SM).

Pre-published



X.1042(18)_F7-1

Figure 58 – Network resources in SDN-based security services

The security services defined based on SDN are classified into two kinds of networking: (i) Intra-domain networking, e.g. centralized firewall service and centralized honeypot service; and (ii) Inter-domain networking, e.g. centralized DDoS-attack mitigation service and centralized illegal device management service

Recommendation ITU-T X.1042 describes the service scenarios for the centralized firewall service allowing the firewall rules to be managed flexibly, and for the collaborated firewall service with a deep packet inspection (DPI) application achieving centralized voice over internet protocol (VoIP) / voice over long term evolution (VoLTE) flow monitoring and management. The basic concept and service scenarios of centralized honeypot service for stateless domain name services (DNS) servers and for stateful web servers are also provided.

The centralized DDoS-attack mitigation service can adds, deletes or modifies rules to each SDN switch, and the centralized illegal device management service can manage the blacklist of illegal devices to prevent the traffic from/to those devices, such as stolen mobile devices.

Also, the basic concept of access control management (ACM) service based on SDN is introduced. The ACM module with SDN controller can manage the access right policies hierarchically in order to prevent illegal accesses to the resources, and specified how to implement SDN-based security services.

10.7.5 Security framework of SDN-based service function chaining

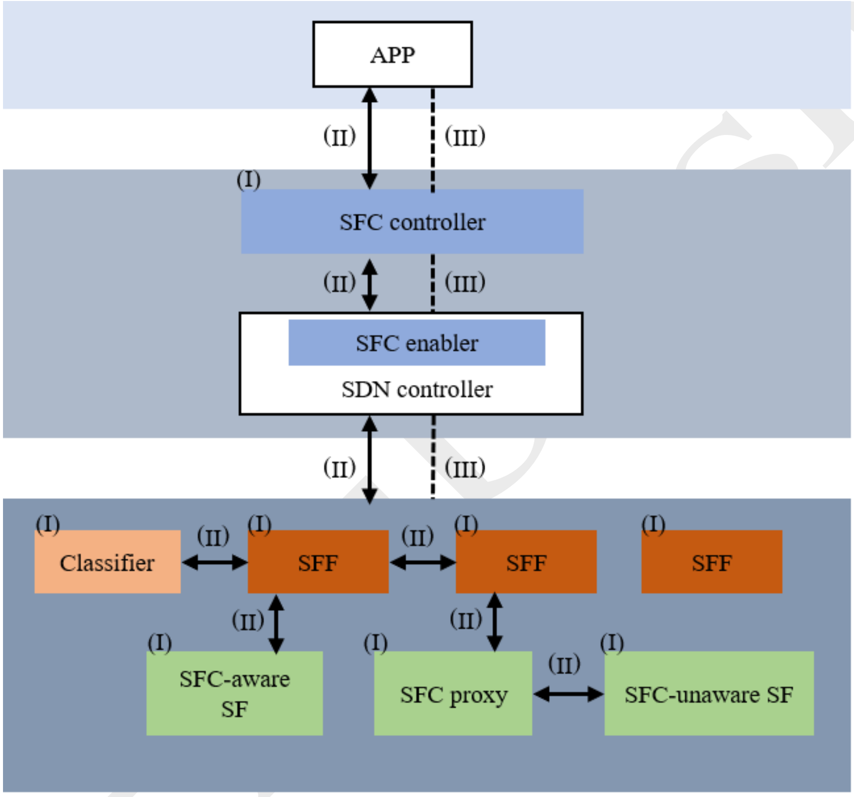
Recommendation ITU-T X.1043 analyses security threats encountered in service function chaining based on software-defined networking (SDN) and specifies security guidelines for SDN-based service function chaining architectures. The security reference architecture for SDN in Figure 57 is specified in ITU-T X.1038 and can be applied to SDN-based service function chaining, with the addition of some specific security features.

Three security feature groups are defined in Figure 59

(I) Critical network elements security: A set of security features that provides security functions on network entities to support secure creation, running, maintenance and deletion of a service function chain (SFC).

(II) Interface security: A set of security features that provides security functions to ensure secure transportation of communication data.

(III) Policy management: A set of security features that provides policy lifecycle security, e.g., the policy is created by a legal SFC application (app), sent with security protection and implemented correctly. It also resolves the SFC policy conflict, e.g., the conflict between the new SFC classification rules and the stored active SFC classification rules in the SFC repository of the SFC controller, the conflict between the translated flow rules from the SFC classification rules and the traditional SDN flow rules on the SDN controller.



X.1043(19)_F7-1

Figure 59 - General security framework of software-defined networking-based service function chaining

10.7.6 Architecture of security service chain

Recommendation ITU-T X.1045 supports provision of customized dynamic and adaptive security services for networks and applications. This Recommendation defines the security service chain and an architecture design for the security service chain. This Recommendation applies the security service chain to networks and applications. This Recommendation also enables tracing network attacks to their resources in a service function chain (SFC) overlay network with high performance and the mitigating/preventing of those attacks automatically.

Figure **60** shows the architecture of a security service chain which enables security service providers to create a stand-alone SSC to then manage and operate stand-alone security services such as packet filtering, intrusion detection and prevention and traffic cleaning.

Pre-published

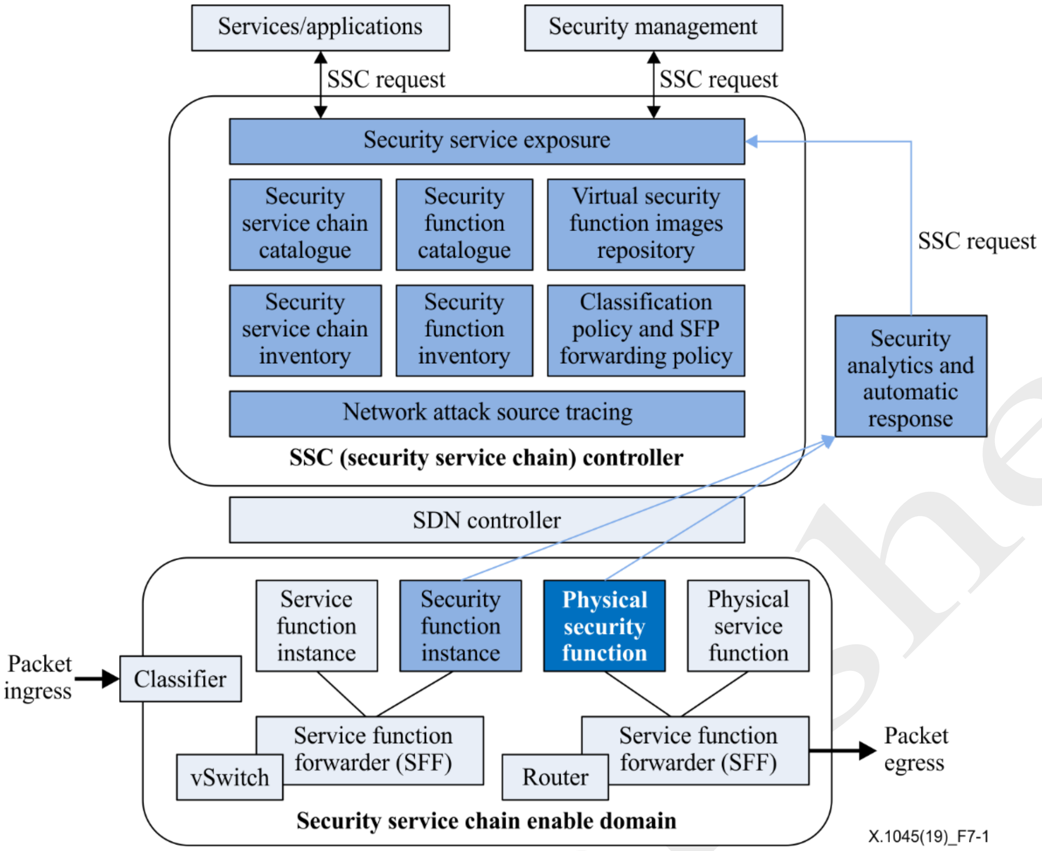

Services/applications
Security management
SSC request
SSC request
Security service exposure
Security service chain catalogue
Security function catalogue
Virtual security function images repository
Security service chain inventory
Security function inventory
Classification policy and SFP forwarding policy
Network attack source tracing
SSC (security service chain) controller
SSC request
Security analytics and automatic response
SDN controller
Packet ingress
Classifier
Service function instance
Security function instance
Physical security function
Physical service function
Service function forwarder (SFF)
Service function forwarder (SFF)
vSwitch
Router
Packet egress
Security service chain enable domain
X.1045(19)_F7-1

Figure 60 - **Security service chain (SSC) architecture**

In Figure 60, the *classifier*, *service function forwarders* (SFFs) and *service functions* (SFs) are as defined in [IETF RFC 7665]. Service functions include virtualized functions (e.g., *service function instance* and *security function instance*) and physical functions (e.g., *physical service function* and *physical security function*). The *SDN controller*, *vSwitch* and *router* are as defined in [b-ONF OpenFlow]. *Services/applications* and *security management* send an SSC request to the *SSC controller* according to their security requirements and then obtain customized security services from the *SSC controller*.

The functionalities of the SSC controller components and security analytics and automatic response (SAAR) are described in Recommendation ITU-T X.1045.

10.8 IMT-2020/5G security

Recommendation ITU-T X.1814 identifies all components related to the security of IMT-2020 communication systems and defines security guidelines for the IMT-2020 communication system. It describes a generic IMT-2020 architecture and its domains. It also identifies threats to and specifies requirements for security capabilities for each component, taking into account unique network features. This Recommendation is based on the 3GPP 5G security architecture.

Pre-published

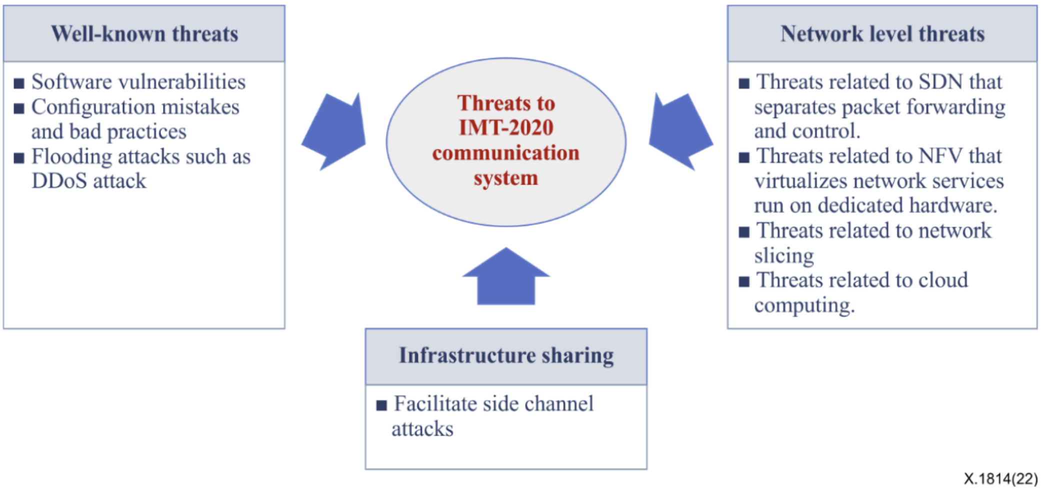

Well-known threats
■ Software vulnerabilities
■ Configuration mistakes and bad practices
■ Flooding attacks such as DDoS attack
Threats to IMT-2020 communication system
Network level threats
■ Threats related to SDN that separates packet forwarding and control.
■ Threats related to NFV that virtualizes network services run on dedicated hardware.
■ Threats related to network slicing
■ Threats related to cloud computing.
Infrastructure sharing
■ Facilitate side channel attacks
X.1814(22)

Figure 61 – Exemplar threats in IMT-2020

This Recommendation ITU-T X.1811 covers an introduction to the security architecture of International Mobile Telecommunications-2020 (IMT-2020) systems, a security assessment of IMT-2020 systems when commercial quantum computers are available and a specification of the usage of quantum-safe algorithms in IMT-2020 systems.

Recommendation ITU-T X.1812 identifies stakeholders in an International Mobile Telecommunications-2020 (IMT-2020; also known as fifth generation) ecosystem, analyses trust relationships amongst them, identifies threats and clarifies security responsibilities for each stakeholder, specifies security boundaries between stakeholders, and establishes a security framework based on these trust relationships.

Recommendation ITU-T X.1813 specifies the security requirements for the operation of vertical services supporting ultra-reliable and low-latency communications (URLLC) in IMT-2020 private networks. It identifies security threats and risks that arise when providing vertical services supporting URLLC in IMT-2020 private networks and describes security deployment scenarios of the IMT-2020 private networks for the operation of vertical services supporting URLLC.

Pre-published

11. Cybersecurity and incident response

Pre-published

Pre-published

11 Cybersecurity and incident response

As we have been seeing for some years now, threats and attacks also continue to evolve in increasingly innovative ways. It will remain an on-going challenge to design and develop timely and effective countermeasures to these threats. It will also be a challenge to achieve better, more secure design and implementation of systems and networks so that inherent vulnerabilities are reduced. And it will be increasingly difficult to achieve a rapid response to counter the new threats, a situation that, once again, highlights the importance of secure design and implementation. One positive step is the sharing of information on threats, as evidenced by our cybersecurity exchange work. This will improve the ability of the global telecommunications/ICT community to respond to threats and diminish their impact.

11.1 Cybersecurity information sharing and exchange

Cyber-attacks are widespread and cause a complex range of problems to users, service providers and operators. Effective response to such attacks is dependent on understanding the source and nature of the attack and sharing information with monitoring agencies. Countering cyber-attacks by technical means requires the development of a framework and requirements for detecting, protecting against, mitigating the effects of, and recovering from cyber-attacks, and addressing important technical issues facing network operators, enterprises, and governments. ITU-T has already developed a number of Recommendations on the efficient sharing of security and vulnerability information across domains and is developing solutions to support telecommunications/ICT accountability, incident response, threat monitoring and risk assessment.

11.1.1 Overview cybersecurity information exchange (CYBEX)

CYBEX techniques, which are addressed in the ITU-T X.1500 series of Recommendations, are directed towards enhancing the exchange of cybersecurity information in a way that takes account of the fact that the techniques themselves and the environment in which they are used are continuously-evolving.

The techniques embodied in the CYBEX Recommendations will enable telecommunication/ ICT organizations, including Computer Incident Response Teams (CIRTs), both within and between jurisdictions, to have the information necessary to facilitate secure, collaborative processes and controls to improve the level of assurance in information exchanges between organizations and also to support decision making, thereby substantially enhancing the security of global telecommunication/ICT facilities and services. In addition, these Recommendations enable a coherent approach to managing and exchanging cybersecurity information globally and improve security awareness and collaboration to diminish the impact of cyber threats, attacks and malware.

Recommendation ITU-T X.1500 presents a CYBEX model and discusses techniques that can be used to facilitate the exchange of cybersecurity information. These techniques can be used individually or in combination, as desired or appropriate, to enhance cybersecurity through coherent, comprehensive, global, timely and assured information exchange. No obligations to exchange information are implied, nor are the means of acquisition or ultimate use of the information treated. The techniques include the structured global discovery and interoperability of cybersecurity information in such a way as to allow for evolution to accommodate continuous advances being made in the various cybersecurity forums.

The general cybersecurity information exchange model shown in Figure 62 consists of basic functions that can be used separately or together as appropriate, and extended as needed in order to facilitate assured cybersecurity information exchanges. These are:

- structuring cybersecurity information for exchange purposes;
- identifying and discovering cybersecurity information and entities;
- establishing trust and policy agreement between exchanging entities;

- requesting and responding with cybersecurity information; and
- assuring the integrity of the cybersecurity information exchange.

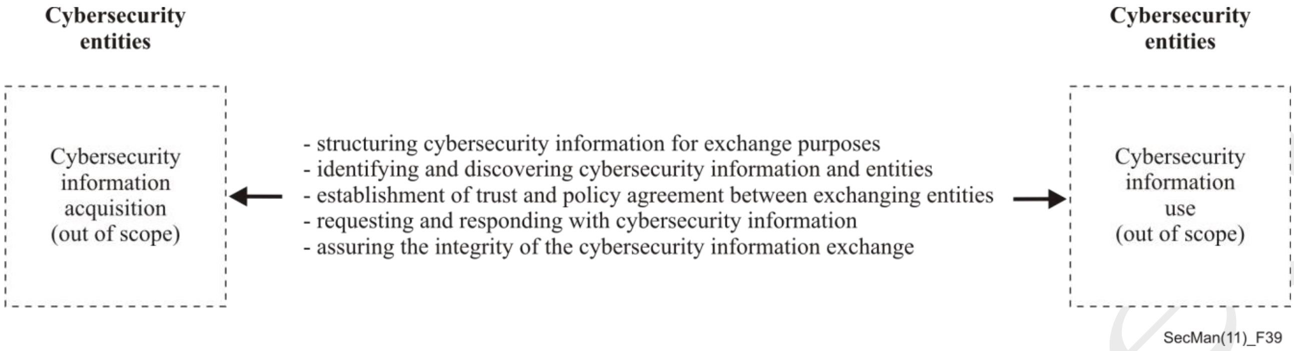

Cybersecurity entities
Cybersecurity information acquisition (out of scope)
- structuring cybersecurity information for exchange purposes
- identifying and discovering cybersecurity information and entities
- establishment of trust and policy agreement between exchanging entities
- requesting and responding with cybersecurity information
- assuring the integrity of the cybersecurity information exchange
Cybersecurity entities
Cybersecurity information use (out of scope)
SecMan(11)_F39

Figure 62 – CYBEX model

These techniques are further organized into “clusters” in the ITU-T X.1500 series Recommendations:

- Weakness, vulnerability and state;
- Event, incident, and heuristics;
- Information exchange policy;
- Identification, discovery, and query;
- Identity assurance; and
- Exchange protocols.

11.1.2 Exchange of vulnerability information

Recommendation ITU-T X.1520 on the common vulnerabilities and exposures (CVE) provides a structured means to exchange information on security vulnerabilities and exposures and provides a common identifier for publicly- known problems. This Recommendation defines the use of CVE to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this common identifier. This Recommendation is designed to allow vulnerability databases and other capabilities to be used together, and to facilitate the comparison of security tools and services. CVE contains only the standard identifier number with status indicator, a brief description, and references to related vulnerability reports and advisories. (It does not contain information such as risk, impact, fix information, or detailed technical information).

The primary focus of CVE is to identify known vulnerabilities and exposures that are detected by security tools along with any new problems that are detected.

11.1.3 Vulnerability scoring

ICT management must identify and assess vulnerabilities across many disparate hardware and software platforms. These vulnerabilities must then be prioritized and, those that pose the greatest risk, remediated. With so many vulnerabilities, and with each being scored using different scales, ICT managers are left to determine how to compare and prioritize them.

Recommendation ITU-T X.1521 on the common vulnerability scoring system (CVSS) is an open framework that standardizes vulnerability scores, explains the properties and individual characteristics used to derive a score, and prioritizes risk by making the vulnerability scores indicative of the actual risk in relation to other vulnerabilities.

Pre-published

CVSS metrics are divided into three groups: base metrics, temporal metrics and environmental metrics as illustrated in Figure 63.

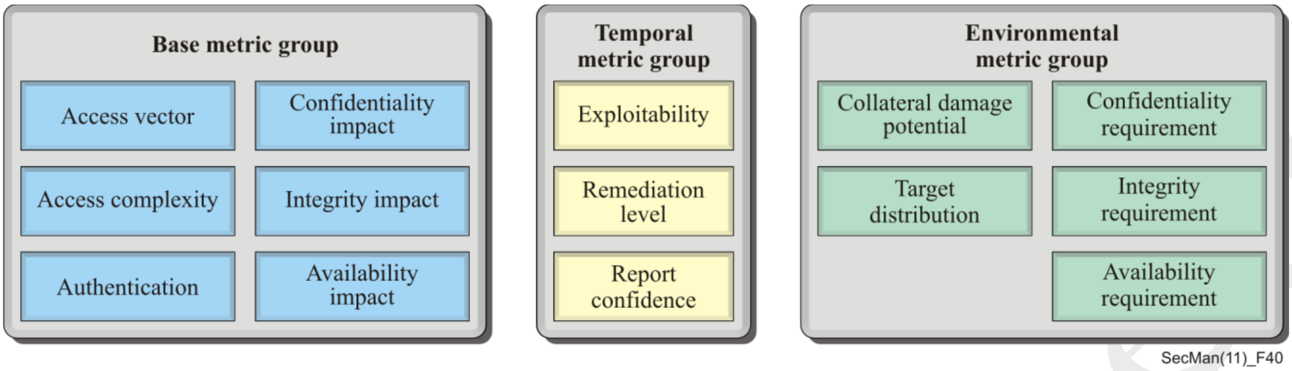


Figure 63 – CVSS metric groups

Base metrics represent intrinsic and fundamental vulnerability characteristics that are constant over time and user environments. Temporal metrics represent vulnerability characteristics that change over time but not among user environments. Environmental metrics represent vulnerability characteristics that are relevant and unique to a particular user's environment.

The CVSS base group of metrics defines the fundamental characteristics of a vulnerability. This provides users with a clear and intuitive representation of a vulnerability. Users can then invoke the temporal and environmental groups to provide contextual information that more accurately reflects the risk to their unique environment. This allows them to make more informed decisions when trying to mitigate risks posed by the vulnerabilities.

CVSS is being used in a number of different ways:

- Vulnerability bulletin providers are including CVSS base and temporal scores and vectors in their bulletins. These bulletins offer much information, including the date of discovery, systems affected and links to vendors for patching recommendations;
- Software application vendors are advising their customers of CVSS base scores and vectors to help them understand the severity of vulnerabilities in their products, thus helping the customers to manage their ICT risk more effectively;
- User organizations are using CVSS internally to make informed vulnerability management decisions. They use scanners or monitoring technologies to first locate host and application vulnerabilities. They combine this data with CVSS base, temporal and environmental scores to obtain more contextual risk information and remediate those vulnerabilities that pose the greatest risk to their systems;
- Vulnerability management organizations scan networks for ICT vulnerabilities and provide CVSS base scores for each vulnerability, on each host. User organizations then use this data to manage their security operations and protect against malicious and accidental ICT threats;
- Security risk management firms use CVSS scores as one of the inputs in calculating an organization's risk or threat level. When combined with information such as network topology and assets, this can provide customers with a more informed perspective of their risk exposure; and
- The open framework of CVSS enables researchers to perform statistical analysis on vulnerabilities and vulnerability properties.

Pre-published

11.1.4 Exchange of weakness information

Recommendation ITU-T X.1524 on the use of the common weakness enumeration (CWE) provides a structured means to exchange unified, measurable sets of software weaknesses that aims to provide common names for publicly known problems. The goal of CWE is to make it easier to enable more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as to promote better understanding and management of software weaknesses related to architecture and design.

The intention of CWE is to be comprehensive with respect to the causes behind all publicly known vulnerabilities and exposures, whether from weaknesses in the software's architecture, design, code, or deployment. While CWE is designed to contain mature information, the primary focus is on identifying the weaknesses that can cause vulnerabilities and exposures. The review authority determines conformance on the use of CWE identifiers, as defined in this Recommendation.

CWE gives leverage to existing work from within the cybersecurity community such as the large number of diverse real-world vulnerabilities specified in Recommendation ITU-T X.1520, Common vulnerabilities and exposures (CVE). Many sources and examples are leveraged to develop the specific and succinct definitions of the CWE list elements and classification tree structures. In addition, appropriate mappings are created between CWEs and CVE names so that each CWE identifier has a list of the specific CVE names that belong to that particular CWE category of software security weaknesses. In constructing the CWE list and classification tree, maximum comprehensive coverage across appropriate conceptual, business, and technical domains is sought.

11.1.5 Weakness scoring

Software developers often face hundreds or thousands of individual bug reports for weaknesses that are discovered in their code. In certain circumstances, a software weakness can even lead to an exploitable vulnerability. Due to this high volume of reported weaknesses, stakeholders are often forced to prioritize which issues they should investigate and fix first. In short, people need to be able to reason and communicate about the relative importance of different weaknesses. While various scoring methods are used today, they are either ad hoc or inappropriate for application to the still-imprecise evaluation of software security.

Recommendation ITU-T X.1525, Common weakness scoring system (CWSS), provides an open framework for communicating the characteristics and impacts of information and communication technologies (ICT) weaknesses during development of software capabilities. The goal of this Recommendation is to enable ICT software developers, managers, testers, security vendors and service suppliers, buyers, application vendors and researchers to speak from a common language of scoring ICT weaknesses that could manifest as vulnerabilities when the software is used.

CWSS is organized into three *metric groups*: Base Finding, Attack Surface, and Environmental, as shown in Figure 64. Each group contains multiple metrics – also known as *factors* – that are used to compute a CWSS score for a weakness.

Pre-published

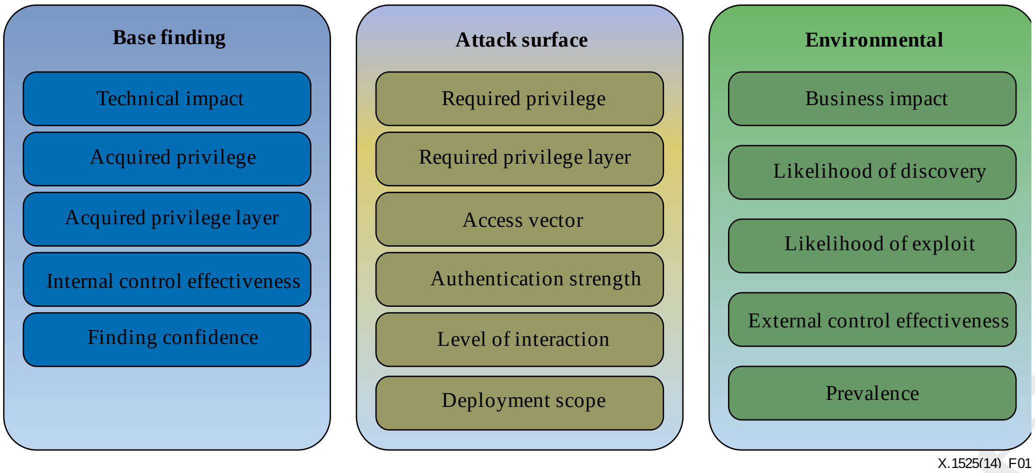


Figure 64 – CWSS metric groups

The Base Finding metric group captures the inherent risk of the weakness, confidence in the accuracy of the finding, and strength of controls. The Attack Surface metric group represents the barriers that an attacker must overcome in order to exploit the weakness. The Environmental metric group represents characteristics of the weakness that are specific to a particular environment or operational context.

11.1.6 Exchange of attack pattern information

Recommendation ITU-T X.1544, Common attack pattern enumeration and classification (CAPEC), is an XML/XSD-based specification for the identification, description and enumeration of attack patterns. Attack patterns are a powerful mechanism to capture and communicate the attacker's perspective. They are descriptions of common methods for exploiting software. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples. The objective of CAPEC is to provide a publicly-available catalogue of attack patterns along with a comprehensive schema and classification taxonomy.

CAPEC enables:

- Standardizing the capture and description of attack patterns;
- Collecting known attack patterns into an integrated enumeration that can be consistently and effectively leveraged by the community;
- Classifying attack patterns so that users can easily identify the subset of the entire enumeration that is appropriate for their context; and
- Linking, through explicit references, the attack patterns and the common weakness enumerations (CWEs) that they are effective against.

11.1.7 Exchange of malware characteristics information

Recommendation ITU-T X.1546, Malware attribute enumeration and characterization (MAEC), is an international, information security, community standard to promote open and publicly-available security content about malware and malware behaviours. This Recommendation also aims to standardize the transfer of this information across the entire spectrum of security tools and services that can be used to monitor and manage defences against malware. MAEC is a language used to encode malware relevant details.

Pre-published

The MAEC language aims to: improve human-to-human, human-to-tool, tool-to-tool, and tool-to-human communication about malware; reduce potential duplication of malware analysis efforts by researchers; and allow for the faster development of countermeasures by enabling the ability to leverage responses to previously observed malware instances. Threat analysis, intrusion detection, and incident management are processes that deal with all manner of cyberthreats. MAEC, through its uniform encoding of malware attributes, provides a standardized format for the incorporation of actionable information regarding malware in these processes.

As shown in Figure 65, MAEC is composed of a data model that spans several interconnected schemas, thus representing the grammar that defines the language. These schemas permit different forms of MAEC output to be generated, which can be considered as specific uses of the aforementioned grammar.

The MAEC container, MAEC package and MAEC bundle schemas are targeted at different use cases and thus capture different types of malware-related information.

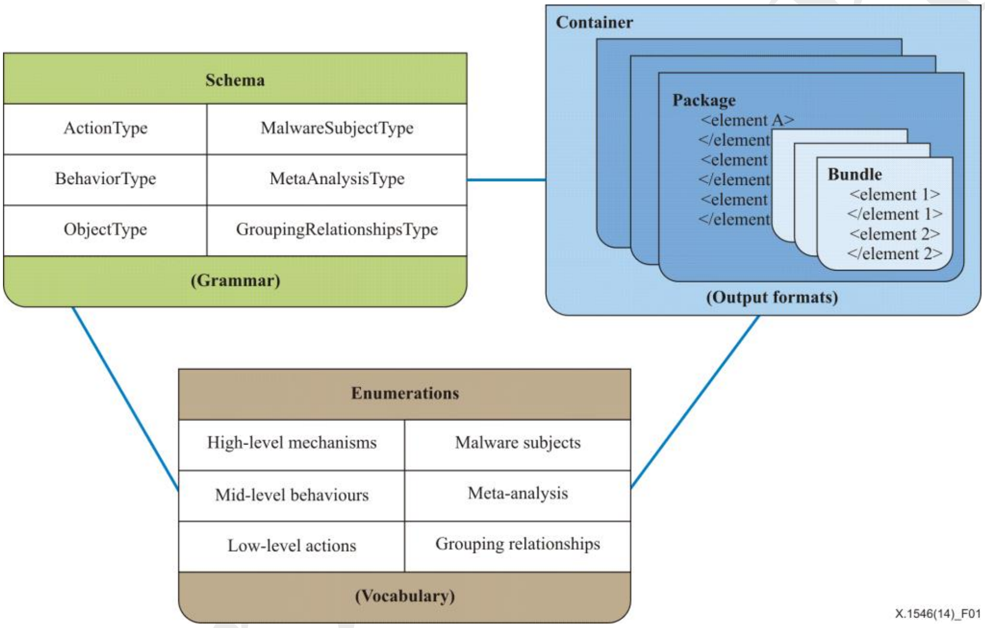


Figure 65– High-level MAEC overview

11.1.8 The structure threat information expression (STIX)

The structured threat information expression (STIX) is a structured language to share cyber threat intelligence and information, defined by OASIS. STIX provides structured representations that is expressive, flexible, extensible, automatable, and readable cyber threat information. Recommendation ITU-T X.1215 provides various use cases for how the STIX language may be used to support cyber threat intelligence and information sharing context. The Figure 66 depicts the overview of an example STIX.

Pre-published

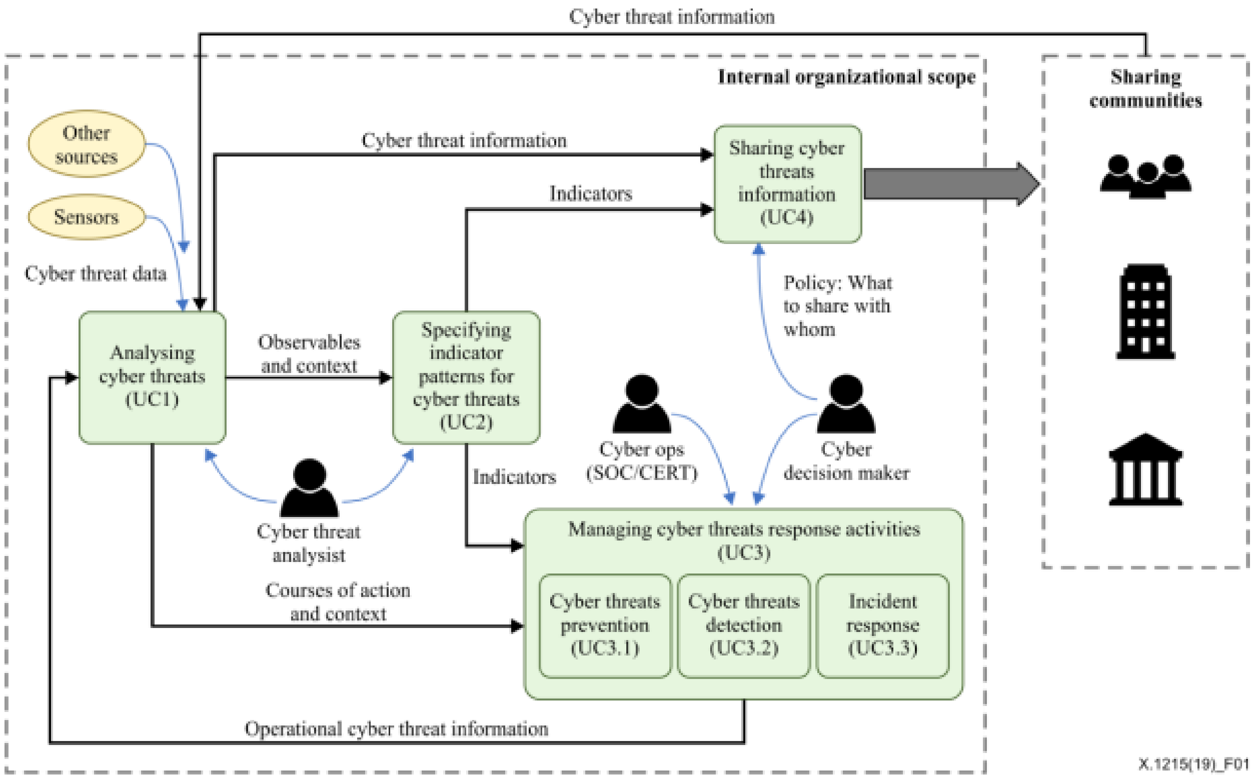

Cyber threat information
Internal organizational scope
Sharing communities
Other sources
Sensors
Cyber threat data
Cyber threat information
Sharing cyber threats information (UC4)
Indicators
Policy: What to share with whom
Analysing cyber threats (UC1)
Observables and context
Specifying indicator patterns for cyber threats (UC2)
Cyber ops (SOC/CERT)
Cyber decision maker
Indicators
Cyber threat analysist
Managing cyber threats response activities (UC3)
Courses of action and context
Cyber threats prevention (UC3.1)
Cyber threats detection (UC3.2)
Incident response (UC3.3)
Operational cyber threat information
X.1215(19)_F01

Figure 66 – Overview of STIX use case

11.2 Discovery of cybersecurity information

Discovery of cybersecurity information involves three entities: a retriever; a source; and a directory. The retriever obtains information by sending a request to the source which provides the requested information. The directory registers the metadata of the source's information and helps the retriever to find a proper source.

Recommendation ITU-T X.1570 provides a framework for discovering cybersecurity information and the mechanism that enables this. The framework covers how to publish cybersecurity information, obtain the candidate list, and acquire the needed information.

Discovery schemes rely on information registries which may be centralized or decentralized. With a centralized registry, an object identifier-based discovery mechanism is typically used to identify and locate the sources of cybersecurity information. Where registries are distributed, the party seeking the information uses a Resource Description Framework-based discovery mechanism. Both of these mechanisms are described in this Recommendation.

The discovery mechanism is intended to find the following seven types of cybersecurity information: User Resource Database; Provider Resource Database; Incident Database; Warning Database; Product & Service Knowledge Base; Cyber Risk Knowledge Base; and Countermeasure Knowledge Base. The acquisition, accumulation and use of cybersecurity information, which consists of a set of operation domains, roles, and information types, is described in an ontology model shown in Figure 67 which also shows the relationship between the information types used in this model.

Pre-publication

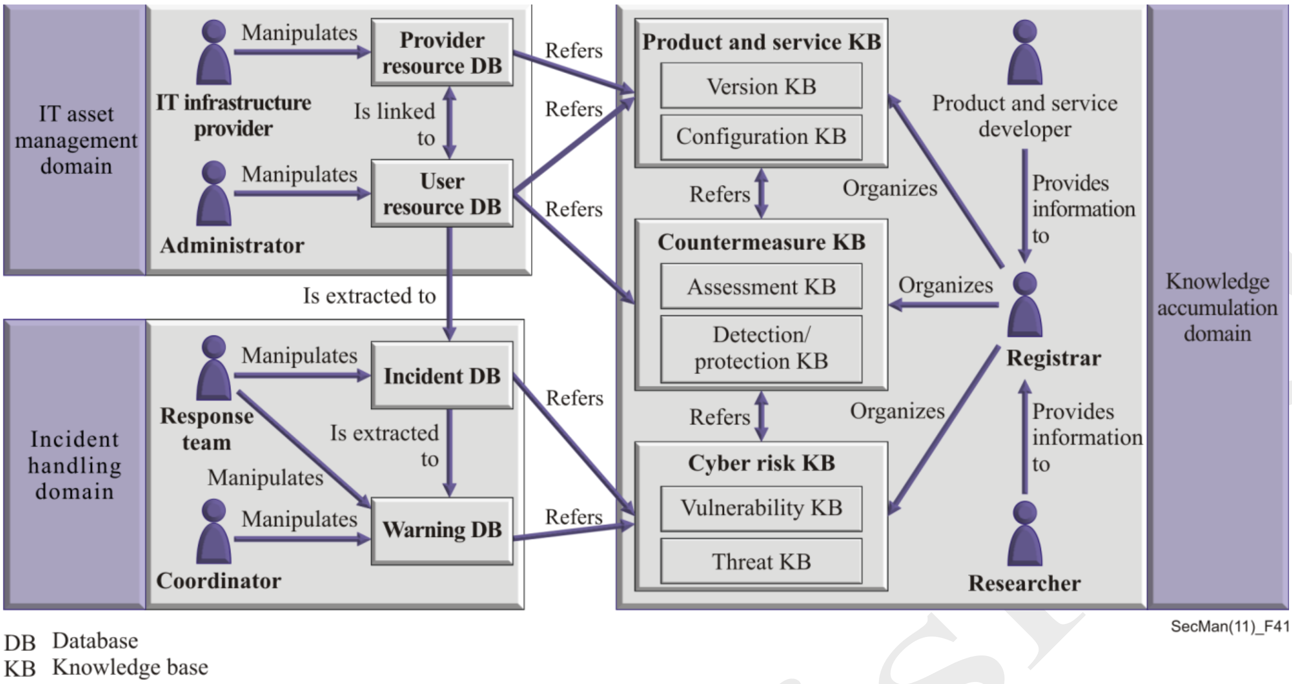


Figure 67 – Cybersecurity operational information ontologys

The roles, illustrated with human icons in the figure, are generic and entities such as CIRTs may encompass one or more of these functions. This model is used to define domains for cybersecurity operations, which are then used to identify required cybersecurity entities to support the operations in each domain.

11.3 Access control for incident exchange network

Cybersecurity incident exchange practices introduce a variety of information-sharing models that are implemented in centralized or federated environments. Incident information sharing is based on a level of trust that correlates with associated risks and imposes the need to assure that confidential or sensitive information is not inappropriately shared. This makes some access control models more effective than others in terms of performance, implementation and security assurance.

Recommendation ITU-T X.1550, Access control models for incident exchange networks, provides the mechanisms and approaches which may be used as profiles that provide access control policies implementation for underlying cybersecurity information exchange (CYBEX)-formats and transport protocols.

Incident information exchange models are represented as "Peer-to-peer", "Hub-spokes", "Post-to-all". "Peer-to-peer" model, in general, may not require a high degree of trust since the single communication channel can be controlled by diverse variety of methods. "Hub-spokes" model usually requires a high or medium (since "hub" may filter information) level of trust, while "Post-to-all" model usually requires a high degree of trust among participants. It is naturally implied that the higher the level of trust, the simpler the requirements and granularity for access control. That is, the level of trust directly influences the level of complexity for access control mechanisms.

There are several access control models starting from conservative models (considering less granular policies) to adaptive models (considering more granular and environment-dependent policies). Figure 68 illustrates the taxonomy of access control models.

Pre-published

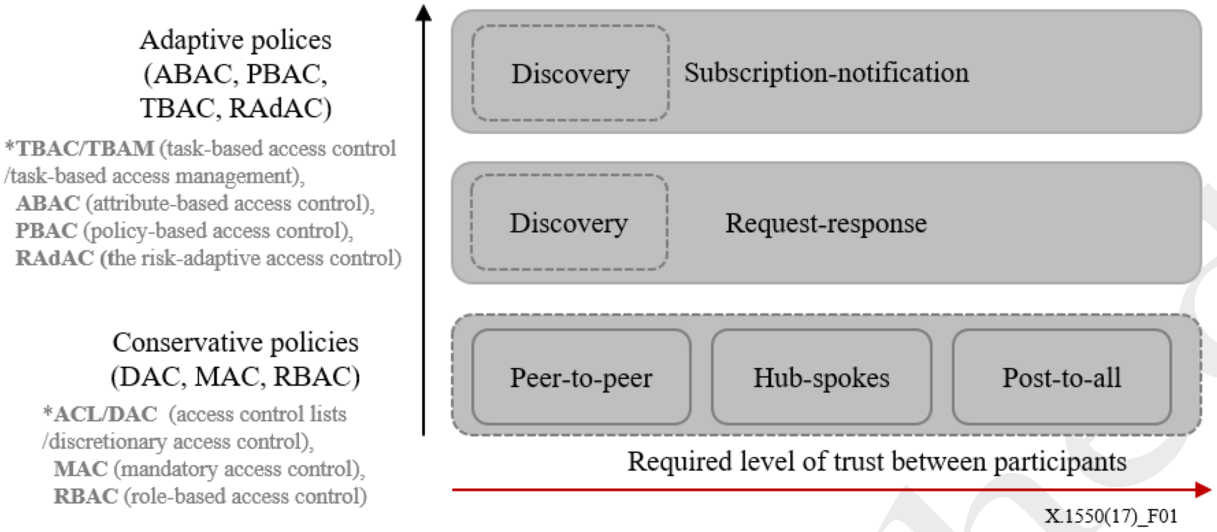

Adaptive polices (ABAC, PBAC, TBAC, RAdAC)
*TBAC/TBAM (task-based access control /task-based access management),
ABAC (attribute-based access control),
PBAC (policy-based access control),
RAdAC (the risk-adaptive access control)
Conservative policies (DAC, MAC, RBAC)
*ACL/DAC (access control lists /discretionary access control),
MAC (mandatory access control),
RBAC (role-based access control)
Discovery
Subscription-notification
Discovery
Request-response
Peer-to-peer
Hub-spokes
Post-to-all
Required level of trust between participants
X.1550(17)_F01

Figure 68 – Access control models, sharing models and trust level taxonomy

To facilitate implementation of access control policies, this Recommendation provides the appropriate policy definition languages, policy conflicts resolution strategies, performance evaluation mechanisms under various environments for access control models.

11.4 Incident handling

Consistency in detecting, responding to, and disseminating information about security-related incidents is a routine part of security management. Unless all such incidents are properly evaluated and appropriately handled, organizations will be vulnerable to subsequent, possibly more serious, attacks.

Unless an incident handling procedure is in place, when a security-related incident is detected, there may be no proper reporting or analysis of the incident. There may also be no procedures for escalating the reporting or obtaining technical assistance or management direction, even though issues raised by such incidents often have ramifications that extend well beyond IT or networking. For example, incidents may imply legal, financial or reputational risk or they may be matters for law enforcement. Lack of effective incident handling procedures may result in a "quick fix" or work-around being used, instead of the problem being properly addressed, documented and reported, in which case there is the risk of more serious problems later.

As organizations become sensitized to the need for consistent and effective security management of networks and operations, incident handling is becoming a more routine practice. Properly trained and mandated staff can handle security incidents in a prompt and correct manner.

To be able to succeed in incident handling and incident reporting, an understanding of how incidents are detected, managed and resolved is necessary. By establishing a structure for incident handling (i.e., physical, administrative or organizational, and logical incidents) it is possible to obtain a picture of the structure and flow of an incident. Recommendation ITU-T E.409 provides guidance for planning an organization to detect and handle security-related incidents. It is generic in nature and does not identify or address requirements for specific networks.

Consistent use of terminology is essential when reporting or handling an incident. The use of different terminology can lead to misunderstandings, which may result in a security incident getting neither the proper attention, nor the prompt handling that is needed in order to contain the incident and prevent it from recurring.

Pre-published

In addition, the definition of what is considered to be an incident can vary among professions, organizations and people. Recommendation ITU-T E.409 defines terminology for incident detection and reporting and shows how to classify incidents according to their severity, as illustrated in Figure 69.

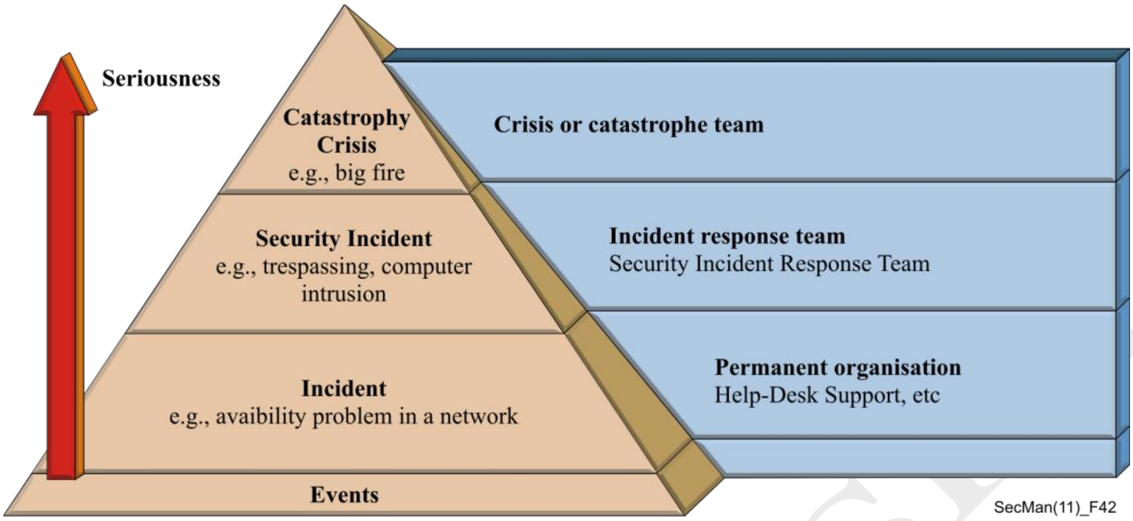


Figure 69 – ITU-T E.409 pyramid of events and incidents

Recommendation ITU-T E.409 also defines an incident handling structure (as illustrated in Figure 70) and sets out procedures for detecting, classifying, assessing, handling and following-up incidents.

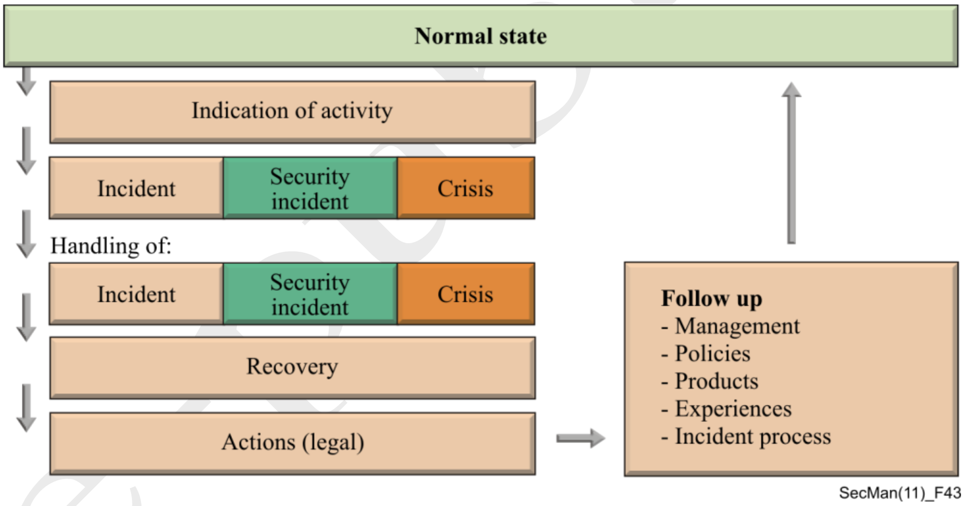


Figure 70 – ITU-T E.409 incident handling structure

The recently-approved Recommendation ITU-T X.1056 builds on the guidance provided in Recommendation ITU-T E.409. Telecommunication organizations need to have processes in place both to handle incidents and to prevent them re-occurring. Five high-level incident management processes – Prepare, Protect, Detect, Triage and Respond – are described in Recommendation ITU-T X.1056 along with the relationship to security management. These are illustrated in Figure 71.

Pre-published

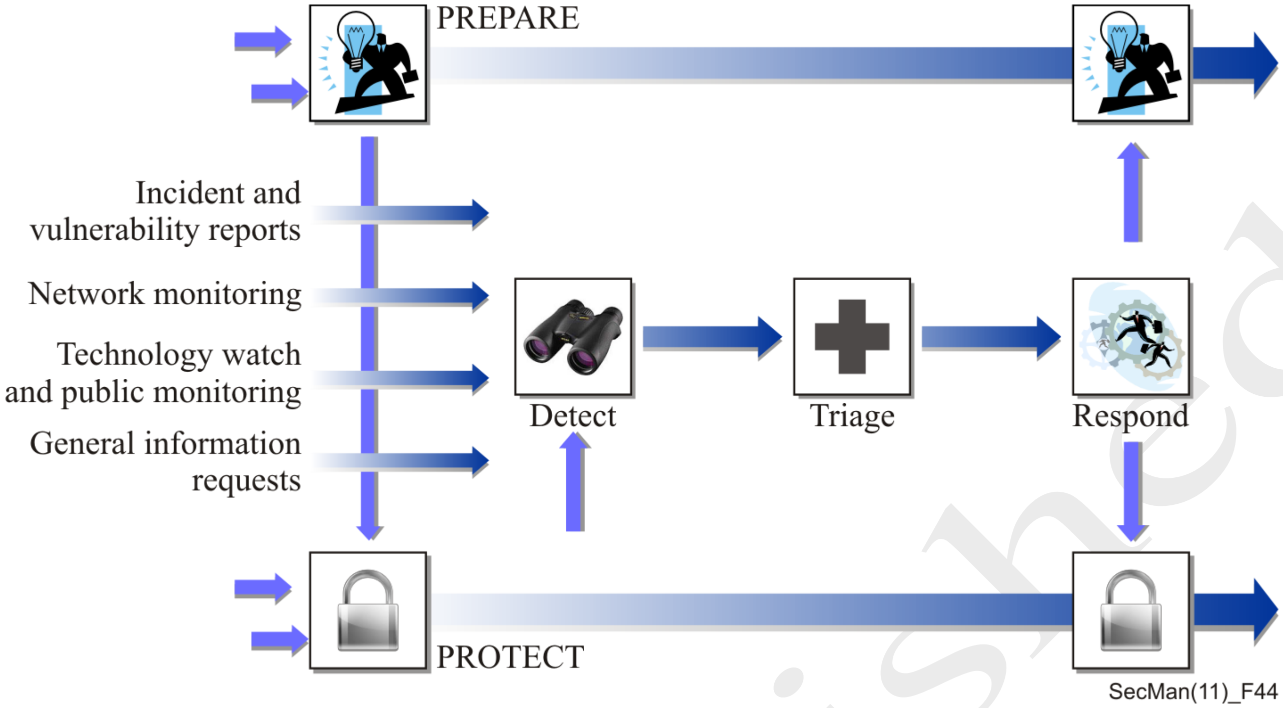

PREPARE
Incident and vulnerability reports
Network monitoring
Technology watch and public monitoring
General information requests
Detect
Triage
Respond
PROTECT
SecMan(11)_F44

Figure 71 – Five high-level incident management processes

In addition, Recommendation ITU-T X.1056 identifies a range of proactive, reactive, and security quality management services that a security incident management team can provide.

11.5 Unified Security Model (USM)

A system-level security design that protects a process creating value, the target requires not only effective security controls but a complete set of controls that addresses all vulnerabilities. Carefully identifying the applicable in-scope security controls to protect a target starts with the defining the target. It is achieved by applying a systematic process anchored on the target that methodically goes through every value asset enabling the process and addresses each vulnerability, identifies potential threats, and designs the appropriate countermeasures.

Such a process is described by the Unified Security Model (USM), a neutral integrated systematic approach to designing cybersecurity, based on an actual target. The USM represents all logical associations of threats to a specific target and corresponding countermeasures. The USM adopts a role-based decomposition model defining six security Actors[1] engaged in five security relationships[2]; resulting in an understanding of the residual risks from the imbalance between four digital value forces[3]: Value Creation Force, Value Risk Force, Value Preservation Force and Value Assurance Force.

[1] **Security Actors** perform the roles of the four Digital Forces and are represented by shapes

[2] **Security Relationships** are the execution of roles between Security Actor(s) illustrated by arrows between Actors

[3] **Digital Value Forces**: There are four Digital Forces as represented by four colors one for each core roles. Value Creation Force (gold) creates value anywhere. Value Risk Force (red) threatens the Value Creation Force. The Value Preservation Force (Blue) provides countermeasures against the Value Risk Force. The Value Assurance Force (Orange) ensures that the Value Creation Force is reasonable protected from the Value Risk Force.

Pre-published

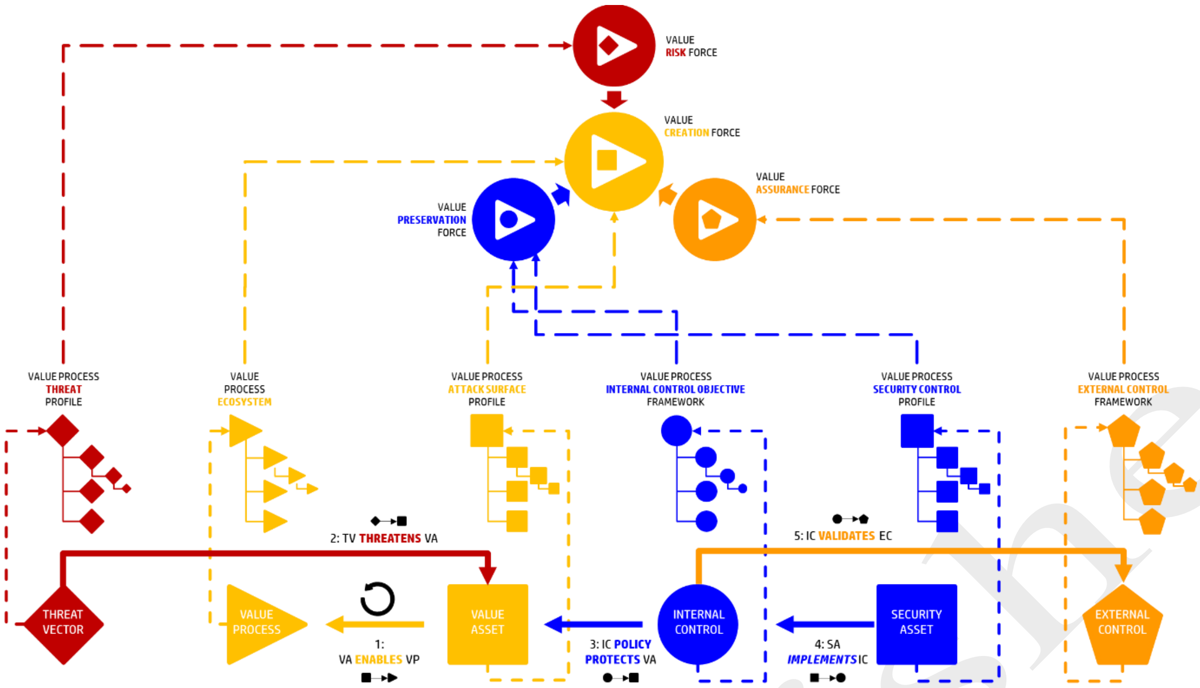


Figure 72 – Unified Security Model

Starting with gold triangle, for one Value Process[4] selected from the Value Process Ecosystem[5], iterate through all Value Assets[6] that enable the Value Process; for each identify the potential likelihood and impact of Threat Vectors[7] to each Value Asset vulnerability creating the Value Process Threat Profile[8]. Define the reasonable level of protection by policy given the Value Asset's criticality and sensitivity in the Value Process creating the custom Value Process Internal Control Framework[9]. Once the reasonable level of protection is defined, the people, process and technology required to fulfill each of the requirements of the Internal Controls[10] protecting all the Value Assets enabling the Value Process, creating the Value Process Security Control Profile[11].

Pre-published

[4] **Value Process** (gold triangle): a process creating, transferring, or consuming value

[5] **Value Process Ecosystem** (framework of gold triangles): system of multiple Value Processes

[6] **Value Asset** (solid gold square): people, process or technology enabling Value Process

[7] **Threat Vector** (red diamond): a threat designed to exploit a specific Value Asset vulnerability

[8] **Value Process Threat Profile:** all possible threat to a Value Process based on all vulnerabilities of Value Assets

[9] **Value Process Internal Control Framework**: (framework of blue circles): all internal policies related to the protection of a Value Process.

[10] **Internal Control** (Blue hollow square): a policy decision to secure a Value Asset based on the Threat Vector

[11] **Value Process Security Control Profile**: (framework of hollow blue squares): the set of all security controls (people process or technology) delivering against the requirements of all Internal Controls.

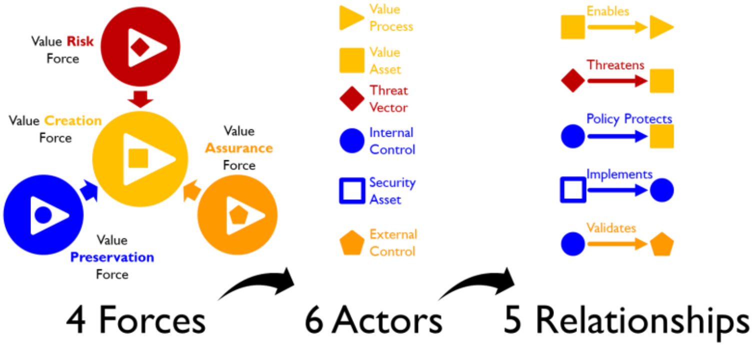


Figure 73 – Unified Security Model Leg

Pre-published

12. Application security

Pre-published

12 Application security

With the increasing awareness of the importance of security, application developers today are paying more attention to the need to build security into their products, rather than trying to retrofit security after the application moves into production. In spite of this, most applications, at some point in their lifecycle, are found to have some inherent vulnerabilities. In addition, evolving threats frequently expose and exploit vulnerabilities that were previously unknown.

In this section, the security features of a number of ICT applications are examined with particular emphasis on the security features addressed by ITU-T Recommendations.

12.1 Voice over Internet protocol (VoIP) and multimedia

VoIP, also known as IP telephony, is the provision of services traditionally offered by the circuit-switched Public Switched Telephone Network (PSTN) via a network using the Internet protocol (IP). Primarily, these services include voice, but also include other forms of media, including video and data. VoIP also includes many other associated supplementary services and intelligent network services such as conferencing (bridging), call forwarding, call waiting, multi-line, call diversion, park and pick-up, consultation, and "follow-me".

Recommendation ITU-T H.323, is an umbrella Recommendation that provides a foundation for audio, video, and data communications over packet-switched networks including the Internet, local-area networks (LANs), and wide-area networks (WANs), that do not provide a guaranteed quality of service (QoS). By complying with ITU-T H.323, multimedia products and applications from multiple vendors can interoperate, allowing users to communicate without concern for compatibility. Recommendation ITU-T H.323 was the first VoIP protocol to be defined and is considered to be the cornerstone for VoIP-based products for consumer, business, service provider and entertainment. Security specifications for the ITU-T H.323 series of Recommendations are contained in: the ITU-T H.235.x series of Recommendations, which includes nine security frameworks and standards; Recommendation ITU-T H.460.22, *Negotiation of security protocols to protect ITU-T H.225.0 call signalling messages*; and ITU-T H.530. Mobility for ITU-T H.323 multimedia systems and services is addressed in Recommendation ITU-T H.510.

Recommendation ITU-T H.323 is broad in scope and includes stand-alone devices and embedded personal computer technology as well as point-to-point and multipoint communications.

Recommendation ITU-T H.323 defines four major components for a network-based communications system: terminals, gateways, gatekeepers, and multipoint control units. In addition, border or peer elements are also defined. These help facilitate intra and inter-domain communication. These elements are illustrated in Figure 74.

Examples of where Recommendation ITU-T H.323 is used include wholesale transit by operators, especially for VoIP backbones and calling card services. In both corporate and residential environments, Recommendation ITU-T H.323 is used for audio- and video-conferencing, for voice/data/video collaboration, and distance learning.

Pre-published

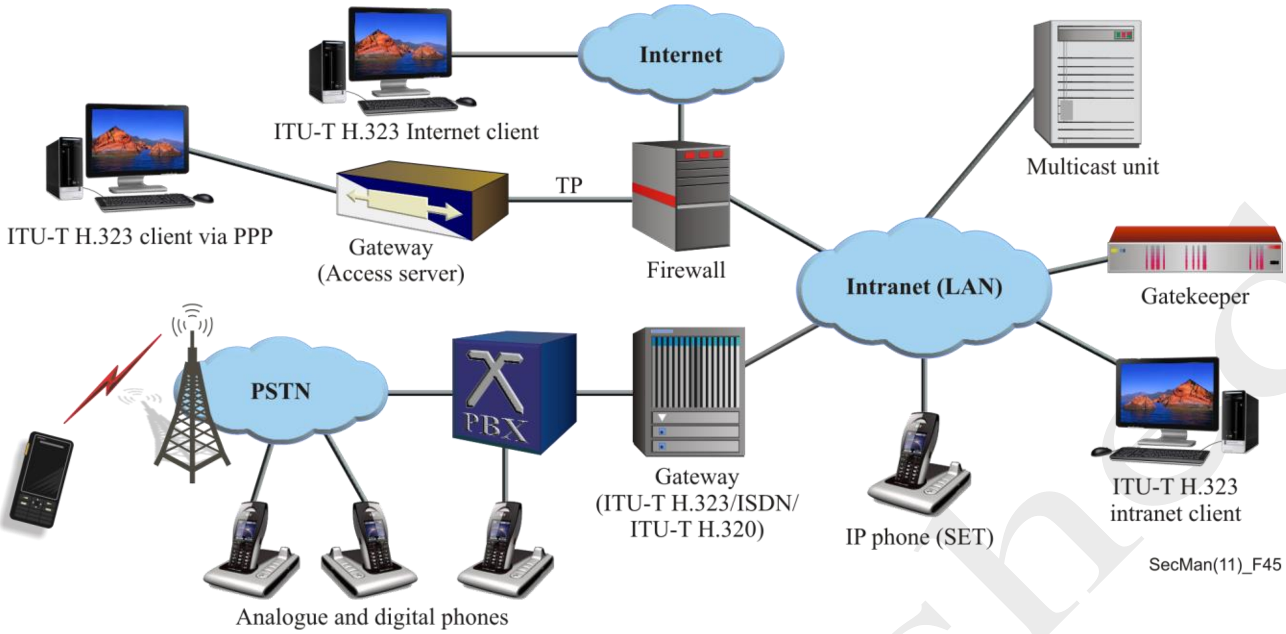


Figure 74 – ITU-T H.323 system: components and deployment scenarios

12.1.1 Security issues in multimedia and VoIP

The elements of a Recommendation ITU-T H.323 system can be geographically distributed and, due to the open nature of IP networks, several security threats exist, as illustrated in Figure 75.

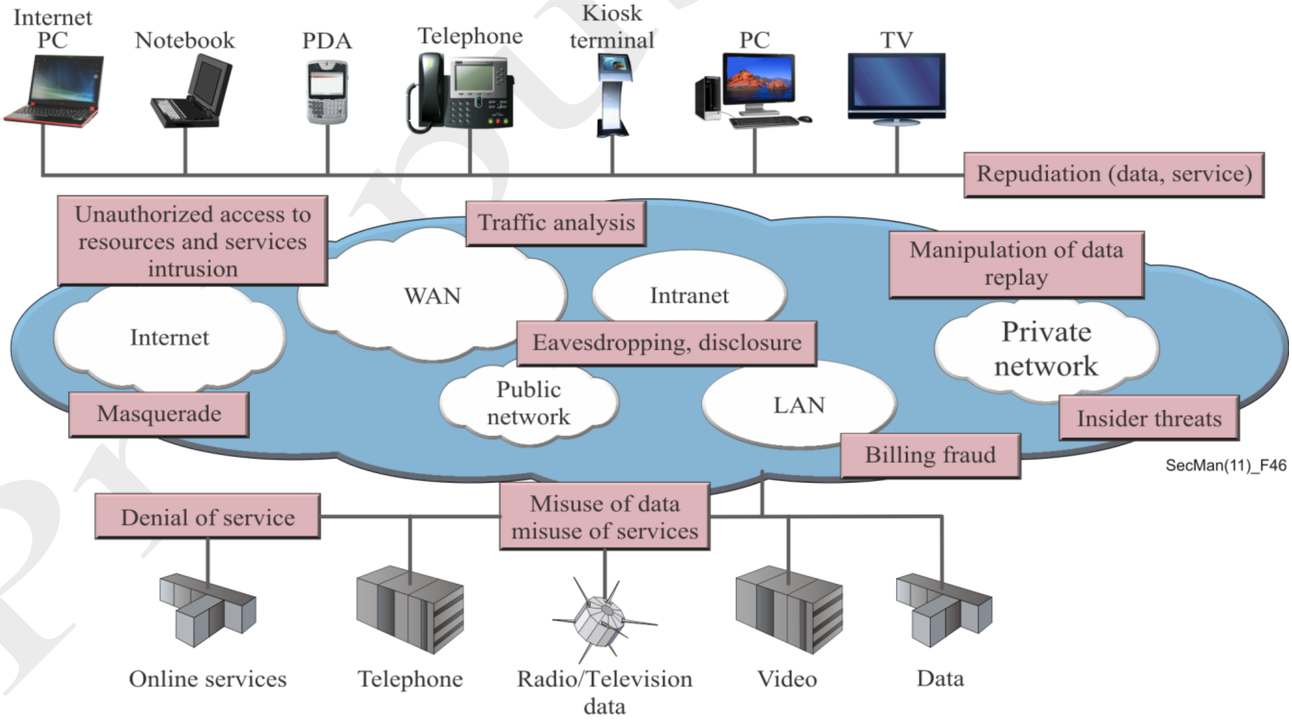


Figure 75 – Security threats in multimedia communications

Prepublished

The main security requirements for multimedia communications and IP telephony are as follows:

- User and terminal authentication: VoIP service providers need to know who is using their service in order to correctly account for, and possibly bill the service usage. As a prerequisite for the authentication, the user and/or the terminal have to be identified. Then a user/terminal has to prove that the claimed identity is in fact the true identity. This typically occurs through strong cryptographic authentication procedures (e.g., protected password or ITU-T X.509 digital signatures);
- Server authentication: Since VoIP users typically communicate with each other through some VoIP infrastructure that involves servers, gateways and possibly multicast techniques, both fixed and mobile users need to know if they are talking with the proper server and/or with the correct service provider;
- User/terminal and server authentication: This is needed to counter security threats, such as masquerade, man-in-the-middle attacks, IP address spoofing and connection hijacking;
- Call authorization: This is the decision-making process to determine if the user/terminal is actually permitted to use a service feature (e.g., calling into the PSTN) or a network resource. Most often authentication and authorization functions are used together to make an access control decision. Authentication and authorization help to thwart attacks like masquerade, misuse and fraud, manipulation and denial-of-service;
- Signalling security protection: This addresses protection of the signalling protocols against manipulation, misuse, confidentiality and privacy. Signalling protocols are typically protected by using encryption as well as by integrity and replay protection measures. Special care has to be taken to meet the critical performance requirements of real-time communication to avoid any service impairment due to security processing;
- Voice and other media confidentiality: This is realized through encryption of the packets (to protect against eavesdropping) of multimedia applications. Advanced protection of media packets also includes authentication/integrity protection of the transmitted packets;
- Key management: This may be a separate task from the VoIP application (password provisioning) or may be integrated with signalling when security profiles with security capabilities are being dynamically negotiated and session-based keys are to be distributed; and
- Inter-domain security: This addresses the problem where systems in heterogeneous environments have implemented different security features because of different needs, different security policies and different security capabilities. As such, there is a need to dynamically negotiate security profiles and security capabilities such as cryptographic algorithms and their parameters. This becomes of particular importance when crossing domain boundaries and when different providers and networks are involved. An important security requirement for the inter-domain communication is the ability to traverse firewalls smoothly and to cope with constraints of network address translation (NAT) devices.

This list is not comprehensive but covers core security for Recommendation ITU-T H.323. Security issues that are considered outside the scope of Recommendation ITU-T H.323 include security policy, network management security, security provisioning, implementation security, operational security and security incident handling. Security requirements for multicast communication are addressed in Recommendation ITU-T X.1101.

Pre-published

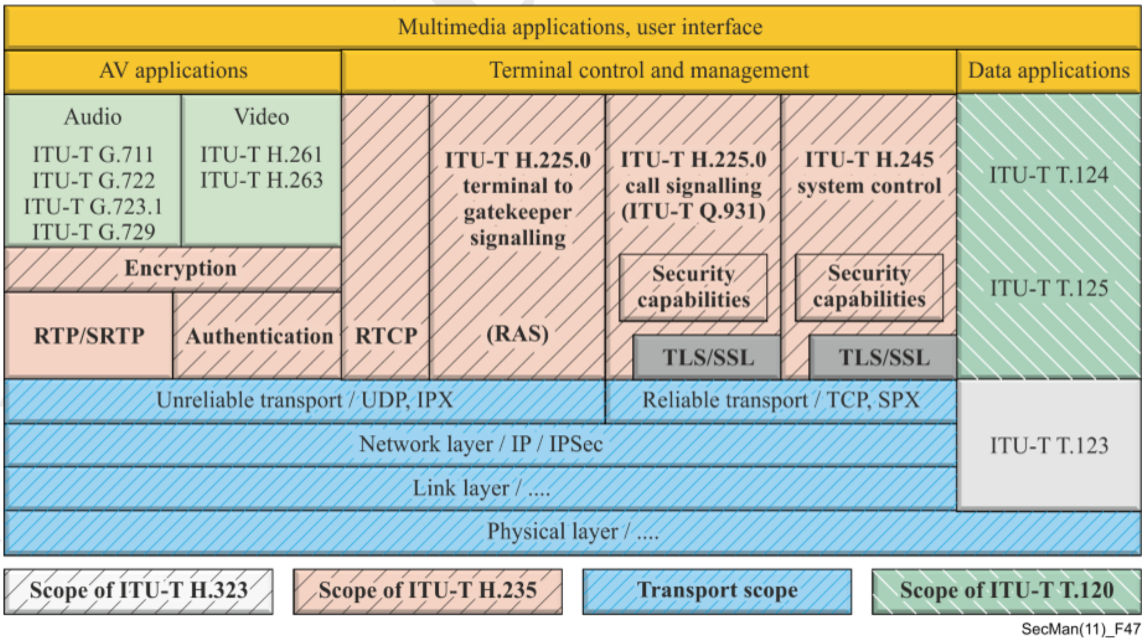
12.1.2 Overview of the ITU-T H.235.x sub-series Recommendations

The ITU-T H.235.x series of Recommendations provide specification of the security mechanisms and protocols plus detailed guidance on implementing security in the ITU-T H.323 series of Recommendations. They provide scalable security solutions for small groups, enterprises and large-scale carriers and provide cryptographic protection of the control protocols as well as the audio/video media stream data.

The ITU-T H.235.x series provides the means to negotiate the required cryptographic services, crypto algorithms and security capabilities. Key management functions for setting up dynamic session keys are fully integrated into the signalling handshakes and thereby help to reduce call set-up latency. Configurations supported include the "classic" point-to-point communication as well as multipoint configurations with multicast units where several multimedia terminals communicate within a group.

The ITU-T H.235.x series utilizes special optimized security techniques such as elliptic curve cryptography and AES encryption to meet the stringent performance constraints. Encryption, when implemented, is done in the application layer by encrypting the RTP/SRTP payloads. This allows implementation with a small footprint in the endpoints through tight interaction with the digital signal processor and the compression codecs without dependency on a specific operating system platform.

Figure 76 shows the scope of ITU-T H.235.x series, which encompasses provisions for setting up calls (ITU-T H.225.0 and ITU-T H.245 blocks) and bidirectional communication (encryption of RTP/SRTP payloads containing compressed audio and/or video). Security mechanisms for authentication, integrity, privacy, and non-repudiation are included. Gatekeepers are responsible for authentication by controlling admission at the endpoints, and for providing non-repudiation mechanisms. Security on transport and lower layers, based on IP, is beyond the scope of ITU-T H.323 and ITU-T H.235.x, but is commonly implemented using the IP security (IPSec) and transport layer security (TLS) protocols. Where required, IPSec or TLS can be used to provide authentication and, optionally, confidentiality at the IP layer transparent to whatever (application) protocol runs above. The negotiation of confidentially mechanisms may be detected via the use of the secure ITU-T H.323 Annex O URI schema or negotiated during call setup by the mechanisms described in ITU-T H.460.22.



NOTE – The scope of H.235.x also covers RTP and SRTP.

Figure 76 – Security in ITU-T H.323 as provided by ITU-T H.235.x

Published

Pre-published

The ITU-T H.235.x-series Recommendations encompass a wide palette of security measures that address different target environments (e.g., intra/inter-enterprise and carriers) and that can be customized and scenario-specific, depending on local factors such as the available security infrastructure and terminal capabilities (e.g., simple endpoints vs. intelligent endpoints).

The available security profiles provide security techniques that range from simple shared-secret profiles, including protected password, to more sophisticated profiles with digital signatures and Recommendation ITU-T X.509 PKI certificates (ITU-T H.235.2). This allows for either hop-by-hop protection, using the simpler but less scalable techniques, or end-to-end protection using the scalable PKI techniques. Recommendation ITU-T H.235.3 is called the hybrid security profile as this Recommendation combines symmetric security procedures from Recommendation ITU-T H.235.1 and PKI-based certificates and signatures from Recommendation ITU-T H.235.2 thereby achieving optimized performance and shorter call-set time. Recommendation ITU-T H.235.4 provides security measures towards securing a peer-to-peer model. It also defines procedures for key management in corporate and in inter-domain environments.

In order to provide stronger security for systems using personal identification numbers (PINs) or passwords to authenticate users, Recommendation ITU-T H.235.5 provides another "*Framework for secure authentication in RAS using weak shared secrets*" by using public-key methods to secure use of the PINs/passwords. Recommendation ITU-T H.235.6 collects all the procedures that are necessary to achieve native H.323 encryption of the RTP media stream including the associated key management.

Recommendations ITU-T H.235.7 and ITU-T H.235.8 describe SIP interoperable mechanisms over SRTP media streams utilising the MIKEY and SDES key exchange mechanisms respectively. Detection and sharing authentication with other elements (such as gateways) in the IP network is covered in Recommendation ITU-T H.235.9.

Secure user and terminal mobility in distributed ITU-T H.323 environments is covered in Recommendation ITU-T H.530, which addresses security aspects such as:

- mobile terminal/user authentication and authorization in foreign visited domains;
- authentication of visited domain;
- secure key management; and
- protection of signalling data between a mobile terminal and visited domain.

Recommendation ITU-T H.235.0 provides the overall security framework for H-series multimedia systems. Recommendation ITU-T H.235.0 and the ITU-T H.350 series of Recommendations provide for scalable key management using the Lightweight Directory Access Protocol (LDAP) and Secure Socket Layer (SSL/TLS). In particular, the ITU-T H.350 series provides capabilities that enable enterprises and carriers to manage large numbers of users of video and voice-over-IP services securely along with a way to connect Recommendation ITU-T H.323, SIP, Recommendation ITU-T H.320 and generic messaging services into a directory service, so that modern identity management practices can be applied to multimedia communications.

12.1.3 Network address translation and firewall devices

The Internet was designed with the "end-to-end" principle in mind. That is, any device on the network may communicate directly with any other device on the network. However, due to concerns about security and a shortage of IPv4 network addresses, firewall (FW) and network address translation (NAT) devices are often employed at the boundary of networks. These boundaries include the residence domain, service provider domain, enterprise domain, and sometimes country domain. Within a single domain, more than one firewall or NAT device is sometimes employed. Firewall devices are designed to control how information moves across network boundaries and are usually configured to block most IP communications. Unless a firewall is explicitly configured to allow Recommendation ITU-T H.323 traffic from external devices to pass through to reach internal Recommendation ITU-T H.323 devices, communication is simply not possible. This poses a problem for any user of Recommendation ITU-T H.323 equipment.

NAT devices translate addresses used within the internal domain into addresses used in the external domain and vice versa. Addresses used within a residential or enterprise domain are generally, though not always, assigned from the private network address spaces defined in IETF RFC 1918. Those are:

Class	Address Range	Number of IP addresses
A	10.0.0.0 – 10.255.255.255	16,777,215
B	172.16.0.0 – 172.31.255.255	1,048,575
C	192.168.0.0 – 192.168.255.255	65,535

NAT devices pose an even more frustrating problem for most IP protocols, especially those that carry IP addresses within the protocol. Recommendation ITU-T H.323, SIP, and other real-time communication protocols that operate over packet-switched networks must provide IP address and port information so that the other parties in the communication will know where to send media streams (e.g., audio and video streams).

The NAT/FW traversal issues are addressed in a series of the ITU-T H.460 series of Recommendations that allow Recommendation ITU-T H.323 communications to traverse one or more NAT/FW devices seamlessly. Those Recommendations are: ITU-T H.460.17; ITU-T H.460.18; ITU-T H.460.19; ITU-T H.460.23; ITU.T H.460.24 and ITU.T H.460.26.

Figure 77 depicts how a special "proxy" device might be used to aid NAT/FW "unaware" devices to properly traverse the NAT/FW boundary.

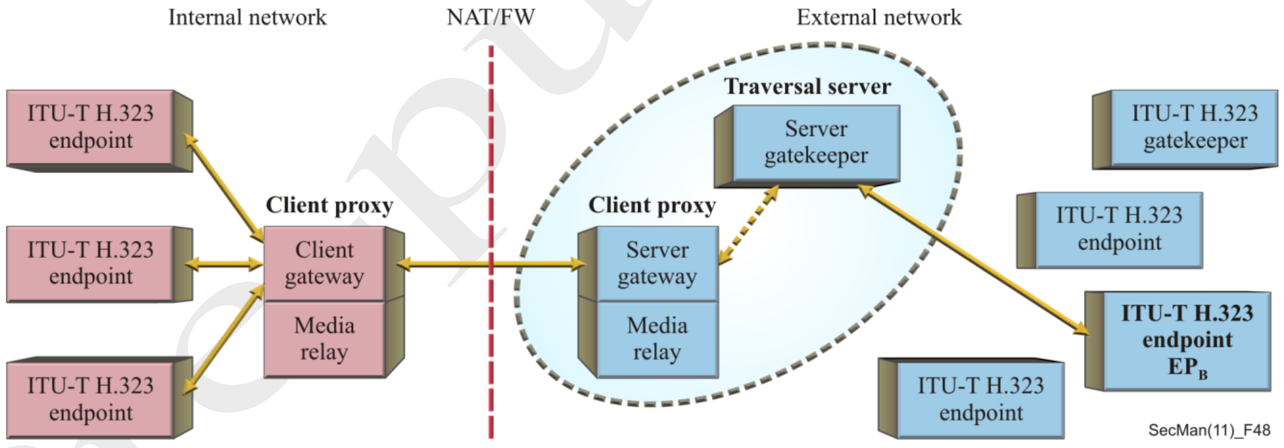


Figure 77 – NAT/FW traversal in ITU-T H.460.18 architecture

The above topology may be used, for example, where an enterprise wishes to control the route along which Recommendation ITU-T H.323 call signalling and media flows through the network. However, Recommendation ITU-T H.460.17 and Recommendation ITU-T H.460.18 also allow endpoints to traverse NAT/FW boundaries without the aid of any special internal "proxy" devices. Figure 78 depicts one such topology:

Prepublished

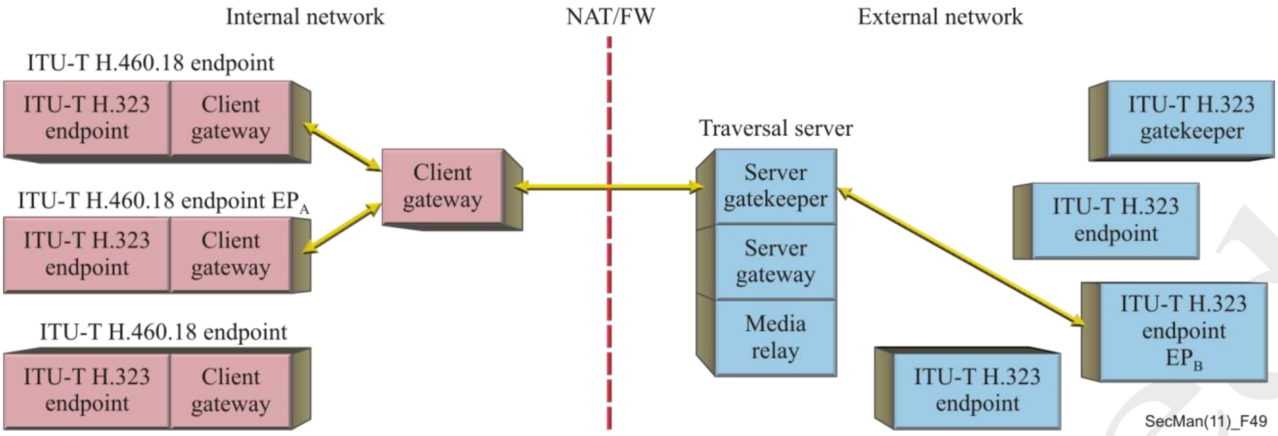


Figure 78 – Gatekeeper communication architecture

In Figure 78 the endpoints on the internal network communicate with the internal network gatekeeper to resolve the address of the external entities (e.g., a phone number or ITU-T H.323 URL to an IP address). The internal network gatekeeper communicates with an external network gatekeeper to exchange that addressing information and conveys that information back to the calling endpoint. When a device within the internal network places a call to a device in the external network, it will use procedures defined in Recommendation ITU-T H.460.18 to open necessary "pin holes" through the NAT/FW devices to get signalling from the internal network to the external network. Further, it will use procedures defined in Recommendation ITU-T H.460.19 to open necessary "pin holes" to allow media streams to properly traverse the internal network to the external network and vice versa. For security reasons, there may be a strict limit on the number of "pin holes" permitted in the NAT/FW device. ITU-T H.460.19 clause 7.2 describes a method for permitting multiple media streams to utilise the same "pinhole".

When the calling and called devices reside in different private networks separated by NAT/FW devices and the public Internet, at least one "server gateway" and one "media relay" device (defined in Recommendation ITU-T H.460.18) is necessary in order to properly route signalling and media between the two private networks. This combination of devices is commonly referred to as a "Session Border Controller". The reason is simply that, by design, there is no way an IP packet within one private network can enter another private network without the aid of some entity in the public network to help "proxy" that packet.

When using ITU-T H.460.19, media must be routed via an ITU-T H.460.19 media relay residing outside the NAT/FW device. ITU-T H.460.23 and ITU-T H.460.24 further expand the reach of ITU-T H.460.17, ITU-T H.460.18 and ITU-T H.460.19 by permitting, where possible, media to travel directly between ITU-T H.323 devices therefore negating the requirement of an ITU-T H.460.19 media relay. ITU-T H.460.23 describes the process by which the NAT/FW device is probed for behavioural characteristics, and ITU-T H.460.24 then goes on to use that information to describe a logical methodology for plotting a possible direct media solution. Figure 79 details the procedures to establish direct media flows using ITU-T H.460.23 and ITU-T H.460.24.

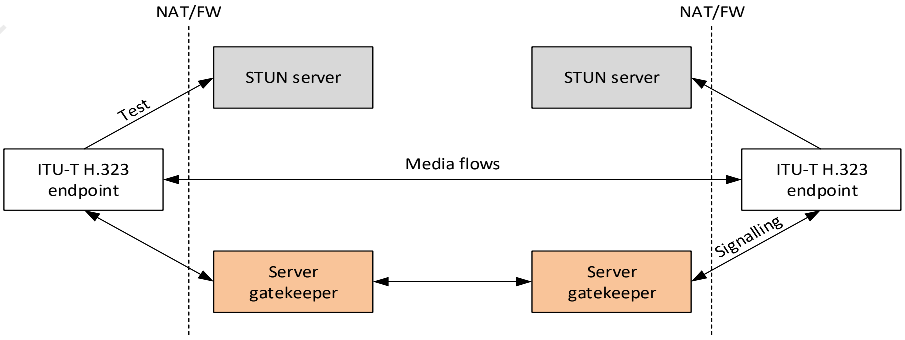


Figure 79 – Sample call flow through double NAT/FW

Under conditions where access from within a NAT/FW is restricted further to a very small number of TCP ports, ITU-T H.460.26 describes a method for tunnelling all signalling and media messages over a single TCP port.

12.2 Internet protocol television (IPTV)

Security provisions for Internet protocol television (IPTV) must cover protection of the content delivered through IPTV services, the terminal devices used, and the provision of such services.

For IPTV, content protection means ensuring that an end user can use the content only in accordance with the rights granted by the rights holder. This includes protecting contents from illegal copying and distribution, interception, tampering and unauthorized use.

Protection of IPTV terminal devices includes ensuring that the device employed by an end user to receive the service can reliably and securely use content, enforce the content usage rights, and protect the integrity and confidentiality of content as well as critical security parameters such as cryptographic keys.

IPTV service protection includes ensuring that end-users can acquire only the service and the content that they are entitled to receive. It also includes protecting the service against unauthorized access.

A number of IPTV-specific security Recommendations have been approved. Recommendation ITU-T X.1191 defines the general security architecture for IPTV as shown in Figure 80. Note that only those functions that apply to the end-user, the network provider and the service provider are considered within the scope of the Recommendation. Functions relating to the content provider are subject to private agreements between the stakeholders and are considered out of scope of this Recommendation.

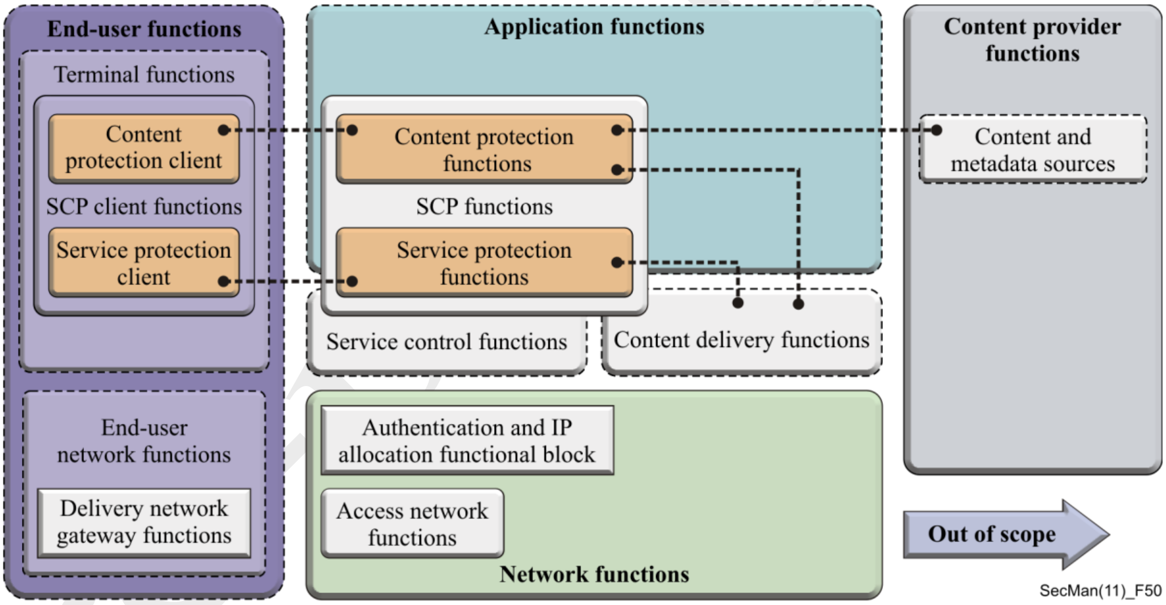

End-user functions
Terminal functions
Content protection client
SCP client functions
Service protection client
End-user network functions
Delivery network gateway functions
Application functions
Content protection functions
SCP functions
Service protection functions
Service control functions
Content delivery functions
Authentication and IP allocation functional block
Access network functions
Network functions
Content provider functions
Content and metadata sources
Out of scope
SecMan(11)_F50

Figure 80 – General security architecture for IPTV

12.2.1 Mechanisms for protecting IPTV content

Security mechanisms that can be used to protect content include:

- content encryption;
- watermarking (e.g., the use of steganography to alter certain content features without such alteration being readily detectable);
- content tracing identification and information to facilitate investigation into unauthorized content access and use;

Pre-published

- content labelling (such as rating information to allow some degree of end-user control over access to inappropriate content); and
- secure transcoding (which permits intermediate network nodes to transform multimedia content to a different format or quality without decryption, thereby preserving end-to-end security).

12.2.2 Mechanisms for protecting IPTV service

Service protection mechanisms include:

- authentication of the end-user (subscriber) and/or terminal device;
- authorization (to make sure the end-user or terminal is authorized to access the services and/or content); and
- access control (particularly to ensure that content that is uploaded from a client to a server can be accessed only by an authorized service provider).

A number of Recommendations have been developed to support IPTV security. Recommendation ITU-T X.1192 defines functional requirements and mechanisms for the secure transcodable scheme of IPTV. Recommendation ITU-T X.1195 defines general requirements for interoperable service and content protection (SCP) between multiple SCP mechanisms. Recommendation ITU-T X.1196 provides a framework for the downloadable SCP scheme in the mobile IPTV environment. It also describes the functional architecture and requirements for the downloadable SCP scheme for roaming in the mobile IPTV environment. Recommendation ITU-T X.1193 defines a key management framework for secure IPTV services. Recommendation ITU-T X.1197 provides guidelines on the criteria for selecting cryptographic algorithms for IPTV SCP, including in the post-quantum context. It also provides a list of cryptographic algorithms to provide confidentiality, data origin authentication, and integrity for IPTV SCP services. Recommendation ITU-T X.1198 specifies a virtual machine-based security platform for renewable SCP under IPTV services.

12.2.3 Protection of subscriber information

A particular concern when implementing IPTV is the need to protect subscriber information which may include tracked data information such as channel number before and after a channel change, time of change, user information for the electronic program guide service, package identification, time of play, etc. This data must be considered sensitive and measures must be taken to prevent unauthorized disclosure via the terminal, the network or the service provider. Suggestions for protecting subscriber information are contained in an annex to Recommendation ITU-T X.1191.

12.2.4 Rights information interoperability

Recommendation ITU-T H.751 is technically aligned with IEC 62698 and gives the high-level specification of the metadata for rights information interoperability, including representation of the minimum required elements. The rights information interoperability (RII) metadata provide descriptive and contextual classification for representing rights information using the permission framework. RII is concerned with finding the greatest common denominators in rights expressions that include the minimum required components when trying to implement the mutual use of rights information.

This Recommendation defines the common semantics and core elements of rights information interoperability for IPTV systems and/or equipment that require multimedia content to be legally used across different platforms.

The rights information includes rights- and security-related metadata that is described in Recommendation ITU-T H.750. This Recommendation describes rights-related information, such as holder ID, content ID, user ID and digital rights permissions, is used to bridge between rights-related metadata, see Figure 81. The

Pre-published

Recommendation does not specify, however, what rights management and content protection technologies should be used. In this sense, it provides a tool to assist in the implementation of content protection mechanisms.

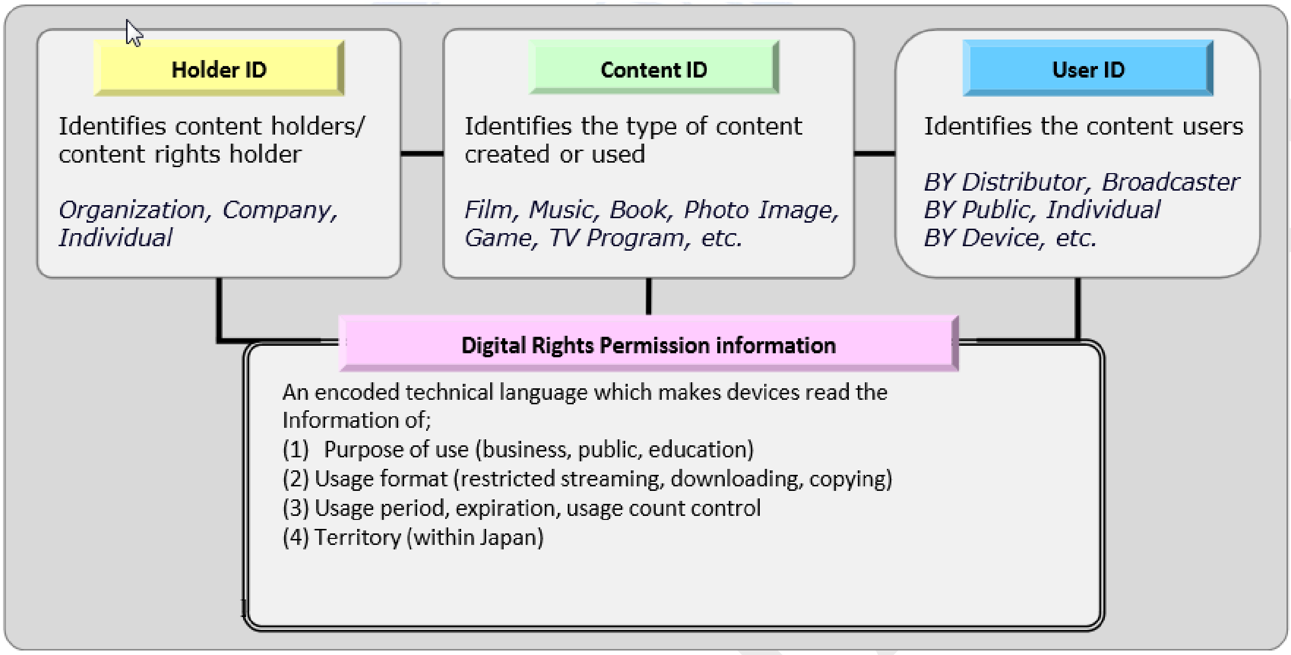

Holder ID
Identifies content holders/ content rights holder
Organization, Company, Individual
Content ID
Identifies the type of content created or used
Film, Music, Book, Photo Image, Game, TV Program, etc.
User ID
Identifies the content users
BY Distributor, Broadcaster
BY Public, Individual
BY Device, etc.
Digital Rights Permission information
An encoded technical language which makes devices read the Information of;
(1) Purpose of use (business, public, education)
(2) Usage format (restricted streaming, downloading, copying)
(3) Usage period, expiration, usage count control
(4) Territory (within Japan)

Figure 81 – RII sets of information

RII metadata can be encoded using various representations, for example XML or binary encoding (such as found in IEC 62227). While XML allows easier reading and management, binary encoding is more compact and efficient, hence suitable for embedded systems (such as TV sets).

Two examples of practical use of ITU-T H.751 for digital broadcasting and for music distribution:

- RII-compliant coding of broadcasting materials, including ad material IDs are now part of the Japanese standard for digital radio broadcasting ISDB-Tsb.
- RII is used for watermarking copyright information in a high-quality audio service (96 kHz/24 bits) in Japan that sells jazz, blues, and soul content owned by members of the Recording Industry Association of Japan via a physical medium. Legal protection is assured by watermarking and the RII mechanism, instead of using digital rights management (DRM).

Guidance is provided on tamper detection during the content distribution process, on secrecy of the distribution format data representing digital rights permissions. It also describes use in 23 use-cases scenarios.

12.3 Digital rights management (DRM) for Cable Television Multiscreen

Rapid deployment of smart-phones and tablet devices is changing the way people watch television, whether at home or outdoors. *TV Everywhere* services, including IP Linear and IP VOD, will inevitably increase the traffic of media streaming and downloading over IP networks that enable both in-home and outdoor services. DRM technology is required for content right protection based on device authentication.

Current DRM is an aggregation of different technologies and each DRM closely depends on the rights of the content holder. Standardized DRM architecture and requirements are highly recommended to enable cable operators to deploy new services in keeping with the content holder's. Such rights should extend to a cable customer's multiple devices.

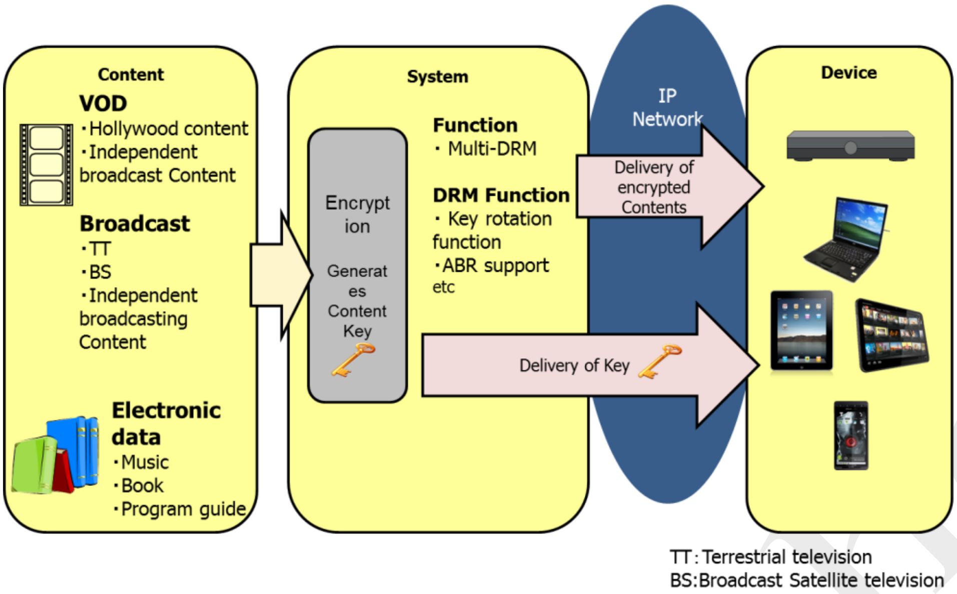


Figure 82 – One aspect of DRM for cable television IP video service

As shown in Figure 82, there are three aspects for DRM, content, head-end and end terminal device. The DRM function itself is independent from content delivery network structures. Generally the raw contents (content that has not been encrypted and mostly supplied by content provider) are entered into the platform. After the authentication of cable customer and customer's end terminal devices by Identity Provider function in the platform, the DRM server encrypts the content. The encrypted contents are distributed to a customer's end terminal devices over the content delivery network and cable network. The content key is encrypted for secure key delivery and distributed separately from the contents. The end terminal device which has a DRM license can only decrypt the content by using the distributed content key and the device key of end terminal device.

12.3.1 Cable platform and DRM

Content right protection is becoming increasingly important due to various types of content, distribution of hi-quality movies, enhancement of user experiences and change of media procurement style. The DRM system offers a content right protection method that can be applicable different service environments. By exchanging license information between the customer terminal device and the DRM system, the terminal device can decrypt content encrypted by the DRM system. It is anticipated that the platform provider will select, install and maintain the DRM system, however a service provider (SP) and a cable operator could also take the place of the platform provider.

Figure 83 depicts DRM related functional components from content provisioning to content distribution for end terminal devices. The content is mainly provided by the content provider (CP) and supplied to the cable platform via a dedicated network. The cable platform is operated by a platform provider. The SP delivers content between the cable platform and cable operator, and cable operator distributes the content to the customer's end terminal devices. In Figure 83, DRM functions (content packaging, encryption, license distribution, etc.) are provided in the cable platform, however this is simply an example and the DRM function can be actually installed either in the SP server or cable operator's server. The license distribution sequence (including DRM message data, etc.) for DRM service must be transmitted securely between the cable platform and the end terminal devices in accordance with the requirements of each DRM system.

Pre-published

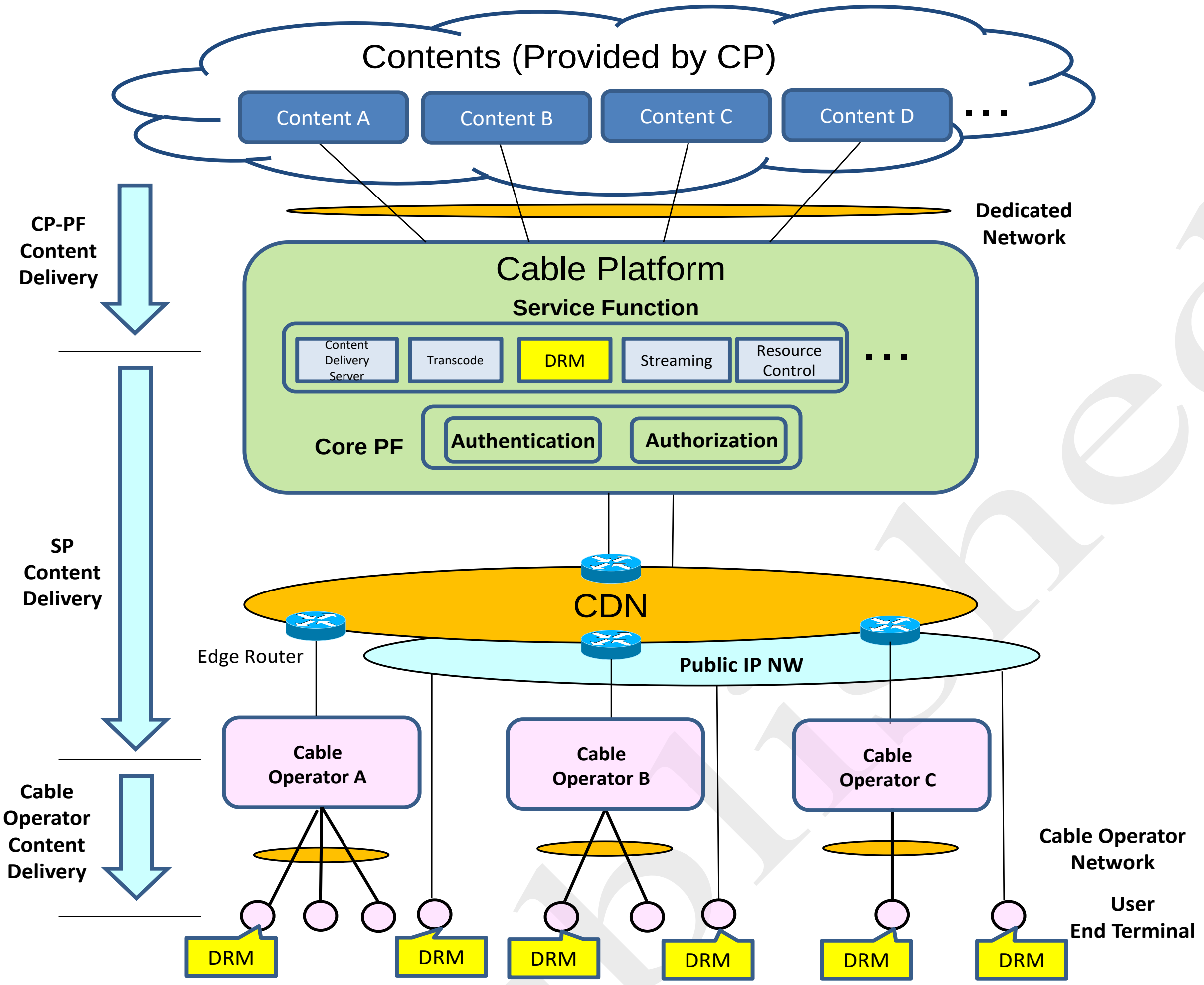


Figure 83 – Cable platform and DRM

Before commencing cable service (including content delivery), user authentication and service authorization are mandatory at the cable platform. The SP then makes a judgement regarding the delivery of content (e.g. confirmation of exclusive control condition for simultaneous viewing) following which the SP selects the content delivery method and the DRM system, encrypts the content, and sends the content to the cable operator’s headend system. The content is delivered to subscriber’s end terminals (set top box (STB), PC, tablet, smart-phone, etc.) via the cable operator’s network. The SP delivers a license with a pre-determined timing and delivery method. Only the end terminal with the licence can decrypt the content. The subscriber can view the content.

The timing of license delivery depends on the DRM system and its usage scenario. Various DRM scenarios are available in the present content market in which DRM offers license delivery before content distribution, after content distribution or every instance of content distribution.

The DRM is required to protect content with encryption between content provider and user end terminals, and must follow the compliance and robustness rules which must be provided by the DRM system supplier.

12.3.2 Service Model

Figure 84 shows an expected service model of IP video content delivery. The video content protected by DRM is delivered to the STB (or other end-terminal) located in the subscriber’s home via the cable platform, the content delivery network and the cable operator’s network. The content can be used for remote services

Pre-published

outdoors and a direct delivery service to outdoor, non-STB end-terminals can be provided via the public IP network using DRM.

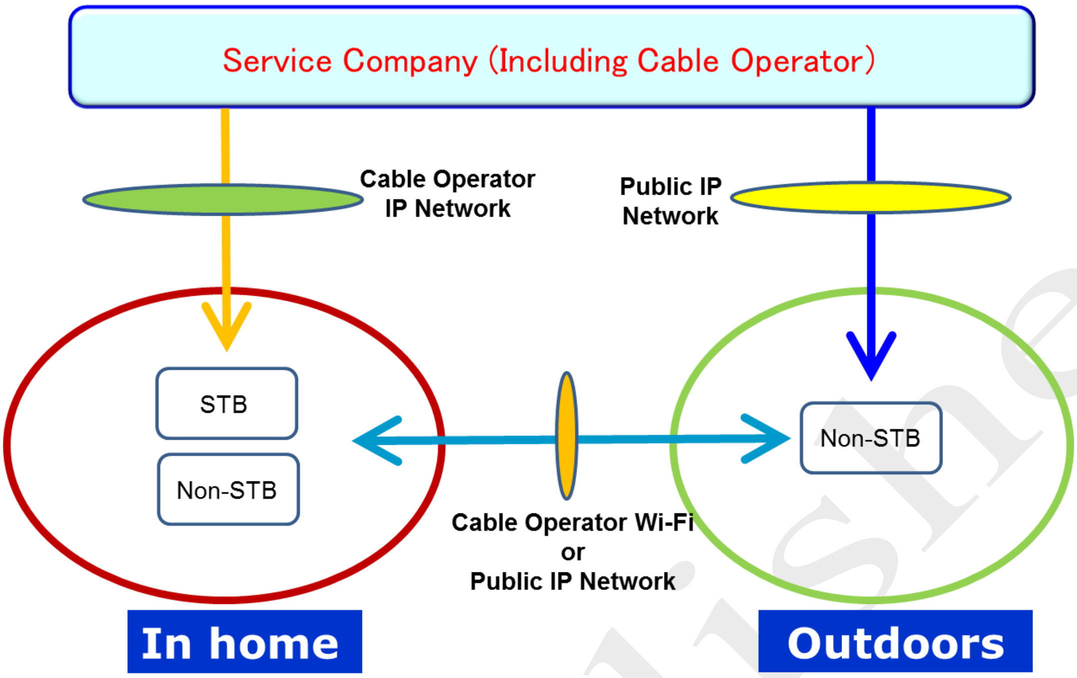

Service Company (Including Cable Operator)
Cable Operator IP Network
Public IP Network
STB
Non-STB
Non-STB
Cable Operator Wi-Fi or Public IP Network
In home
Outdoors

Figure 84 - An expected service model of IP video content delivery

12.3.3 Use cases

Possible basic use-cases for IP video delivery service by a cable operator or SP are categorized in Table 8 and Table 9. Table 8 shows the use-cases for reception and viewing at an end-terminal, without secondary content usage (i.e. remote viewing, copy and move, etc.). Table 9 describes use-cases for content delivery between end-terminals in home or outdoors, with secondary content usage. Table 8 and Table 9 show the example use-cases for possible services based on the service model in Figure 84; This does not exclude other use-cases.

Pre-published

Table 8 – Use-cases for reception and viewing at end-terminal

No.	Style of reception or viewing	Content for delivery	Place of reception or viewing	End-terminal
A-1	Reception of broadcast programme	IP linear content	In-home	STB
				Non-STB
			Outdoors	Non-STB
A-2	Viewing of recorded programme	IP linear content	In-home	STB
				Non-STB
			Outdoors	Non-STB
A-3	Recording of programme	IP linear content	In-home	STB
				Non-STB
			Outdoors	Non-STB
A-4	Exchanging End-terminal	IP linear content	In-home	STB to Non-STB
				Non-STB to STB
				Non STB to Non STB
			Outdoors	Non STB to Non STB
A-5	Streaming viewing	IP VOD Content	In-home	STB
				Non-STB
			Outdoors	Non-STB
A-6	Viewing after download	IP VOD Content	In-home	STB
				Non-STB
			Outdoors	Non-STB
A-7	Downloading	IP VOD Content	In-home	STB
				Non-STB
			Outdoors	Non-STB

Pre-pu d

Table 9 – Use-cases for content delivery between end-terminals in-home or outdoors

No.	Transmission Method	Content for delivery	Place of reception or viewing	End-terminal
B-1	Streaming	Recorded IP linear content	In-home	STB to Non-STB
			In-home	Non-STB to STB
			In-home	Non-STB to Non-STB
		Recorded IP VOD content	In-home	STB to Non-STB
			In-home	Non-STB to STB
			In-home	Non-STB to Non-STB
B-2	Remote streaming	Recorded IP linear content	Outdoors	STB to Non-STB
			In-home	Non-STB to STB
			Outdoors	Non-STB to Non-STB
		Recorded IP VOD content	Outdoors	STB to Non-STB
			In-home	Non-STB to STB
			Outdoors	Non-STB to Non-STB
B-3	Copy	Recorded IP linear content	In-home	STB to Non-STB
			In-home	Non-STB to STB
			In-home	Non-STB to Non-STB
		Recorded IP VOD content	In-home	STB to Non-STB
			In-home	Non-STB to STB
			In-home	Non-STB to Non-STB
B-4	Move	Recorded IP linear content	In-home	STB to Non-STB
			In-home	Non-STB to STB
			In-home	Non-STB to Non-STB
		Recorded IP VOD content	In-home	STB to Non-STB
			In-home	Non-STB to STB
			In-home	Non-STB to Non-STB

12.4 Secure fax

Facsimile remains a popular application but confidence in fax services is highly dependent on the effectiveness of in-built security measures. Initially, fax standards were developed for transmission over the PSTN (Recommendation ITU-T T.4) and then for ISDN (Recommendation ITU-T T.563). More recently, extensions were specified for fax transmission in real time over IP networks (including the Internet) (Recommendation ITU-T T.38) and via store-and-forward systems (Recommendation ITU-T T.37).

Regardless of the mode of transmission, the security issues faced by fax services include confidentiality of the data transmitted, authentication, and non-repudiation. These issues have become even more important as traffic has moved to the Internet due to the open and distributed characteristics of the medium.

Fax security is addressed in Recommendation ITU-T T.36, which defines two independent technical solutions that may be used for encrypting the documents exchanged. One option specified is to use the *Rivest, Shamir & Adleman* (RSA) cryptographic algorithm; the other method uses a combination of *Hawthorne Key Management* (HKM) and *Hawthorne Facsimile Cipher* (HFX). Security services defined are:

- mutual authentication (mandatory);
- security service (optional), which includes mutual authentication, message integrity, and confirmation of message receipt;
- security service (optional), which includes mutual authentication, message confidentiality (encryption), and session key establishment; and

- security service (optional), which includes mutual authentication, message integrity, confirmation of message receipt, message confidentiality (encryption), and session key establishment.

The combination of *Hawthorne Key Management* (HKM) and *Hawthorne Facsimile Cipher* (HFX) systems provide the following capabilities for secure document communications between entities:

- mutual entity authentication;
- secret session key establishment;
- document confidentiality;
- confirmation of receipt; and
- confirmation or denial of document integrity.

12.5 Web services

Web technologies including service-oriented architectures (SOA) are being widely applied as they enable efficient and cost-effective development and deployment of new services and integration of content from a variety of sources to form composite services easily and rapidly. There are many security aspects of web services. Authentication and single sign-on (SSO) mechanisms are required as well as security mechanisms to support mobile web services.

Economies of scale have driven computing platform vendors to develop products with highly-generalized functionality, so that they can be used in the widest possible range of situations. These products are delivered with the maximum possible privilege for accessing data and executing software, so that they can be used in as many application environments as possible, including those with the most permissive security policies. Where a more restricted security policy is required, the platform's inherent privileges must be constrained, by local configuration.

The security policy of a large enterprise has many elements and many points of enforcement. Elements of policy may be managed by different parts of the organization (e.g. IT staff, security staff, human resources, legal services etc) and from different points of enforcement (e.g. via the extranet, the WAN or via remote-access systems). It is common for each point of enforcement to be managed independently.

The use of a common language for expressing security policy allows the enterprise to manage the enforcement of all elements of its security policy in all the components of its information systems. Managing security policy may include some or all of the following steps: writing, reviewing, testing, approving, issuing, combining, analyzing, modifying, withdrawing, retrieving and enforcing policy.

In addition, a framework for exchanging security information is needed. To facilitate these exchanges, mark-up languages, including the Security Assertion Markup Language and the eXtensible Access Control Markup Language (XACML) have been developed. These were originally developed by OASIS but have now been adopted and published by the ITU-T with the assistance of OASIS.

12.5.1 Security Assertion Markup language

Recommendation ITU-T X.1141 defines the Security Assertion Markup Language (SAML 2.0). SAML is an XML-based framework for exchanging security information. This security information is expressed in the form of *assertions* about *subjects*, where a subject is an entity that has an identity in some security domain. A single assertion might contain several different internal statements about authentication, authorization and attributes.

Typically there are a number of *service providers* that can make use of assertions about a subject in order to control access and provide customized service, and accordingly they become the relying parties of an asserting party called an *identity provider*.

Pre-published

Recommendation ITU-T X.1141 defines three different kinds of assertion statements that can be created by a SAML authority. All SAML-defined statements are associated with a subject. The three kinds of statement defined in ITU-T X.1141 are:

- authentication: The assertion subject was authenticated by a particular means at a particular time;
- attribute: The assertion subject is associated with the supplied attributes; and
- authorization decision: A request to allow the assertion subject to access the specified resource has been granted or denied.

Recommendation ITU-T X.1141 also defines a protocol by which clients can request assertions from SAML authorities and get a response from them. This protocol, consisting of XML-based request and response message formats, can be bound to many different underlying communications and transport protocols. In creating their responses, SAML authorities can use various sources of information, such as external policy stores and assertions that were received as input in requests.

A set of profiles has been defined to support single sign-on (SSO) of browsers and other client devices. Figure 85 illustrates the basic template for achieving SSO.

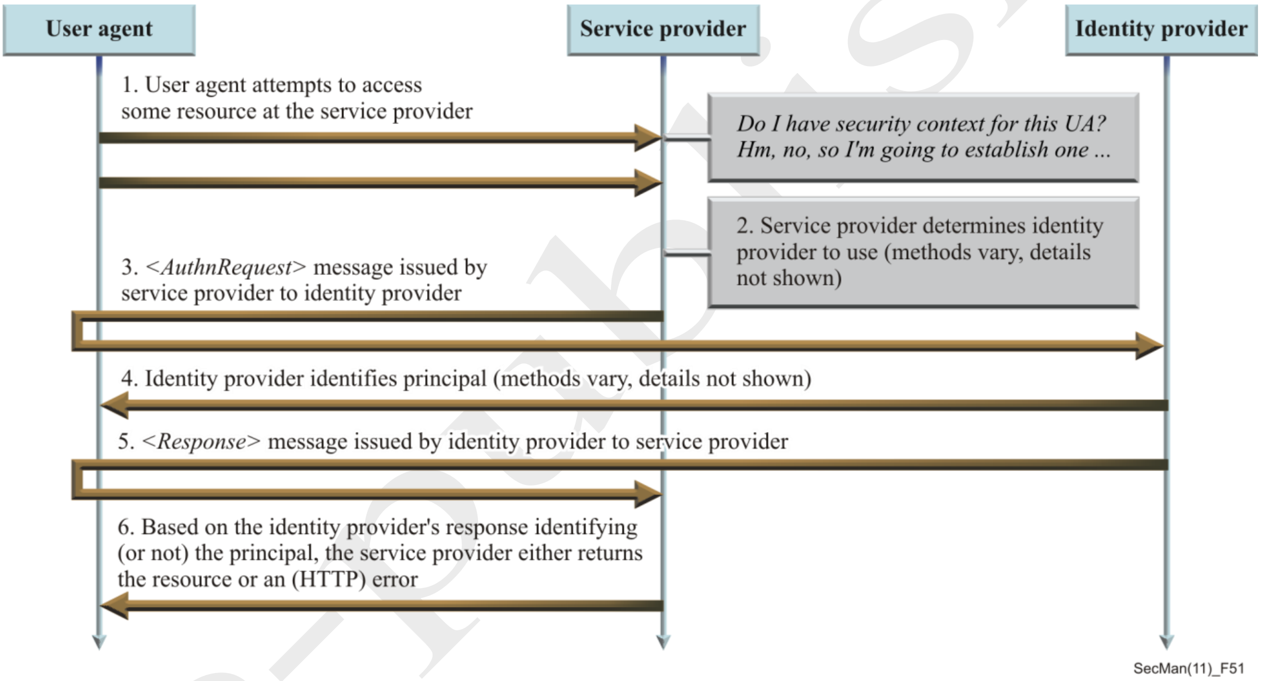

User agent
Service provider
Identity provider
1. User agent attempts to access some resource at the service provider
Do I have security context for this UA? Hm, no, so I'm going to establish one ...
2. Service provider determines identity provider to use (methods vary, details not shown)
3. <AuthnRequest> message issued by service provider to identity provider
4. Identity provider identifies principal (methods vary, details not shown)
5. <Response> message issued by identity provider to service provider
6. Based on the identity provider's response identifying (or not) the principal, the service provider either returns the resource or an (HTTP) error
SecMan(11)_F51

Figure 85 - Basic template for achieving SSO

12.5.2 Extensible access control markup language

The eXtensible Access Control Markup Language (XACML) is an XML vocabulary for expressing access control policies. Access control consists of deciding if access to a requested resource should be allowed and enforcing that decision. Recommendations ITU-T X.1142 and ITU-T X.1144 define core XACML including syntax of the language, models, context with policy language model, syntax and processing rules. To improve the security of exchanging XACML-based policies, Recommendations ITU-T X.1142 and ITU-T X.1144 also specify an XACML XML digital signature profile for securing data. A privacy profile is specified in order to provide guidelines for implementers. XACML is suitable for a variety of application environments.

Recommendation ITU-T X.1144 (which is equivalent to OASIS XACML 3.0 (01/2013)) improves the features regarding custom categories, content element, XACML request and response, and XML path. In addition, this

Pre-published

Recommendation defines new datatypes and functions: advice element, policy combination algorithms, scope of XPath expressions, target element, variables in the obligation and advice element.

12.6 Tag-based services

Identification tags (including RFID tags) are being widely deployed but concern is growing over the risk of privacy infringement. This is partly because RFID technology can automatically collect and process data and there is a risk of deliberate or accidental disclosure of sensitive and/or personal information.

For applications that use, or rely on, tag-based identification in applications that involve personal information, such as healthcare, passports and driver's licences, the privacy issue is becoming an increasingly serious problem.

In academia and industry, most of the efforts toward a protection mechanism for personally-identifiable information (PII) have focused on authentication protocols between the ID tag and the ID terminal. However, such efforts do not address the issue completely as meaningful information about the identifier still exists on the server in the network domain. One solution to this problem is to use a profile-based PII protection mechanism.

Recommendation ITU-T X.1171 examines threats to PII in a business-to-customer (B2C)-based environment in which applications use tag-based identification. It identifies requirements for the protection of PII in such environments and specifies PII protection based on a user-defined PII policy profile.

Business-to-Customer (B2C) applications using tag-based identification can be classified into three types:

a) *Device user as the customer*: In this type of service, the customer retrieves the information by using a mobile reader device. Figure 86Figure 81 shows a basic model of this type of application. It consists of two basic network operations: ID resolution and content retrieval. ID resolution is the procedure of translating or resolving an identifier into an address. The mobile terminal equipped with a reader first resolves an identifier as received from the ID tag via a directory service and then performs content retrieval over the network.

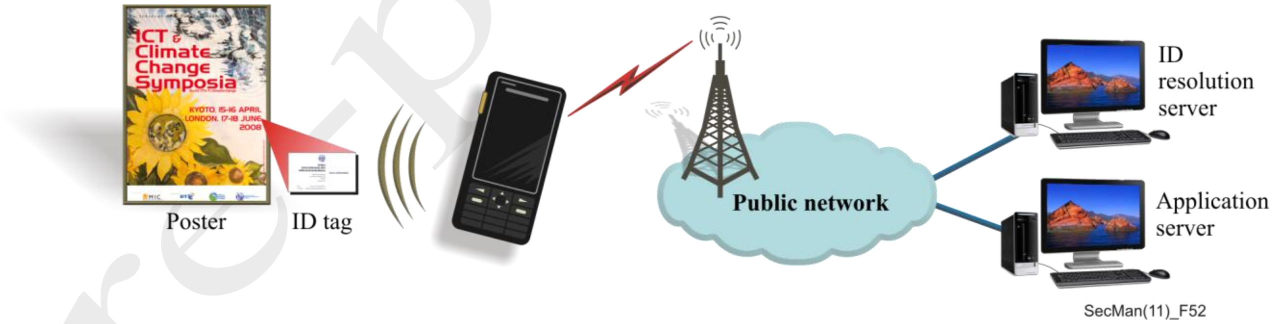


Figure 86 - Basic model of a B2C application using tag-based identification

b) *ID tag user as the customer*: A typical example of this B2C application using tag-based identification deals with access control and/or authentication, e.g., entrance check, passport, license or after-sale management service. In this type of application, reader devices may be incorporated into fixed or mobile terminals. The customer presents the ID tag (e.g. in a passport or on a ticket) in order to receive service.

c) *Customer as both an ID tag user and a device user*: In the product information retrieval service, the customer also becomes a tag user after acquiring the tagged product after browsing the product information using his/her mobile terminal. In another example, a healthcare-related service triggered

Pre-published

by an ID tag-enabled patient card can be considered. In this application, there are many kinds of customers who could be the ID tag user (e.g., patient, doctor, nurse). The ID tag user can browse his/her own patient records through the mobile terminal with a reader device by reading his/her ID tag-enabled patient card.

For B2C applications that use tag-based identification, there are two major risks of PII infringement:

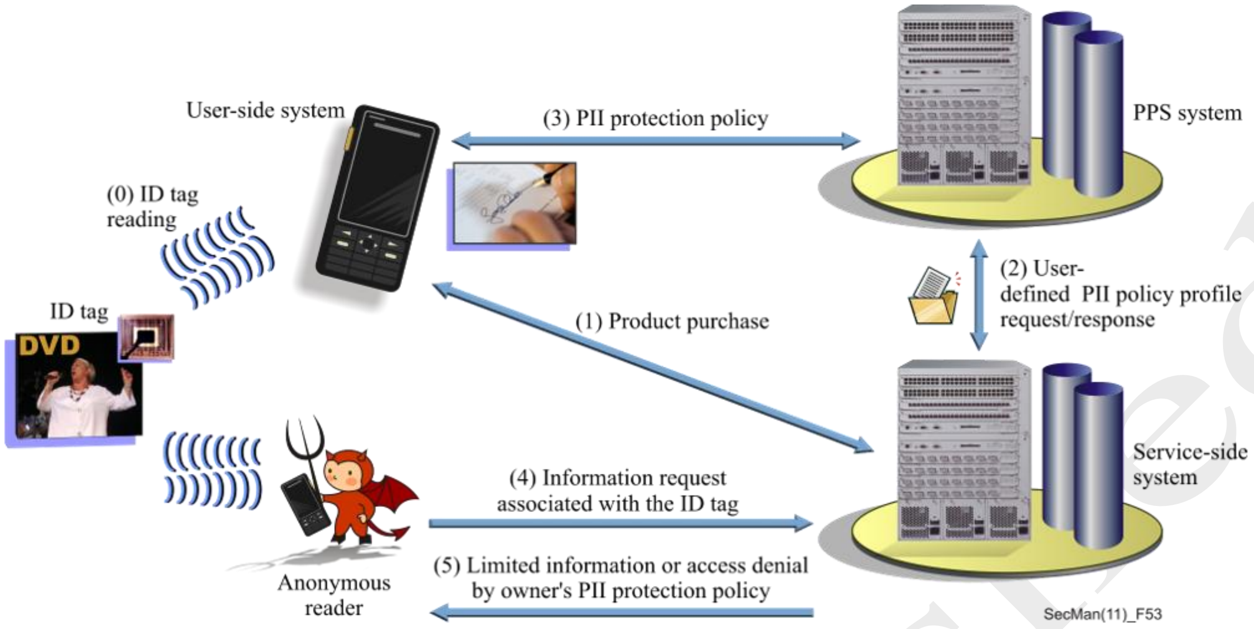
- Leakage of information associated with the identifier: In this instance, an attacker could read information from the ID tag without the knowledge of the user of the tagged product. First, the attacker reads an identifier from an ID tag carried by the user. Then he/she resolves the identifier and queries the information location from the directory service. Finally, the attacker requests for information associated with the ID tag; and
- Leakage of the historical context data: The attacker can extract the user's data (such as preferences, habits, areas of interest, etc.) from the historical context data associated with the ID tag. The attacker could use such data for illegal or commercial purposes without the user's consent.

ITU-T X.1171 describes the following technical requirements to protect PII infringements in B2C applications:

- *Control of PII by ID tag user*: The ID tag user is required to be able to manage or update PII associated with his/her ID tag on the network. In this way, the ID tag user can determine which PII should be deleted or retained in the application;
- *Authentication for ID tag user and/or device user*: The application server is required to provide an authentication procedure for the ID tag user, and the application server may provide an authentication procedure for the user of the device if necessary (some applications using tag-based identification are not required to authenticate the user);
- *Access control to the PII of an ID tag user in an application server*: The application server is required to control access to the relevant information related to the PII of the ID tag user;
- *Data confidentiality of information associated with an ID tag*: The application server is required to provide data confidentiality to ensure that the information associated with an ID tag cannot be read by unauthorized users; and
- *Consent for collection of device user-related log data*: The application server may provide a consent procedure for the collection of device user-related log data if this type of log data collection is necessary for the application.

The following example illustrates a PII protection service (PPS) based on the user's PII policy profile. The service scenario for the PPS generally arises from a tag-personalizing procedure such as tagged product purchase. Figure 87 illustrates the general PPS service flow of the application using tag-based identification.

Pre-published


User-side system
(0) ID tag reading
ID tag
DVD
(3) PII protection policy
PPS system
(2) User-defined PII policy profile request/response
(1) Product purchase
Service-side system
(4) Information request associated with the ID tag
(5) Limited information or access denial by owner's PII protection policy
Anonymous reader
SecMan(11)_F53

1) A consumer reads the identifier from the tagged product using his/her mobile terminal equipped with a reader.
2) The consumer browses the product-related information from the application service network and subsequently purchases the product using one of various payment methods. At this moment, the consumer becomes the ID tag user.
3) The application using tag-based identification then requests the user-defined PII policy profile from the PPS system, which responds with the user-defined PII profile to the application.
4) The PPS system receives the user's PII protection policy profile for this application.
5) Anyone may request the information associated with this ID tag from the service-side system.
6) The requestor can browse all information provided by the service-side system if the requestor is the ID tag user. Otherwise, either the requestor cannot access any information or obtains only limited information.

Figure 87 - General PII protection service (PPS) service flow

12.7 Value-added services

As the development of network and user-terminal capability progresses, more and more telecommunications operators are providing various services based on their network resources to the users. These services are called value-added services as they add the additional value to basic telecommunication services such as voice call, short message service (SMS), multimedia messaging service (MMS) and data access. Typical value-added services include mobile office automation, e-reading, e-commerce, etc. The structure of value-added services is shown in Figure 88.

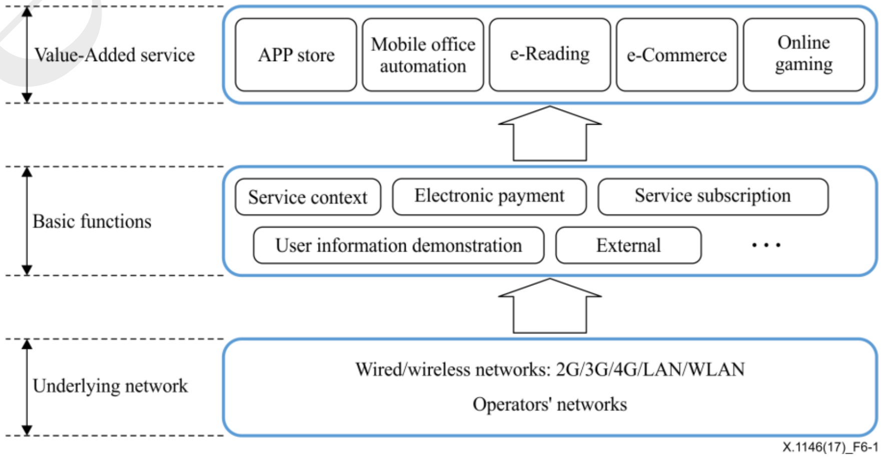


Figure 88 - Structure of value-added services

Pre-published

In many cases, the value-added services will involve sensitive operations or critical data, which will be the target of malicious attackers. Recommendation ITU-T X.1146 analyzes service scenarios, provides security threats and attack methods to the scenarios, and provides technical measures to counter threats and attacks for value-added services provided by telecommunication operators.

Table 10Table 11 shows the typical scenario and related threats for value-added services described in Recommendation ITU-T X.1146.

Table 10 – The threats and protection measures related to typical scenarios for value-added services

Scenario	Threats	Countermeasures
•User identity authentication	•Fake identity •False authentication •Authentication result tampering •Session attack	•Encryption by network protocol or industry-accepted algorithms •Inputs and URL check •Password masking with “*”, etc
•Subscription service	•Subscription information tampering •Subscription repudiation	•Using authentication code (CAPTCHA) •Second confirmation method, etc
•Payment for service	•Payment amount tampering •Payment bypass	•Two-step verification •Abnormality monitoring, etc.,
•User information demonstration	•Revelation on terminal •Transmission interception •Information acquisition without authorization	•Masking sensitive data when displayed on a terminal •Auditing the query and modification operations, etc.,
•Application interface to the external platform	•Illegal input •Replay attacks	•Black/white list of source of data input into API •Discarding abnormal parameter input, etc.,
•Password retrieval	•Evidence tracking •Evidence forgery •Authentication on the user-side	•Restrictions on using of simple password •Secure session ID •Measures to avoid replay attack, etc.,

Recommendation ITU-T X.1146, provides following basic protection measures that can be used to ensure the security of value-added services.

– Confirm measures: Critical operations in the service process should be re-confirmed to prevent unauthorized operation with a different authentication method from the one used for user authentication.

– Tamper-proof measures: A tamper-proof encryption measures should be used to protect the information exchanged between the user- and server-side, especially key data.

– Information check measures: All data input from the outside should be validated, filtered and encoded before it is used by the service system.

– System analysis measures: Analysis measures should be taken to identify service abuses that the above protection measures cannot prevent.

- Session security measures: To protect user sessions, the service system should provide appropriate session ID and session cookie.
- User information protection measures: In the process of displaying, using and storing user information, the following protection measures should be taken to prevent user information leakage.
- User-side application restriction measures: Due to security uncertainties concerning the user-side, some key operations, such as user information authentication and API-based interaction should not be executed on the user-side.
- Interaction protection measures: To prevent replay attacks, message transmissions between the user-side and server-side should adopt a measures such as time-stamp or sequential number.

This Recommendation provides secure protection guidelines for value-added services provided by telecommunication operators. This will help the operators to assure the security of the value-added service and will also protect the users' benefits.

Pre-published

13. Countering common network threats

Pre-published

13 Countering common telecommunication threats

Threats to computer systems, the networks that link them and the telecommunication services/applications are many and varied. Although many attacks can be initiated locally, the vast majority of attacks today are conducted via communications networks. The fact that vast and increasing numbers of computers and network devices are connected to the Internet and operated from homes and workplaces by people with little training, awareness or knowledge of IT security greatly increases the ease and probability of remote, often indiscriminate, attacks. Spam, spyware, viruses and other attack vectors are released in ever greater numbers. The attackers often rely on weak and inadequately protected systems as conduits for their malware.

In this section, an overview of the work of the ITU-T to respond to some of these threats is presented.

13.1 Spam

Spam is any unsolicited, unwanted or potentially harmful message. While the most widely recognized form of spam is e-mail spam, the term also applies to other forms such as instant messaging spam, mobile messaging spam, and VoIP spam. In fact, its meaning is evolving and broadening with the development of technologies that provide novel opportunities to create spam. Spam is recognized as a widespread problem that interferes with legitimate operations of telecommunication operators, service providers and users. It consumes bandwidth and processing cycles and, in extreme cases, can result in denial of service attacks by flooding networks. No single anti-spam measure is effective on its own and, given the agility and resourcefulness of spammers, even a combination of measures often proves effective only to the extent of reducing the volume of spam. Examples of measures being used include: regulation; technical measures; international cooperation; and education of users and Internet service providers.

13.1.1 Technical strategies on countering spam

The ITU-T work on spam focuses primarily on technical counter-measures. Recommendations are being developed using a framework that allows for extensibility as illustrated in Figure 89.

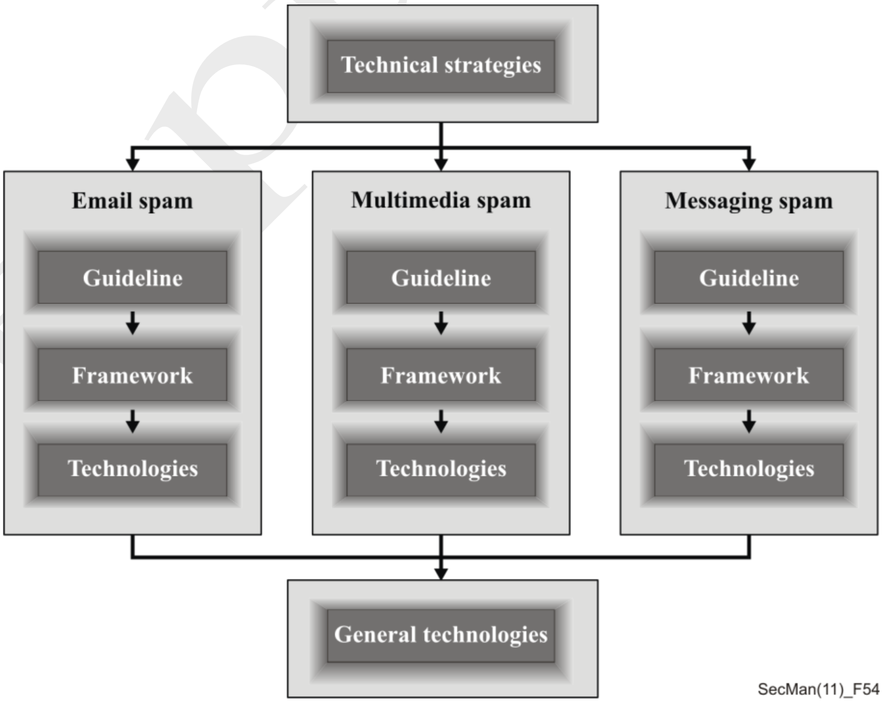


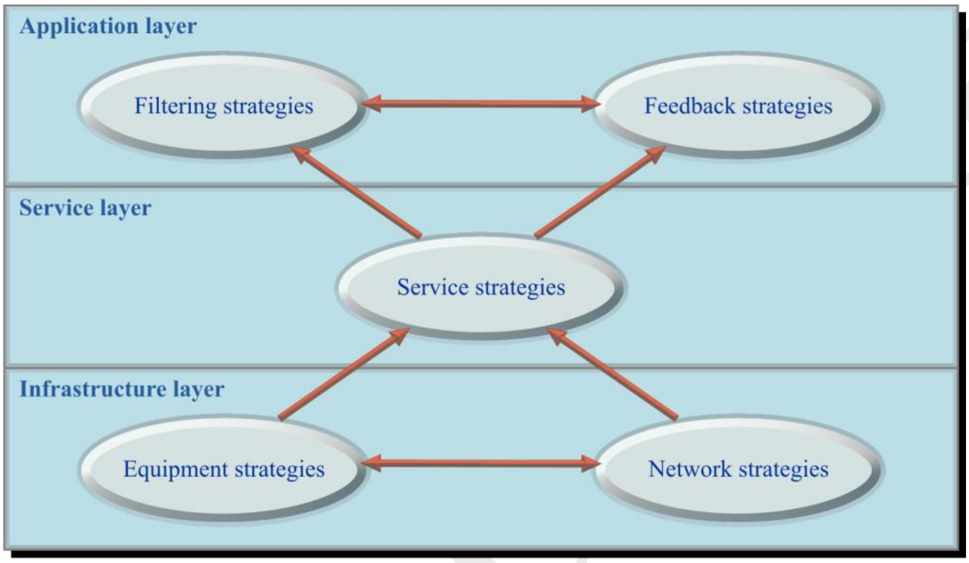
Figure 89 - Standardization framework for countering spam

Prepublished

Pre-published

Recommendation ITU-T X.1231 sets out requirements for combating spam and serves as a starting point for the work. This Recommendation describes the different types of spam and its common characteristics and provides an overview of technical approaches to counter spam. It also proposes a general model that can be used to develop an effective anti-spam strategy.

This model is hierarchical and has five strategies distributed across three layers. The relationships between the strategies are illustrated in Figure 90. The model indicates that there is a high degree of interdependence between the strategies but that cost considerations may preclude use of all strategies in individual cases. Also, customization is necessary according to the particular application scenario.



SecMan(11)_F55

Figure 90 - General model for countering spam

13.1.2 E-mail spam

The most widely recognized form of spam is e-mail spam. It presents complex technical challenges, and solutions to eliminating it need to be supported by appropriate technical measures. While government action and legislation are helpful, they are insufficient to meet the challenges posed by e-mail spam. The issue is complicated by the difficulty of identifying the spammer when the SMTP protocol is used.

Two Recommendations are designed to assist in countering e-mail spam. Recommendation ITU-T X.1240 is directed towards users who want to develop technical solutions for countering e-mail spam. It specifies basic concepts, characteristics, effects, and the technical issues associated with countering e-mail spam. It also identifies current technical solutions and related activities from standards development organizations and other groups that are working on countering e-mail spam.

Recommendation ITU-T X.1241 describes a recommended structure for an anti-spam processing domain and defines the functionality of the major modules in the domain. The framework establishes a mechanism to share information about e-mail spam between different e-mail servers. It aims to promote greater cooperation between service providers in tackling spam. In particular it provides a framework for enabling a communication methodology for alerts on identified spam. Another document, *Supplement 6 to the ITU-T X-series of Recommendations* reviews international fora where spam is being addressed and includes a case study.

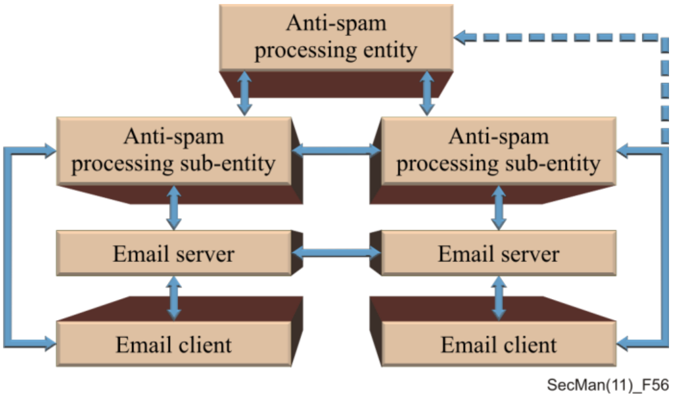

Anti-spam processing entity
Anti-spam processing sub-entity
Anti-spam processing sub-entity
Email server
Email server
Email client
Email client
SecMan(11)_F56

Figure 91 - General structure of e-mail anti-spam processing domain

Figure 91 illustrates the processes of the Recommendation ITU-T X.1241 framework. The anti-spam processing entity is located in an independent system while the sub-entities are located in one or more e-mail service providers. The processing entity delivers new rules to the sub-entities which must verify and refine the rules. A function also exists to resolve any conflicts in the rules.

13.1.3 IP multimedia spam

Recommendation ITU-T X.1244 specifies the basic concepts, characteristics, and technical issues related to countering spam in IP multimedia applications such as IP telephony and instant messaging. The various types of IP multimedia application spam are categorized, and described according to their characteristics. The standard describes various spam security threats that can cause IP multimedia application spam and identifies the aspects that should be considered in countering such spam. Some of the techniques developed to control e-mail spam can also be used in countering IP multimedia application spam. Recommendation ITU-T X.1244 analyzes the conventional spam-countering mechanisms and discusses their applicability to countering IP multimedia application spam.

Anti-spam techniques for IP multimedia spam can be applied according to the particular characteristics of the spam. Table 11 shows the classification used in Recommendation ITU-T X.1244.

Table 11 – Classification of IP multimedia application

	Text	Voice	Video
Real-time	• Instant messaging spam • Chat spam	• VoIP spam • Instant messaging spam	• Instant messaging spam
Non Real-time	• Text/multimedia message spam • Text spam over P2P file sharing service • Website text spam	• Voice/multimedia message spam • Voice spam over P2P file sharing service • Website voice spam	• Video/multimedia message spam • Video spam over P2P file sharing service • Website video spam

Recommendation ITU-T X.1245, provides the general framework for countering spam in IP-based multimedia applications such as IP telephony, instant messaging and multimedia conferencing.

Figure 92 illustrates the framework for countering spam in IP-based multimedia applications. The framework consists of four anti-spam functions: core anti-spam functions (CASF); recipient-side anti-spam functions (RASF); sender-side anti-spam functions (SASF); and spam recipient functions (SRF). This Recommendation describes the functionalities and the interfaces of each function for countering IP multimedia spam.

Published

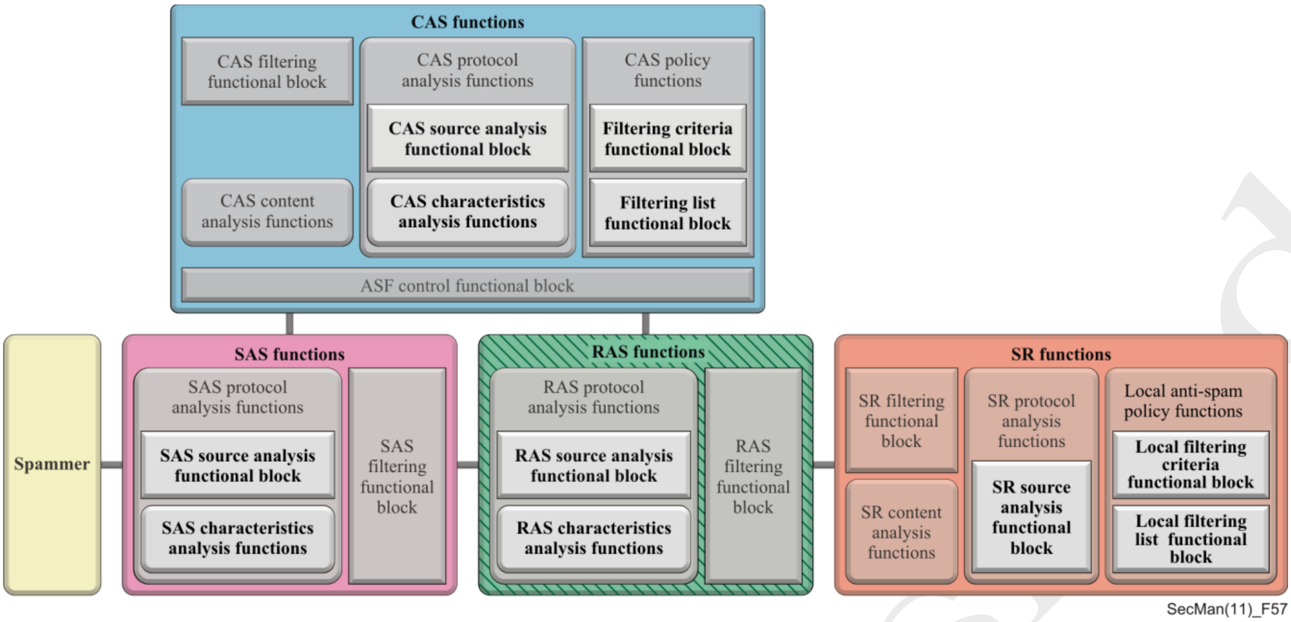

CAS functions
CAS filtering functional block
CAS protocol analysis functions
CAS policy functions
CAS source analysis functional block
Filtering criteria functional block
CAS content analysis functions
CAS characteristics analysis functions
Filtering list functional block
ASF control functional block
Spammer
SAS functions
SAS protocol analysis functions
SAS source analysis functional block
SAS characteristics analysis functions
SAS filtering functional block
RAS functions
RAS protocol analysis functions
RAS source analysis functional block
RAS characteristics analysis functions
RAS filtering functional block
SR functions
SR filtering functional block
SR protocol analysis functions
Local anti-spam policy functions
Local filtering criteria functional block
SR source analysis functional block
SR content analysis functions
Local filtering list functional block
SecMan(11)_F57

Figure 92 - Framework for countering IP media spam

Recommendation ITU-T X.1246, gives an overview of voice spam, and summarizes the existing anti-spam technologies which are used by users and telecommunication networks alike, and the collaboration mechanism between them.

Recommendation ITU-T X.1248 identifies characteristics of spam over instant messaging (SPIM) and specifies technical requirements for countering it.

Recommendation ITU-T X.1249 provides a technical framework for countering mobile in‑application advertising spam. Mobile in-application advertising spam is the sending of unsolicited advertisements, which are displayed within a mobile phone application

Supplement 11 to the ITU-T X-series of Recommendations provides a technical framework based on RBL for countering VoIP spam. Figure 93 illustrates four functional entities for countering VoIP spam: VoIP spam prevention system (VSPS), VoIP spam prevention policy server (VSPPS), RBL central system for VoIP spam prevention (VSP-RBL), and user reputation system (URS). This Supplement also specifies the functionalities, procedures, and interfaces of each functional entity for countering VoIP spam.

Supplement 28 to ITU-T X.1245 is to analyze the threats and to recommend technical measures and mechanisms to counter spoofed calls in the terminating network of voice over long term evolution (VoLTE) if the identity of the incoming calls cannot be trusted securely by the terminating network.

Supplement 33 to ITU-T X.1231 provides an overall technical framework and related best practices for countering telephone service scams.

Pre-published

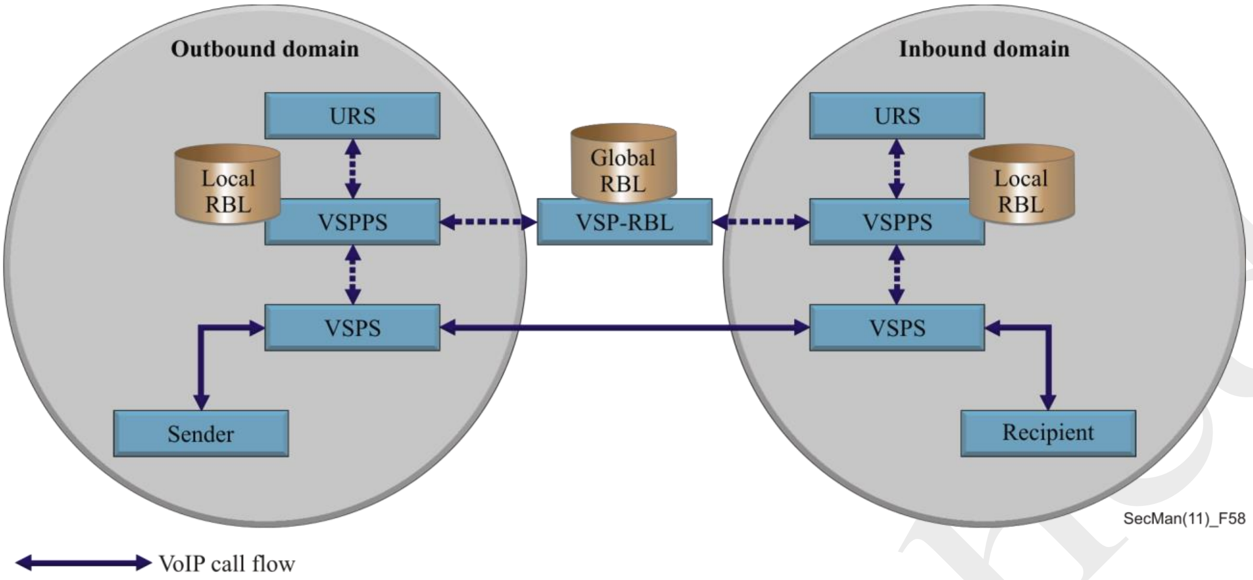


Figure 93 - Functional architecture for countering VoIP spam

13.1.4 Mobile messaging spam

Mobile messaging spam includes both *short message service* (SMS) spam and *multimedia messaging service* (MMS) spam. Recommendation ITU-T X.1242 defines the structure and functions of the SMS spam filtering system along with users' service management, communication protocols and basic functional requirements of terminals with SMS functions. Methods by which users can manage (query, delete and restore) filtered short messages are defined. Filtering can be based on characteristics such as address, telephone number, time, or content. Requirements for terminal software to support SMS spam filtering are provided in an appendix to Recommendation ITU-T X.1242.

Recommendation ITU-T X.1247 gives an overview of mobile messaging anti-spam processes and proposes a technical framework for countering mobile messaging spam.

Supplement 12 to ITU-T X-series Recommendations, in particular to Recommendation ITU-T X.1240, describes the basic concept and characteristics of mobile messaging spam. Supplement 29 to Recommendation ITU-T X.1242 provides universal guidelines on short message service (SMS) phishing by defining a security guideline about security technology against SMS phishing incident and method, and specification of report contents.

13.1.5 Interactive gateway system for countering spam

Technology collaboration has been recognized as a key component in countering spam. Recommendation ITU-T X.1243 illustrates such a system and specifies a technical means for countering inter-domain spam. The gateway system enables spam notification among different domains and prevents spam traffic from passing from one domain to another. In addition, this Recommendation specifies the architecture for the gateway system, describes basic entities, protocols and functions of the system, and provides mechanisms for spam detection, information sharing and specific actions for countering spam.

13.2 Malicious code, spyware and deceptive software

Systems and networks are arguably at greatest risk from malicious code (viruses, worms, Trojans, etc.) but spyware and other deceptive software (e.g., software that performs unauthorized activities) also pose significant risk. Unless organizations and individuals implement a range of proactive measures (including

Pre-published

firewalls, anti-virus measures and anti-spyware measures) against these threats, compromise is virtually assured. However, available countermeasures vary in effectiveness and are not always complementary.

Regulators in many countries are increasingly demanding assurances from service providers regarding the security and safety measures they have taken and requiring the service providers to do more to help users to achieve safe and secure Internet use.

Supplement 9 to the ITU-T X-series of Recommendations provides guidelines for reducing malware in ICT networks.

Recommendation ITU-T X.1207 is a standard to:

a) promote best practices regarding clear notices, user consents and user controls for web hosting services; and

b) promote security best practices (via telecommunication service providers) to home users on safe and secure use of personal computers and the Internet.

Recommendation ITU-T X.1207 provides clear guidance for service providers on security risk management, the use of safe and secure products, network monitoring and response, support, timely updating and secure web hosting. Advice is provided on user guidance and education and technical protective measures for end users. A non-integral appendix provides links to additional resource material.

13.3 Notification and dissemination of software updates

Malicious code can spread with alarming speed and, even with state-of-the art protection measures, new threats can be propagated so rapidly that systems and networks that do not contain the latest updates are vulnerable. Systems are also particularly vulnerable to "zero-day" exploits (i.e., new or previously unknown threats for which no antivirus signature or patch has yet been developed). In this environment, timely distribution and installation of updates is essential. However, there are a number of problems associated with the distribution and implementation of these updates.

Most off-the-shelf software, including operating systems and systems designed to provide security protection (anti-virus, anti-spyware, firewalls, etc.), contains a feature that permits automatic updating. However, this must be enabled by the user. Where a user is simply notified that updates are available (or perhaps that updates have been downloaded) the user must take action to permit the download and/or installation of the updates. Many updates require systems to be rebooted following installation, something that individual users may or may not do immediately. Organizations with a well-managed security program usually manage the updating centrally, forcing updates on end-user systems. In contrast, updating of individual systems (e.g., home computers) and updating within small organizations is generally quite haphazard.

Another concern with routine updating is that software vendors do not use consistent practices for notifying users that updates are available or tell users of the possible consequences of failure to install the updates. Nor do they have a uniform method for keeping users informed of the latest best practices to maintain the security of the software. In addition, there is no consistent method for notification of user-detected problems following implementation of an update.

Recommendation ITU-T X.1206 discusses the difficulties associated with maintaining up-to-date software and provides a vendor-neutral way of addressing the problem. Once an asset is registered, updates on vulnerability information and patches or updates can be automatically made available to users or directly to applications. Recommendation ITU-T X.1206 provides a framework that any vendor can use for notification as well as to provide vulnerability information and disseminate required patches/updates. It also defines the format of the information that should be used in and between components.

Pre-published

ITU-T X.1206 makes it possible for system administrators to know the condition of any asset for which they are responsible. It describes the problems of maintaining assets from an asset identification point of view, as well as from information dissemination and systems/network management points of view. A description of the security that should be considered in the vendor-neutral framework is also provided.

Definitions of the data structures of components that are needed for this work, including the related XML schema, are provided in Recommendation ITU-T X.1206 together with the format of the information that should be used in and between components implementing this framework.

Pre-published

14. Security aspects of cloud computing and big data infrastructure

Pre-published

14 Security aspects of cloud computing and big data infrastructure

An area of rapidly growing interest and importance is that of cloud computing and big data infrastructure. Primary responsibility for developing ITU-T Recommendations relating to cloud computing and big data infrastructure has been assigned to Study Group 13 which has already published a number of Recommendations on this topic. For the most part, standards relating to security associated with cloud computing and big data infrastructure are the responsibility of Study Group 17 though some specific aspects of cloud security are being addressed by Study Group 13. For example, Q19 of SG13 covers end-to-end cloud computing management, including security.

In this section, an overview of the work of ITU-T to respond to the security threats and challenges of cloud computing and big data infrastructure is introduced.

14.1 Overview of cloud computing

Recommendation ITU-T Y.3500 provides an overview of cloud computing along with a set of terms and definitions. Its terminology provides a foundation for cloud computing standards. It also illustrates generic cloud computing capabilities and services, and deployment modes.

14.1.1 Definition of cloud computing

Recommendation ITU-T Y.3500 defines *Cloud computing* as: a Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. (Note: examples of resources include servers, operating systems, networks, software, applications, and storage equipment.)

A *cloud service* is defined as: One or more capabilities offered via cloud computing invoked using a defined interface.

14.1.2 Key characteristics of cloud computing

Although the concept of cloud computing is evolving, Recommendation ITU-T Y.3500 identifies some of the key characteristics which include:

Broad network access, such that users can access physical and virtual resources from wherever they need to work, as long as it is network accessible, using a wide variety of clients including devices such as mobile phones, tablets, laptops, and workstations;

Measured service, such that usage can be monitored, controlled, reported, and billed;

Multi-tenancy, a feature whereby physical or virtual resources are allocated in such a way that multiple users and their computations and data are isolated from and inaccessible to one another;

On-demand self-service, where a cloud service customer can provision computing capabilities, as needed, automatically or with minimal interaction;

Rapid elasticity and scalability, so that physical or virtual resources can be rapidly and elastically adjusted, in some cases automatically, to increase or decrease resources quickly; and

Resource pooling, such that a cloud service provider's physical or virtual resources can be aggregated to serve one or more cloud service customers.

Pre-published

14.1.3 Generic cloud computing capabilities and services

Functionality provided by a cloud service is called a capability. The three capabilities defined in Recommendation ITU-T Y.3500 are:

Application capabilities, in which the cloud service customer can use the cloud service provider's applications;

Infrastructure capabilities, in which the customer can provision and use processing, storage or networking resources; and

Platform capabilities, in which the customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider.

Cloud service categories currently defined are:

- Communications as a Service;
- Compute as a Service;
- Data Storage as a Service;
- Infrastructure as a Service;
- Network as a Service;
- Platform as a Service; and
- Software as a Service.

14.1.4 Deployment models

Cloud deployment models represent how cloud computing can be organized based on the control and sharing of physical or virtual resources. Defined deployment models include:

Public cloud: that may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud service provider;

Private cloud: where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer. A private cloud may be owned, managed, and operated by the organization itself or a third party and may exist on premises or off premises;

Community cloud: where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection; and

Hybrid cloud: which uses at least two different cloud deployment models that remain unique entities but are bound together by appropriate technology that enables interoperability, data portability and application portability. A hybrid cloud may be owned, managed, and operated by the organization itself or a third party and may exist on premises or off premises. Hybrid clouds represent situations where interactions between two different deployments may be needed but remained linked via appropriate technologies.

Pre-published

14.1.5 Emerging cloud services

The cloud computing marketplace is evolving rapidly and is expected to continue to develop as cloud services grow in popularity. Table 12 presents some of the currently-evolving cloud services.

Table 12 – Emerging cloud service categories

Emerging cloud service categories	Capabilities
Database as a Service	The cloud service customer is provided with database functionalities on demand where the installation and maintenance of the databases are performed by the cloud service provider.
Desktop as a Service	The cloud service customer is provided with the ability to build, configure, manage, store, execute, and deliver users' desktop functions remotely.
E-mail as a Service	The cloud service customer is provided with a complete e-mail service including related support services such as storage, receipt, transmission, backup, and recovery of e-mail.
Identity as a Service	The cloud service customer is provided with Identity and Access Management that can be extended and centralized into existing operating environments. This includes provisioning, directory management, and the operation of a single sign-on service.
Management as a Service	The cloud service customer is provided with capabilities that include application management, asset and change management, capacity management, problem management (service desk), project portfolio management, service catalog, and service level management.
Security as a Service	The cloud service customer is provided with an integrated suite of security services within the existing operating environment by the cloud service provider. This may include authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management, among others.

14.2 A security framework for cloud computing

Given the characteristics, the capabilities, the range of services and the deployment models, it is evident that a broad approach to security will be needed to address the potential threats. Topics that must be addressed include a full range of protection measures including physical security, application security, security policy, security management, incident monitoring and response, availability, audit, authentication, authorization, privacy protection, identity management, system and data integrity, confidentiality and protection against various kinds of false repudiation.

Recommendation ITU-T X.1601 presents a security framework for cloud computing. The Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges.

The security threats and challenges in adopting cloud computing, and the security requirements vary to a great extent for different cloud computing service deployment models and service categories. The distributed and multi-tenant nature of cloud computing, the prevalence of remote access to cloud computing services and the number of entities involved in each process make cloud computing inherently more vulnerable to both internal and external security threats than other paradigms. Many of the security threats can be mitigated with the application of traditional security processes and mechanisms. Security touches upon and impacts many parts of a cloud computing service. Therefore, security management of both the cloud computing services and the associated resources is a critical aspect of cloud computing.

The Recommendation advises that before migrating an ICT system to a cloud computing environment, a potential cloud service customer should identify the security threats and security challenges. The risk assessment will enable informed decisions to be made as to whether to adopt cloud computing at all and, if so, which service providers and architecture will be suitable.

14.2.1 Security threats and security challenges to cloud computing

Recommendation ITU-T X.1601 distinguishes between security threats and security challenges. Security threats are those associated with attacks (both active and passive), and also environmental failures or disasters. Security challenges comprise difficulties arising from the nature and operating environment of cloud services. When not properly addressed, security challenges may leave doors open for threats.

Based on these identified security threats and challenges, the security capabilities are described to mitigate security threats and address security challenges for cloud computing. The specific threats encountered are highly dependent on the specific cloud service chosen and threats apply to both cloud service customers and cloud service providers. The respective threats are summarized in Table 13. Table 14 summarizes the security challenges.

Table 13 – Emerging cloud service categories

Threat target	Threat	Example(s)
Cloud service customer	Data loss and leakage	Compromise of encryption keys, authentication codes and access privilege
	Insecure service access	Compromise of Identity credentials
	Insider threats	Careless, accidental or malicious actions on part of staff
Cloud service provider	Unauthorized administration access	Impersonation of authorized administrators
	Insider threats	Careless, accidental or malicious actions on part of staff

Table 14 – Summary of cloud computing security challenges

Security challenges for cloud service customers	Security challenges for cloud service providers	Security challenges for cloud service partners
Ambiguity in responsibility Loss of trust Loss of governance Loss of confidentiality and privacy Service unavailability Cloud service provider lock-in Misappropriation of intellectual property Loss of governance/control Loss of software integrity	Ambiguity in responsibility Shared environment Inconsistency and conflict of protection mechanisms Jurisdictional conflict Evolutionary risks Bad migration and integration Business discontinuity Cloud service partner lock-in Supply chain vulnerability Software dependencies	Ambiguity in responsibility Misappropriation of intellectual property Loss of software integrity

Published

14.2.2 Specific cloud computing security capabilities

A number of security-specific capabilities are defined in Recommendation ITU-T X.1601. These are:

- A common trust model;
- Identity and access management (IAM), authentication, authorization and transaction audit;
- Physical security;
- Interface security;
- Computing virtualization security;
- Network security;
- Data isolation, protection and privacy protection;
- Security coordination;
- Operational security;
- Incident management;
- Disaster recovery;
- Service security assessment and audit;
- Interoperability, portability and reversibility; and
- Supply chain security.

It is intended that the parameters associated with these capabilities be incorporated into service level agreements.

14.2.3 Application of the security framework for cloud computing

The final step in applying the framework defined in Recommendation ITU-T X.1601 is to develop a mapping of the threats and challenges of the selected cloud computing service against the business, technology and regulatory requirements. On completion of this step, it should be possible to identify the particular security controls, policies and procedures that will be needed for a given cloud service. Examples are provided in the Recommendation.

14.3 Cloud computing security design

14.3.1 Security requirements of could service categories

According to Recommendation ITU-T Y.3500, a cloud service category is a group of cloud services that proposes a common set of quantities. Cloud computing offers various service categories, including Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Network as a Service (NaaS), etc. Ensuring the security of these cloud services is paramount to protect sensitive data and maintain the trust of users.

Pre-published

Recommendation ITU-T X.1602, *Security requirements for software as a service application environments*, analyses the maturity levels of Software as a Service (SaaS) application and proposes security requirements to provide a consistent and secure service execution environment for SaaS applications. These proposed requirements originate from cloud service providers (CSP) and cloud service partners (CSN) as they need a SaaS application environment to meet their demands on security. The requirements are general and independent of any service or scenario specific model (e.g. web services, or representational sate transfer), assumptions or solutions.

Network as a Service (NaaS) is one of the cloud service categories in which the capability provided to the cloud service customer (CSC) is transport connectivity and any related network capabilities. Recommendation ITU-T X.1604, *Security requirements of Network as a Service (NaaS) in cloud computing,* analyses security threats and challenges on Network as a Service (NaaS) in cloud computing and specifies security requirements of NaaS in NaaS application, NaaS platform and NaaS connectivity aspects based on corresponding cloud capability types.

Infrastructure as a Service (IaaS) platforms and virtualized services face different, and perhaps more, challenges and threats than traditional information technology infrastructure and application. IaaS platforms that share computing, storage and networking services need protections specific to threats in an IaaS environment. Recommendation ITU-T X.1605, *Security requirements of public Infrastructure as a Service (IaaS) in cloud computing,* documents security requirements of public IaaS in order to help IaaS providers to improve security of the IaaS platform throughout the planning, building and operating stages.

Recommendation ITU-T X.1606, *Security requirements for communications as a service application environments,* identifies security threats and recommends security requirements for communications as a service (CaaS) application environments. The Recommendation describes scenarios and features of CaaS containing multi-communication capabilities. Then it identifies specific threats arising from unique CaaS features and recommends appropriate CaaS security requirements.

14.3.2 Data security requirements for cloud computing

Cloud monitoring data faces similar security threats and challenges that are defined in Recommendation ITU-T X.1601, such as data loss and leakage, insecure service access, unauthorized administration access, etc. Recommendation ITU-T X.1603, *Data security requirements for the monitoring service of cloud computing*, analyses data security requirements for the monitoring service of cloud computing which include monitoring data scope requirements, monitoring data lifecycle, security requirements of monitoring data acquisition and security requirements of monitoring data storage. Monitoring data scope requirements include the necessary monitoring scope that cloud service providers (CSPs) should provide to maintain the cloud security and the biggest monitoring scope of CSPs. Monitoring data lifecycle includes data creation, data store, data use, data migrate, data present, data destroy and data backup. Monitoring acquisition determines the security requirements of the acquisition techniques of monitoring service. Monitoring data storage determines the security requirements for CSPs to store the monitoring data.

14.3.3 Information security management controls for cloud services

The Recommendation ITU-T X.1631|International standard ISO/IEC 27017, as like ITU-T X.1051 and ITU-T X.1058, provides protection guidance when using cloud services based on ISO/IEC 27002.

The use of cloud computing has changed how organizations should assess and mitigate information security risks because of the significant changes in how computing resources are technically provided. The provision and use of cloud services is a kind of supplier relationship, where the cloud service customer is an acquirer, and the cloud service provider is a supplier. In the cloud computing environment, cloud service customer data is stored, transmitted and processed by a cloud service. Therefore, a cloud service customer's business processes can depend upon the information security of the cloud service. Without sufficient control over the cloud service, the cloud service customer might need to take extra precautions with its information security practices.

Pre-published

Pre-published

Before entering into a supplier relationship, the cloud service customer needs to select a cloud service, taking into account the possible gaps between the cloud service customer's information security requirements and the information security capabilities offered by the service. Once a cloud service is selected, the cloud service customer should manage the use of the cloud service in such a way as to meet its information security requirements. In this relationship, the cloud service provider should provide the information and technical support that are necessary to meet the cloud service customer's information security requirements. When the information security controls provided by the cloud service provider are preset and cannot be changed by the cloud service customer, the cloud service customer may need to implement additional controls of its own to mitigate risks.

This Recommendation provides additional cloud-specific implementation guidance for controls in ISO/IEC 27002, for cloud service providers and cloud service customers, respectively. Also, additional controls to address cloud-specific information security threats and risks considerations, the implementation guidance and other information for the controls are provided in Annex A.

The cloud service customers and cloud service providers can refer to ISO/IEC 27002 and this Recommendation | International Standard to select controls with the implementation guidance, and add other controls if necessary. This process can be done by performing an information security risk assessment and risk treatment in the organizational and business context where cloud services are used or provided.

This example illustrates the case where this Recommendation | International Standard applies to an organization both as a cloud service customer and as a cloud service provider. Because cloud service customers and cloud service providers form a supply chain through the design and implementation of the cloud service(s), clause "15.1.3 Information and communication technology supply chain" of ISO/IEC 27002 applies.

Before entering into a supplier relationship, the cloud service customer needs to select a cloud service, taking into account the possible gaps between the cloud service customer's information security requirements and the information security capabilities offered by the service. Once a cloud service is selected, the cloud service customer should manage the use of the cloud service in such a way as to meet its information security requirements. In this relationship, the cloud service provider should provide the information and technical support that are necessary to meet the cloud service customer's information security requirements. When the information security controls provided by the cloud service provider are preset and cannot be changed by the cloud service customer, the cloud service customer may need to implement additional controls of its own to mitigate risks.

14.4 Cloud computing security best practices and guidelines

As cloud computing technology has been developing rapidly, cloud infrastructure has already become an important digital infrastructure that support the development of industries, which carrying a large number of key business systems and important data of the industries. Meanwhile, more and more attackers are launching against cloud infrastructure. To ensure the security of cloud environments, a set of best practices and guidelines have been introduced for cloud service customer (CSC) and cloud service providers (CSP).

Recommendation ITU-T X.1641, *Guidelines for cloud service customer data security*, provides generic security guidelines for the cloud service customer (CSC) data in cloud computing. It analyses the CSC data security lifecycle and proposes security requirements at each stage of the data lifecycle. Furthermore, the Recommendation provides guidelines on when each control should be used for best security practice.

Recommendation ITU-T X.1642, *Guidelines for the operational security of cloud computing*, provides generic operational security guidelines for cloud computing from the perspective of cloud service providers (CSPs). It analyses the security requirements and metrics for the operation of cloud computing. A set of security measures and detailed security activities for the daily operation and maintenance are provided to help CSPs mitigate security risks and address security challenges for the operation of cloud computing.

Virtualization container is partition of a compute node that provides an isolated virtualized computation environment in cloud computing environments. Recommendation ITU-T X.1643, *Security requirements and guidelines for virtualization containers in cloud computing environments*, analyses security threats and challenges for virtualization containers in cloud computing environments and specifies a reference framework with security guidelines for virtualization containers in the cloud.

The distributed cloud is emerging because more and more latency-sensitive services (such as video and Internet of Things services) require much faster response speeds; it is an extension of traditional cloud computing and extends its capabilities further to the edge of the network. It can provide localized cloud services much closer to the customer as well as to the data source, and can interact with other clouds to provide distributed, low latency, high performance services. The distributed cloud comprises the distribution of cloud capabilities types to the edge of the network to enable cloud service with low latency and real-time processing on a limited bandwidth by interworking among a pool of physical or virtual resources. A typical distributed cloud includes the core cloud, regional cloud and edge cloud. Recommendation ITU-T X.1644, *Security guidelines for distributed cloud*, analyses security threats and challenges on distributed cloud and proposes security guidelines against threats to distributed cloud, which includes the security guidelines for core cloud, regional cloud and edge cloud.

Network security situational awareness (NSSA) is derived from situational awareness. For cloud computing service providers, the NSSA platform plays an important role in improving cloud computing's security protection, the ability to detect security breaches or anomalous behaviours, security decision-making and emergency response ability, and it can even help improve the early warning mechanism for cloud computing. Recommendation ITU-T X.1645, *Requirements of network security situational awareness platform for cloud computing*, first introduces the concept and development of NSSA, analyses the advantages of NSSA coping with the security challenges of cloud computing and document the requirements for the NSSA platform for cloud computing.

Blockchain as a service (BaaS) has become mainstream in blockchain development due to its promising capabilities and the extensive support it has received from the industry, especially from top cloud providers. BaaS provides the fundamental service and resources for blockchain applications, however, it faces security challenges arising from both blockchain core technologies and cloud platforms. Guidance on Baas security is thus of great importance and a necessity. Recommendation ITU-T X.1411, *Guideline on blockchain as a service (BaaS) security*, provides generic security guidelines for blockchain as a service (BaaS). The security threats and vulnerabilities of BaaS are first analysed and then the security measures of BaaS are provided. The Recommendation also addresses security requirements and provides guidelines for all the activities in the construction, operation and use of BaaS.

14.5 Virtual measurement systems

Access to the virtualized infrastructure can be both more difficult and more resource intensive for physical measurement systems. Measurement functions also can be virtualized along with network functions. When measurement systems are realized in virtual form, the metrics, models and their methods should change or be augmented. Recommendation Y.1550 provides the key considerations for the design and features of virtual measurement systems (VMSs).

Pre-published

Figure 94 illustrates the case where the existing data flows on a service path will be directed through a VMS. A partial service path is shown, where the packet flows from the wide area network (WAN) enter/leave a host through physical ports (arrows indicate one direction of transmission, but service paths are usually bidirectional).

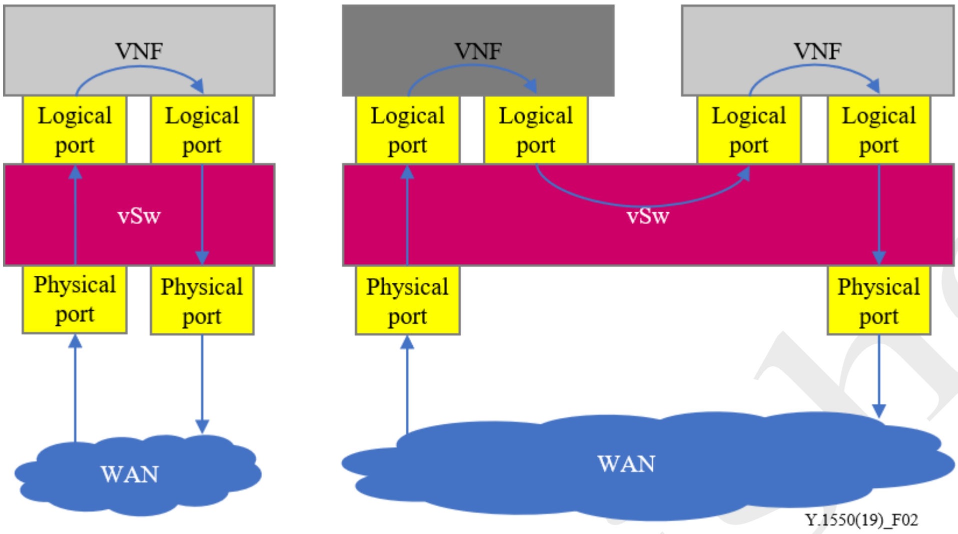


Figure 94 - Example of virtual measurement system (VMS) deployment

There are five study areas for the design and development:

1. **On-demand deployment**: packaging, preferred form of virtualization, positioning, measurement system connectivity, role of software defined networking (SDN) techniques.
2. **Accuracy in deployment**: isolation of the measurement function, mitigation of breaches, trade-offs between accuracy and resource demands, time stamp accuracy considerations.
3. **New opportunities for deployment**: in continuous integration/continuous deployment, (CI/CD) verification testing.
4. **Virtual networking in deployment**: networking needs of measurement systems.
5. **Security**: in collaboration with ITU-T SG17 and Internet Engineering Task Force (IETF).

New methods to characterize the deployment environment and adapt the measurements to better suit the current circumstances are desirable.

14.6 Big data infrastructure security

Big data as a service (BDaaS) is a cloud service category that provides cloud service customers with capabilities to collect, store, analyse, visualize and manage big data, as specified in Recommendation ITU-T Y.3600, *Big data - Cloud computing based requirements and capabilities.* With remarkable growth of data volumes and rapid development of big data business, big data infrastructure has become the central facility to provide BDaaS. Consequently, significant security issues arise for BDaaS. For example, open source big data software design sometimes fails to take security into consideration from the beginning. New technologies introduced by big data analytics can also result in failure of traditional security protection measures. Recommendation ITU-T X.1750, *Guidelines on security of big data as a service for big data service providers*, analyses security challenges BDaaS faces, identifies security roles and responsibilities for provision of BDaaS,

Pre-published

as well as a security framework for a big data infrastructure. It also specifies security protection measures that should be satisfied for services and components related to BDaaS.

With rapid development of big data technology, the value of data has substantially increased. Big data bring new opportunities to telecommunication services. Previously, data were siloed and managed independently in different telecommunication service systems. Data aggregation and fusion trends are inevitable with the construction of big data services. In the process of data fusion convergence, data flow on platforms and in-service processes. Data face various security vulnerabilities at different stages of their lifecycle. Recommendation ITU-T X.1751, *Security guidelines for big data lifecycle management by telecommunication operators*, introduces specific characteristics of telecommunication big data services and data categories, analyses security vulnerabilities of big data lifecycle management and specifies security guidelines for telecommunication operators.

Recommendation ITU-T X.1752, *Security guidelines for big data infrastructure and platform*, analyses security threats and challenges for big data infrastructure and big data platform and specifies a reference framework for mapping security guidelines against threats for the big data infrastructure and platform.

Pre-published

15. The future of ICT security standardization

Pre-published

Pre-published

15 Hot topics for ICT security standardization in ITU-T SG17

The ITU was founded in 1865 as the International Telegraph Union. Although its first area of expertise was the telegraph, the work of ITU now covers the whole ICT sector, from digital broadcasting to the Internet, and from mobile technologies to three-dimensional television. The development of ICT security standards has greatly accelerated in recent years with the rapid growth in use of the Internet and other networks, and with the recognition of the need to protect users and systems against the increasing number and variety of security threats.

It has long been recognized that appropriate and effective security provisions should be an essential and integral part of the system design process. Security by design is far more effective in protecting ICT assets than attempting to respond to every new threat with retrofits and hastily-produced countermeasures. The security Recommendations developed by ITU-T provide a sound basis to support secure system design.

Looking towards the future, telecommunications networks and computer networks will continue to converge. We also know with great certainty that networks and web-based services and applications will continue to grow rapidly and will become an increasingly-important part of everyday life for most individuals as well as for public and private sector organizations. Meanwhile, new technologies are emerging simultaneously; machine learning, Internet of Things, Distributed Ledger Technologies (DLT, including blockchains), autonomous driving, 5G, quantum physics, etc. Efforts for development of security standardization have produced outstanding results in the field of IoT, ITS, DLT and Quantum-based communications.

15.1 Security for Internet of Things (IoT)

It is possible to identify a number of areas where security is a pressing concern. The *Internet of Things* (IoT) is one area of particular interest since it implies a massive increase in the connectivity of everyday devices[12], including consumer devices and sensor devices, in many cases without the consumer being aware or directly involved of the possibility or implications of a security breach. Some dramatic examples of the possible consequences of inadequate security have been demonstrated. These include the hacking & hijacking of currently-installed automobile control systems and interception and unauthorized changes to automated healthcare delivery mechanisms.

SG17 is developing a security framework for IoT and ITU-T has established a new Study Group (SG20) to study IoT and its applications, with an initial focus on smart cities and communities. ITU-T Recommendation Y.2066, renumbered as Y.4100 in 2016 without any modification or being republished, provides the common requirements of Internet of Things (IoT). Recommendation ITU-T X.1361, *Security framework for the Internet of things based on the gateway model*, analyses security threats and challenges in the IoT environment based on the model described in Y.2066, *Common requirements of the Internet of things*. Then it describes capabilities that address and mitigate these security threats and challenges for the Internet of Things (IoT) using security gateways.

Recommendation ITU-T X.1352, *Security requirements for Internet of things devices and gateways*, establishes detailed requirements for five security dimensions applicable to Internet of things (IoT) device and gateway: authentication; cryptography; data security; device platform security; and physical security. Theses security requirements are based on the IoT reference model specified in Recommendation ITU T Y.4100 and the IoT security framework in Recommendation ITU-T X.1361.

[12] The Gartner report "The Internet of Things, Worldwide, 2013" estimates that the number of interconnected devices will rise to 26 billion by 2020.

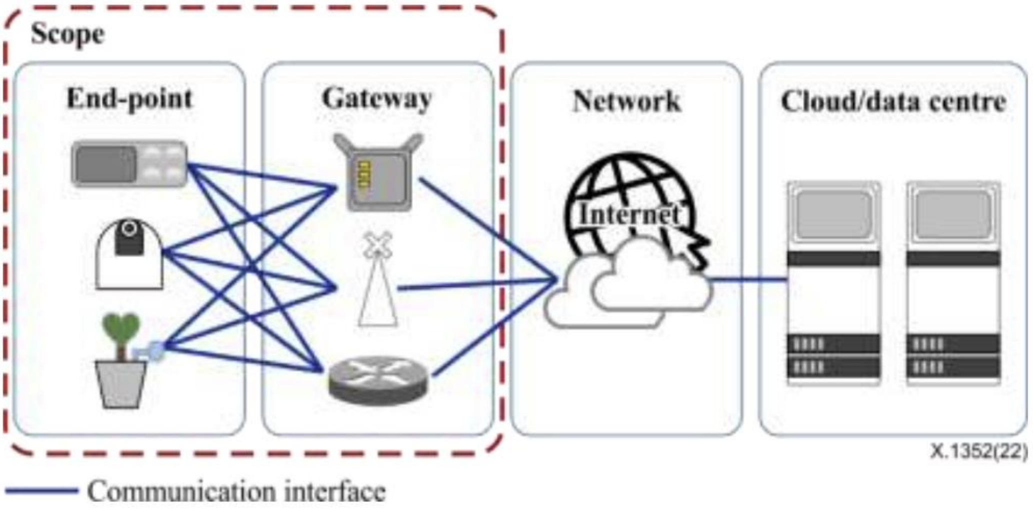


Figure 95- Main components for IoT framework

The authentication dimension includes user authentication, secure use of authentication credentials and device authentication. The cryptography dimension includes the use of secure cryptography, secure key management and secure random number generation. The data security dimension includes secure transmission and storage, information flow control, secure session management and personally identifiable information (PII) management. The device platform security dimension includes five elements: software security; secure update; security management; logging; and timestamp. Likewise, the physical security dimension includes a secure physical interface and tamper-proofing.

Figure 96 shows the targets for security dimensions in an IoT device and gateway.

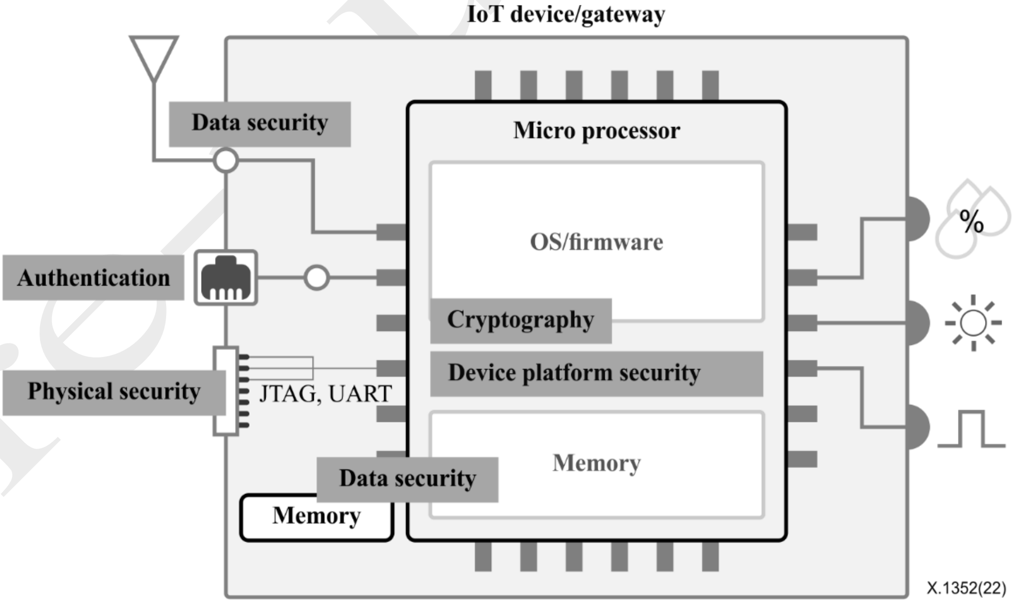


Figure 96 - Example for applied security dimensions on IoT devices and gateways

IoT devices can be used various environment having different characteristics. [Recommendation ITU-T X.1364](), *Security requirements and framework for narrow band Internet of things*, establishes a security framework for operators to safeguard applications of narrow band Internet of things (NB-IoT), based on

Pre-published

cellular mobile network that uses a bandwidth of approximately only 180 KHz. NB-IoT is expected to be massively adopted by operators with wide application in multiple vertical industries, because of its low power dissipation, wide coverage, low cost, and high capacity.

In IoT environment, some IoT devices have capability to collect PII data. As PII data are useful for various types of services, data can be shared among multiple service providers. Recommendation ITU-T X.1363, Technical framework of PII (Personally Identifiable Information) handling system in IoT environment, provides technical framework for IoT user's PII data when collected, shared and used by one or more IoT service providers, based on ITU-T X.1058, *Code of practice for personally identifiable information protection*, and ISO/IEC 29100, *Privacy framework*. Figure 97 depicts the technical framework for PII data handling one IoT services by multiple service providers with a common PII preference management portal.

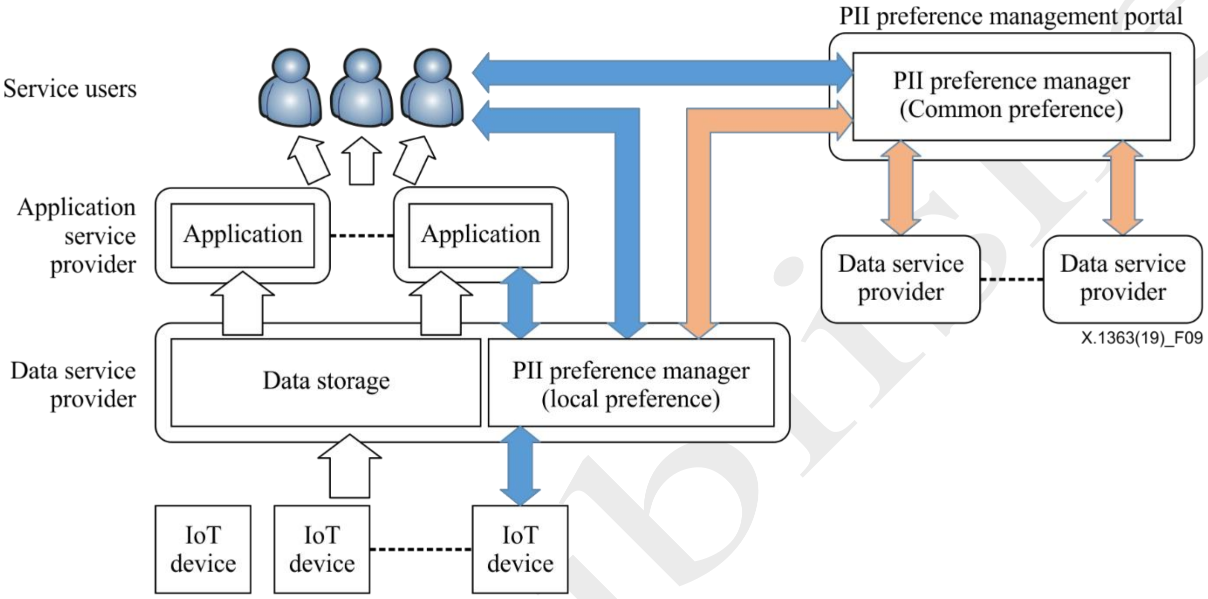


Figure 97 - Technical framework for PII data handling one IoT services by multiple service providers with a common PII preference management portal

Critical infrastructure protection (CIP) is another area for which effective security is absolutely essential. However, the development of standards for this area is complicated by a number of factors including differences of opinion as to what actually constitutes critical infrastructure in different countries and whether or not the development of needed standards lies within the current remit of standards development organizations (SDOs). However, many of the security standards already developed or in development may well be adopted to address CIP security needs. Security of the Smart Grid is another area that is drawing much attention from SDOs. Smart Grid security requirements are under consideration by SG17. Recommendations ITU-T X.1331, *Security guidelines for home area network (HAN)* devices in smart grid systems, analyse the security risks and requirements for devices and communications in a HAN, and provides the security functions and guidelines to protect the HAN. Figure 98shows the general model of HAN with various type of networks in a smart grid. Figure 98 shows the general model of HAN with various type of networks in smart grid.

Pre-published

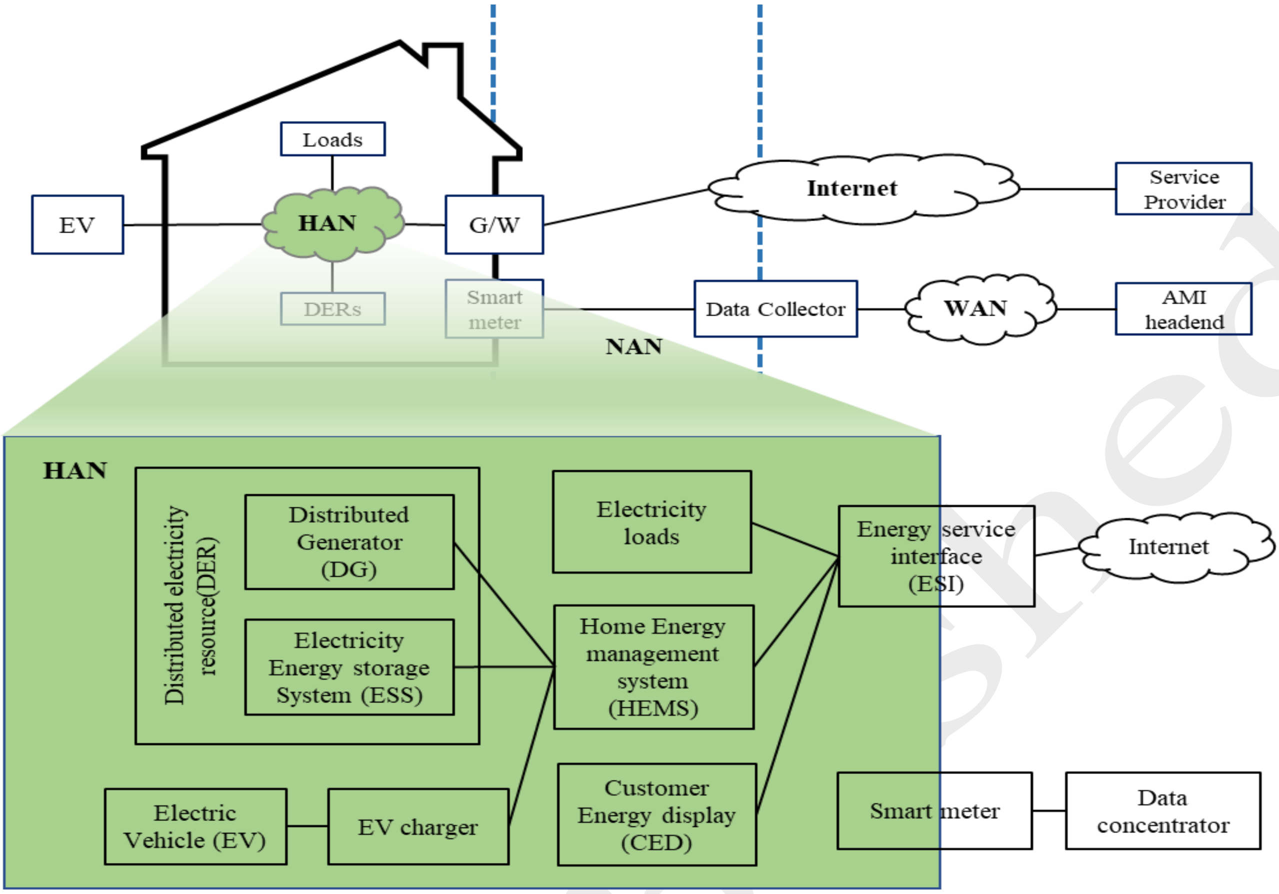

Loads
EV
HAN
G/W
DERs
Smart meter
Internet
Service Provider
Data Collector
WAN
AMI headend
NAN
HAN
Distributed electricity resource(DER)
Distributed Generator (DG)
Electricity Energy storage System (ESS)
Electricity loads
Home Energy management system (HEMS)
Energy service interface (ESI)
Internet
Electric Vehicle (EV)
EV charger
Customer Energy display (CED)
Smart meter
Data concentrator

Figure 98 - General model of HAN with various type of networks in a smart grid

The number of Internet of things (IoT) devices is increasing, and in the near future there will be an enormous number of devices connected to the IoT network including 5G. Recommendation ITU-T X.1366 specifies two message authentication schemes. One is an aggregate message authentication (AMA) scheme for IoT as a basic mechanism. The other is an interactive aggregate message authentication (IAMA) scheme with interactive protocol in a lightweight and secure manner. Both aggregate message authentication schemes can be applied for ensuring "entity (identity) authentication" as well as for ensuring "message authentication". These schemes may not be applicable in all use cases for utilizing IoT devices, but they are quite effective and suitable for use cases in the following conditions where:

- Message authentication is required from tens to tens of thousands of IoT devices.
- Data or message being handled for an authentication process that occurs frequently and intermittently.

Figure 99 shows the concept of aggregate message authentication system.

Pre-published

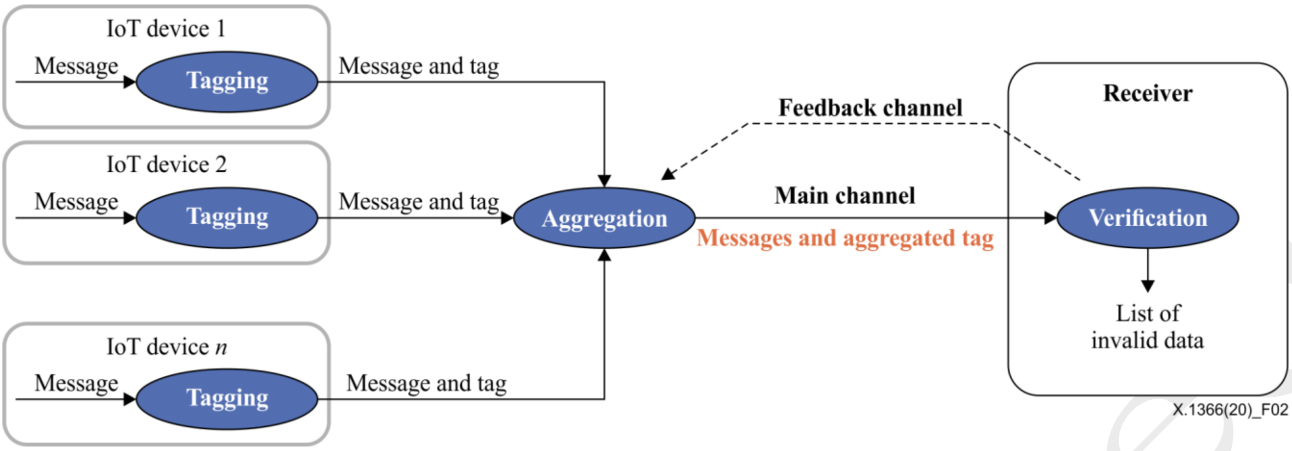


Figure 99 - Basic concept of aggregate message authentication system

There are two issues to handle security incidents from the Internet of things (IoT) ecosystem: The first is the incompatibility of protocols between computer networks using transmission control protocol/Internet protocol (TCP/IP) and IoT edge devices. The second is the lack of compatibility of error codes among edge device manufacturers.

Recommendation ITU-T X.1367 specifies a standardized error log format that can be placed in a protocol payload, such as syslog (see IETF RFC 5424) to be used for converting an error log information issued by an edge device to the standard error log format.

This Recommendation also specifies a standardized error code table to solve the second issue. As a result, security incidents across computer networks and networks for IoT edge devices can be integrally managed.

Recommendation ITU-T X.1368 specifies: 1) basic models and procedures for securely updating firmware or software (FW/SW) of Internet of things (IoT) devices; and 2) requirements and capabilities for updating IoT FW.

A common secure update procedure is specified with general requirements. This procedure allows common IoT SW/FW updates to be securely implemented among stakeholders in the IoT environment, such as IoT device developers and IoT system/service providers.

This Recommendation focuses on updating FW, but it is applicable to updating any other SW of IoT devices.

Recommendation ITU-T X.1369 specifies security requirements for the IoT service platform. It assesses security threats and challenges to the IoT business service platform and describes security measures that could mitigate security threats and challenges.

The security architecture of the IoT service platform focuses on six aspects of security protection requirements: application security, interface security, data security, system security, infrastructure security and operational security.

The overall security architecture is shown in Figure 100.

Pre-published

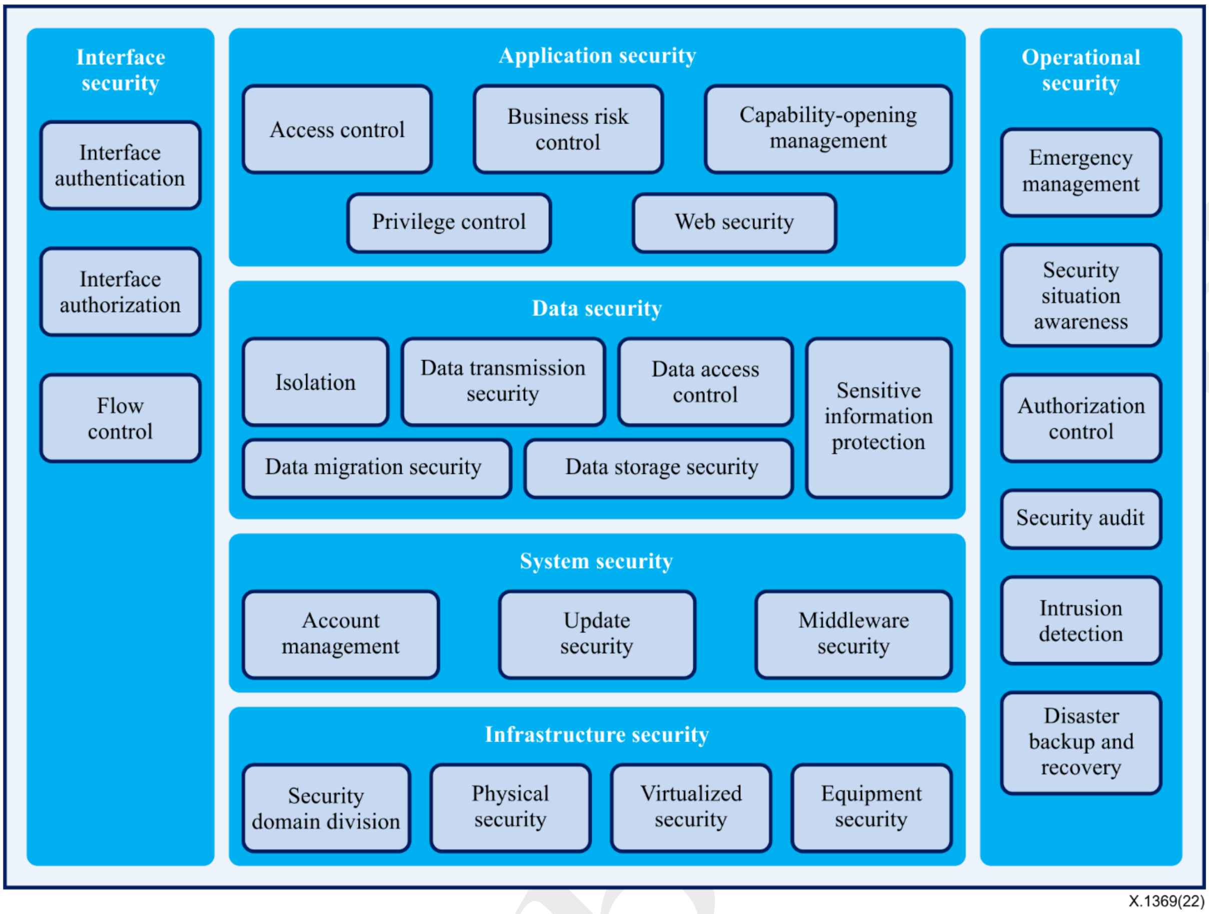


Figure 100 - Security architecture of the IoT service platform

15.2 Security for Intelligent Transport Systems (ITS)

Another area of evolving convergence technology is Intelligent Transport System (ITS). It is the application of monitoring, sensing, analysing, controlling and communicating various information to improve road safety, environmental footprint of transport, and traffic management and at the same time, maximize the transport sector's benefits to public and commercial users in a roadway as well as railway, airway and waterway. In the ITS environment, vulnerabilities of any entity involved in ITS echo-systems can be propagated to other ITS entities since everything is connected to each other. Thus, vulnerabilities of connected ITS entity such as connected vehicle should be managed and handled in order not to influence a lot of other vehicles and ITS systems. Recommendation ITU-T X.1371, *Security threats in connected vehicles*, describes security threats to connected vehicles based on the model in Figure 101.

Pre-publication

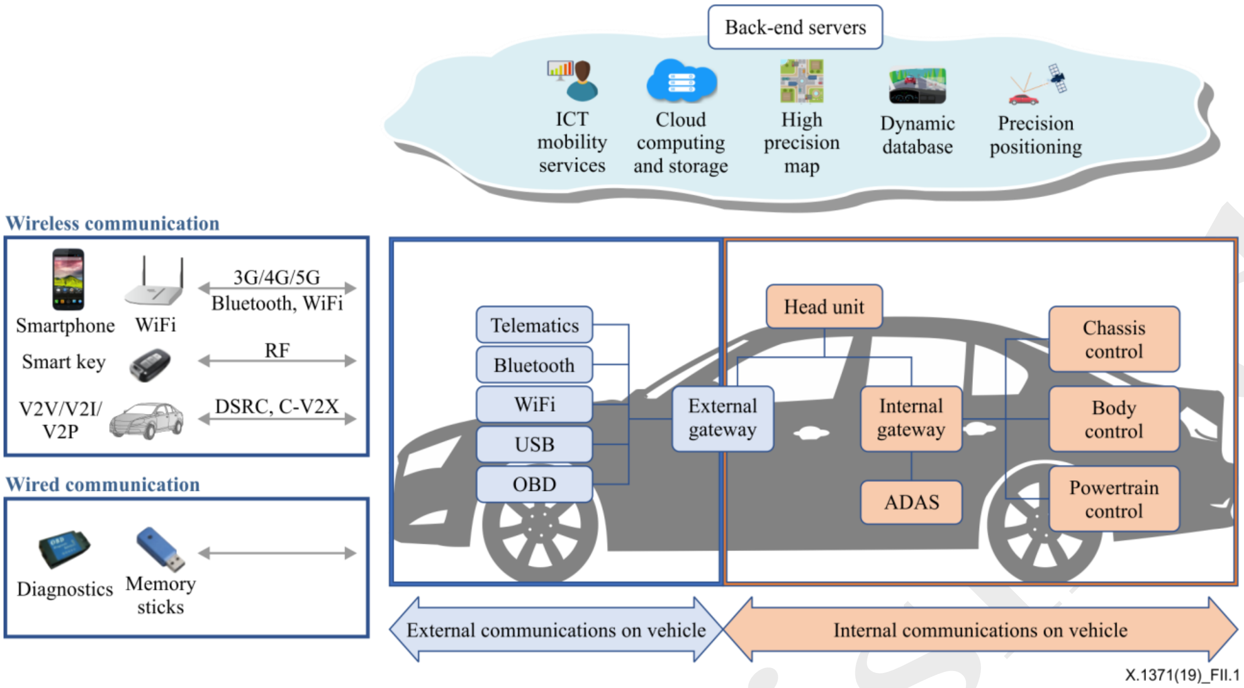


Figure 101 - A concept of connected vehicle

Recommendation ITU-T X.1372, Security guidelines for Vehicle-to-Everything (V2X) communication, provides security guidelines for V2X communication. V2X, or "vehicle-to-everything" is a generic term that covers the communication modes termed as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-nomadic devices (V2D) and vehicle-to-pedestrian (V2P). This Recommendation identifies threats in the V2X communication environment, specifies security requirements and provides description of possible implementation of V2X communication with security.

Pre-published

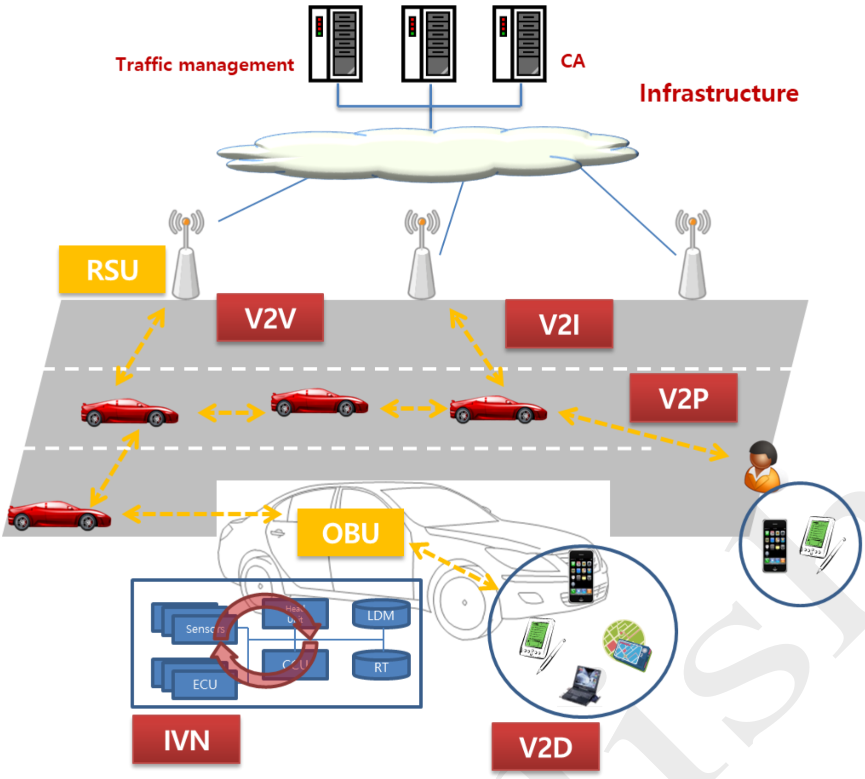


Figure 102 - Overview of vehicular communication

There are many electric devices inside a vehicle such as electronic control units (ECUs), and electric toll collections (ETCs), system and car navigation systems. Software modules inside them need to be appropriately updated for the purpose of bug fixing, and for performance and security improvements to avoid crucial accidents. Recommendation ITU-T X.1373, Secure software update capability for intelligent transportation system communication devices, provides secure software update procedures between software update server and vehicles with appropriate security controls. In the context of updates of software modules in the electric devices of vehicles in the intelligent transportation system (ITS) communication environment, this Recommendation aims to provide a procedure of secure software updating for ITS communication devices for the application layer in order to prevent threats such as tampering of and malicious intrusion to communication devices in vehicles. These procedures can be be practically utilized by car manufactures and ITS-related industries.

15.3 Distributed Ledger Technology (DLT) Security

Distributed Ledger Technology (DLT), well-known as blockchain, is one of the disruptive technologies with immense potential to reshape our economy, culture, and societys. All business is based on transaction records agreed upon and confirmed between transaction parties. DLT enables these transaction records to be stored and maintained in a distributed ledger on an online network through automated consensus between participants without intermediaries. Participants in a DLT system maintain the distributed ledger and participate in the consensus that determines which records are added on. Users perform their work based on the trust of the records provided the DLT service.

This innovative technology facilitates decentralized financial and non-financial applications, eliminating the need for third party intermediaries. It is emerging a new data sharing infrastructure that will accelerate the service revolution in telecommunication-based industries such as finance, healthcare, super logistics, governments, metaverses, etc. The impact of DLT will be significant for telecom service providers, customers and users, as well as related industries. Therefore, ensuring the security of DLT itself and various DLT-based applications is essential.

Pre-published

15.3.1 Security for DLT service

For the DLT security standardization, Recommendation ITU-T X.1400, *Terms and definitions for distribute ledger technology* provides definitions of the most fundamental and commonly-used DLT-specific terms to establish a basis for common understanding. Recommendation ITU-T X.1401, Security threats to distributed ledger technology, identifies security threats to the technology, categorized into protocols, networks and data. It provides descriptions of threats in terms of targeted components, attacks, attack impact, and attack likelihood. Based on the analysis of security threats, Recommendation ITU-T X.1402, Security framework for distributed ledger technology derives security requirements and capabilities that could mitigate those threats in ITU-T X.1401, and provides a methodology to develop a framework for a specific DLT application. The security capabilities for DLT is shown in Figure 93.

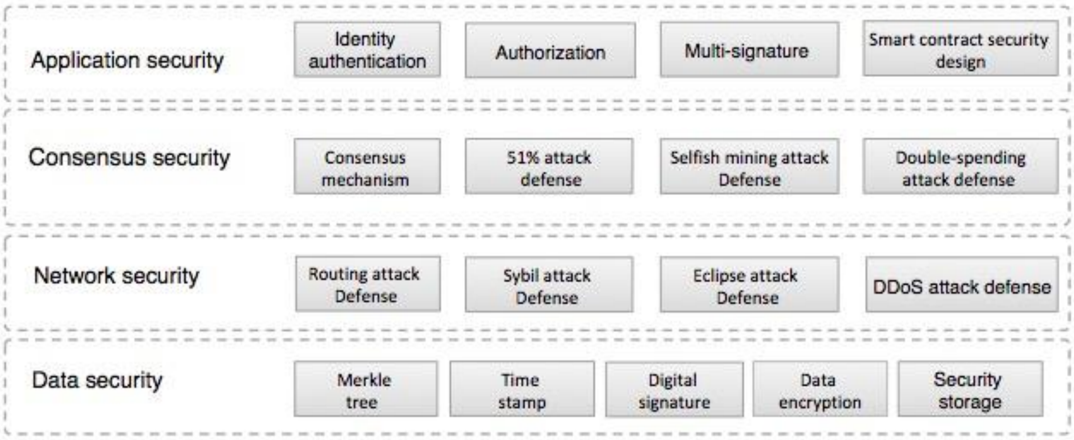


Figure 103 - Security capabilities for DLT

Recommendation ITU-T X.1404, *Security assurance for distributed ledger technology*, presents criteria to achieve three security assurance levels for ten security assurance components, which are data integrity, data confidentiality, credential management, identity proofing of users, entity authentication, authorization, data obfuscation, consensus mechanism strength, smart contract, and PII data protection. Recommendation ITU-T X.1412, *Security requirements for smart contract management based on the distributed ledger technology*, analyses security threats and challenges for smart contract management based on the distributed ledger technology, and provides security requirements based on the analysis. Figure 104 shows the security framework of smart contract management.

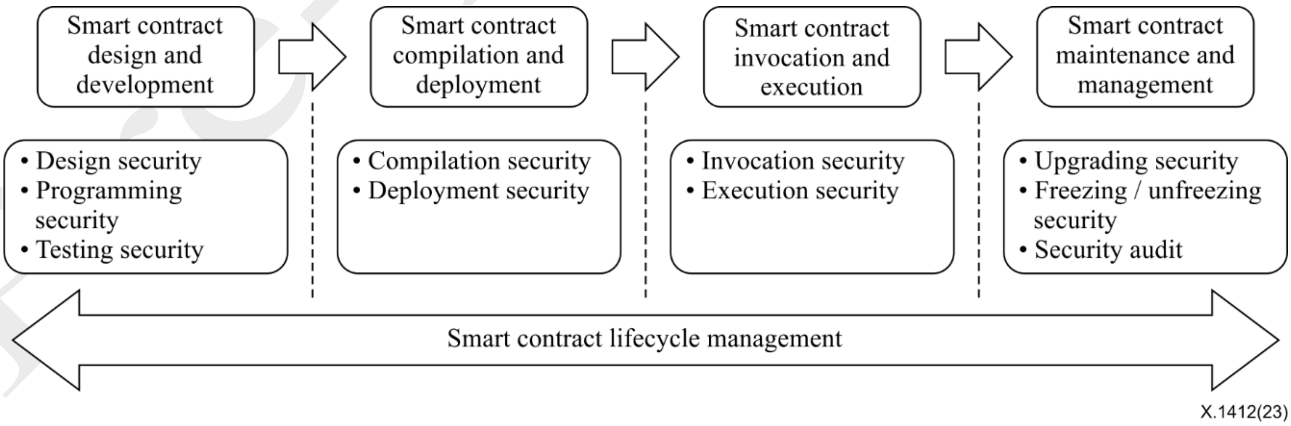

Smart contract design and development
Smart contract compilation and deployment
Smart contract invocation and execution
Smart contract maintenance and management
• Design security
• Programming security
• Testing security
• Compilation security
• Deployment security
• Invocation security
• Execution security
• Upgrading security
• Freezing / unfreezing security
• Security audit
Smart contract lifecycle management
X.1412(23)

Figure 104 - Security framework of smart contract management

For Recommendation ITU-T X.1411, *Guideline on blockchain as a service (BaaS) security*, please refer 14.3.

Pre-published

15.3.2 Security for DLT-based applications

The emergence of DLT provides the opportunity for the development of decentralized identity management. Recommendation ITU-T X.1403, Security guidelines for using DLT for decentralized identity management, discusses security benefits of decentralized identity, introduces the concept of decentralized identity and access management system, and provides guidance concerning controls that should be used to mitigate identity data threats.

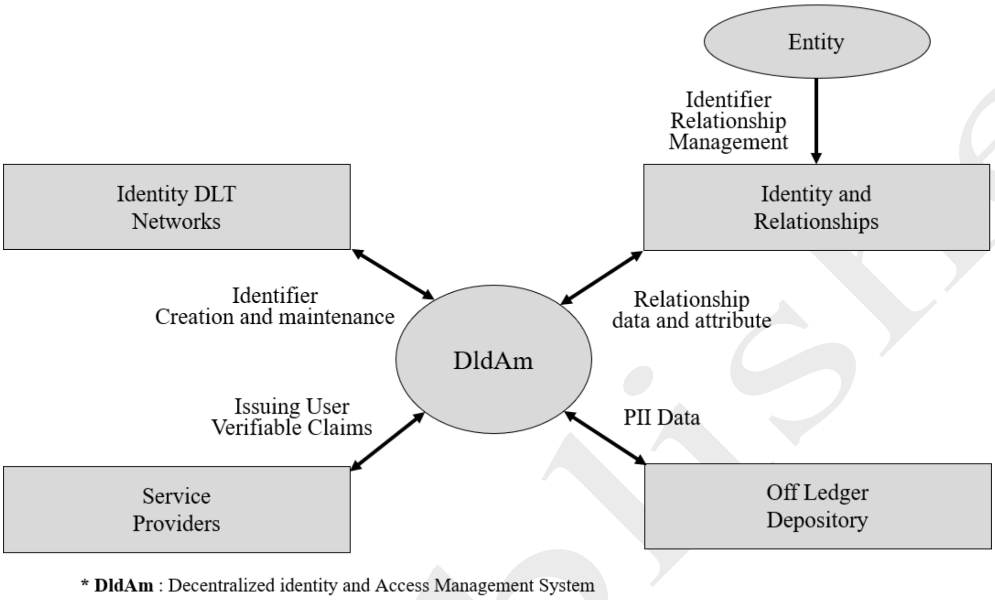


Figure 105 - DIdAm framework

DLT is being most actively adopted in the financial sector. Recommendation ITU-T X.1405, *Security threats and requirements for digital payment services based on distributed ledger technology*, provides a simplified model of digital payment systems based on DLT shown in Figure 106, and analyses security threats and challenges of traditional financial systems and digital payment services using DLT. It also provides the security requirements against the specified threats and challenges

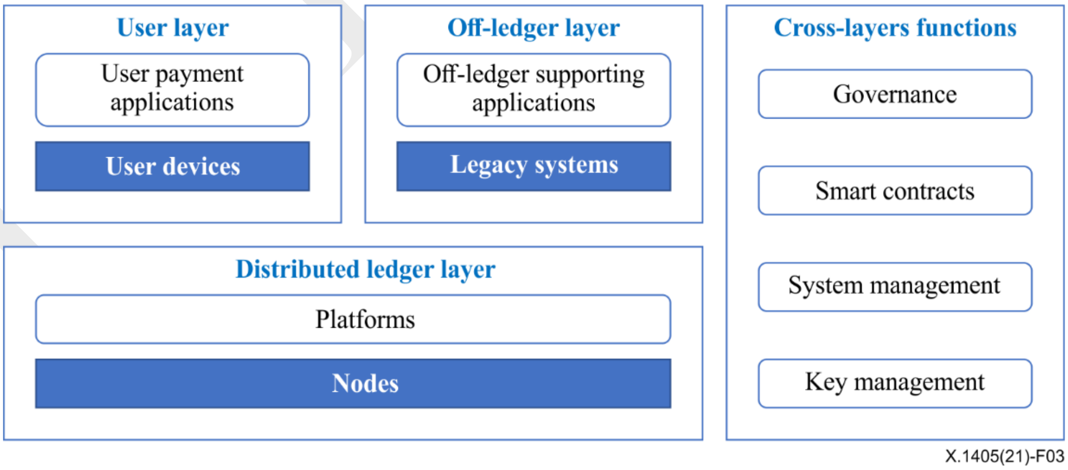


Figure 106 - A simplified model of digital payment systems based on DLT

Recommendation ITU-T X.1408, *Security threats and requirements for data access and sharing based on distributed ledger technology*, provides a model for data access and sharing solution between data controller and data processors. Figure 107 shows the security architecture of DLT-based data-sharing management in Recommendation ITU-T X.1410, *Security architecture of data sharing management based on the distributed ledger technology*.

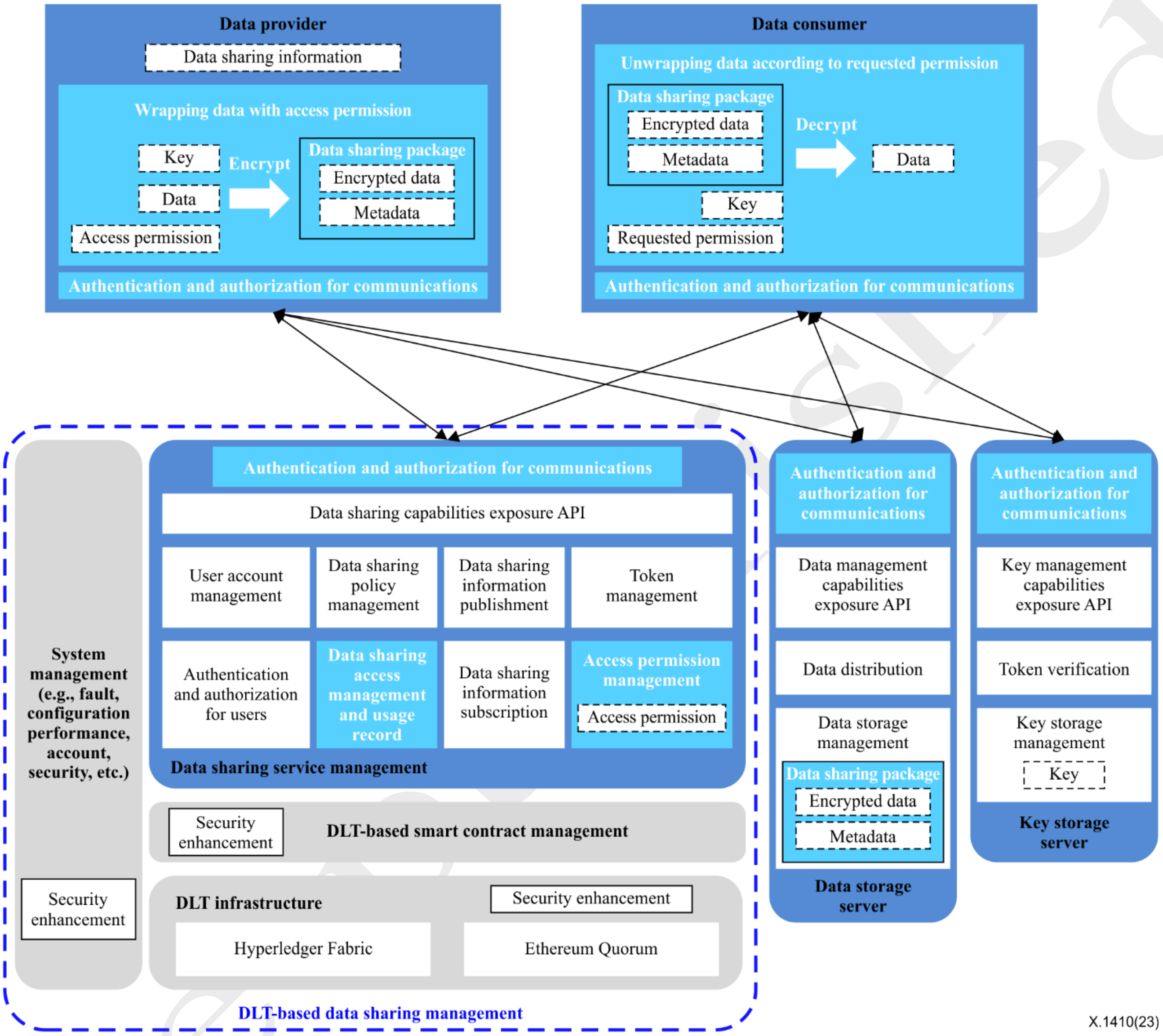

Data provider
Data sharing information
Wrapping data with access permission
Key
Data
Access permission
Encrypt
Data sharing package
Encrypted data
Metadata
Authentication and authorization for communications
Data consumer
Unwrapping data according to requested permission
Data sharing package
Encrypted data
Metadata
Decrypt
Data
Key
Requested permission
Authentication and authorization for communications
System management (e.g., fault, configuration performance, account, security, etc.)
Security enhancement
Authentication and authorization for communications
Data sharing capabilities exposure API
User account management
Data sharing policy management
Data sharing information publishment
Token management
Authentication and authorization for users
Data sharing access management and usage record
Data sharing information subscription
Access permission management
Access permission
Data sharing service management
Security enhancement
DLT-based smart contract management
DLT infrastructure
Security enhancement
Hyperledger Fabric
Ethereum Quorum
DLT-based data sharing management
Authentication and authorization for communications
Data management capabilities exposure API
Data distribution
Data storage management
Data sharing package
Encrypted data
Metadata
Data storage server
Authentication and authorization for communications
Key management capabilities exposure API
Token verification
Key storage management
Key
Key storage server
X.1410(23)

Figure 107 – Security architecture of DLT-based data-sharing management

15.4 Quantum-based security technology

Another new technology that is expected to have a major impact on security is Quantum technology. Quantum computing poses significant risks to security based on cryptography that relies on computationally difficult problems. Quantum computing is notably quick to solve integer-factoring and discrete-logarithm problems, which are relied on by almost all public key cryptography systems. Cryptographic primitives are out of scope of SG 17, but quantum-safe communication is one of the areas that SG 17 should study. Physical implementation of interoperable quantum safe communications requires several key elements including quantum key distribution and quantum random number generators. Recommendation ITU-T X.1702 specifies a functional architecture for random number generation based on quantum phenomena and provide specifications regarding quantum physical entropy sources. Figure 108 shows the functional architecture of a quantum entropy source.

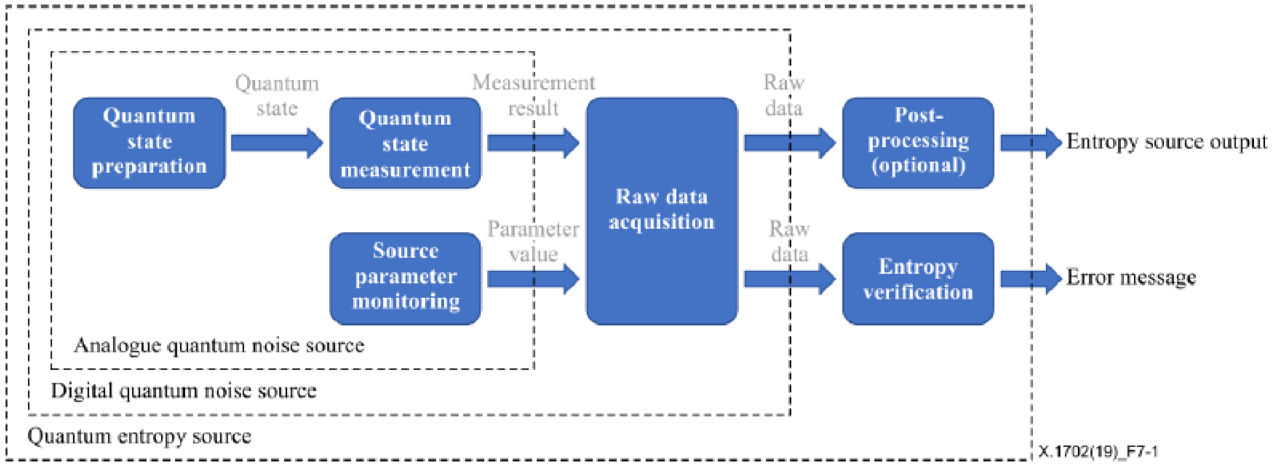


Figure 108 - Functional architecture of a quantum entropy source

This manual has provided a broad overview of some of the key security-related initiatives and achievements of the ITU-T Study Groups in an effort to promote greater understanding of the work and the challenging technical issues facing network users and implementers. Readers are encouraged to take advantage of the ITU-T's extensive on-line resources to obtain more detailed information on the topics presented here and to use the Recommendations and guidance documents to help build a more secure on-line environment and to enhance user confidence in on-line operations.

The 193 Member States and approximately 900 Sector Members and associates of the ITU will continue to respond to these challenges by continuing to develop technical Recommendations and guidelines on security in an aggressive programme of work that is driven by the needs of the members and guided by the organizational structure established by the World Telecommunication Standardization Assembly. Wherever possible, ITU-T will collaborate with other standards development organizations to minimize duplication of effort and to achieve harmonized solutions as efficiently and expeditiously as possible.

Pre-publish

16. Sources of additional information

Pre-published

16 Sources of additional information

This manual presents a broad overview of the ITU-T security work. Much more detailed information, including many of the standards, is freely available via the ITU-T web site.

16.1 Overview of SG17 work

As a first step, the ITU-T SG17 home page provides links to information about the SG17 work including tutorials and presentations, summaries of Recommendations under development, and key personnel. The links to the Lead study group on telecommunication security and the Lead study group on identity management (IdM) provide information on the activities and results of the work of these two Lead Study Groups.

16.2 The Security Compendium

The Security Compendium presents a detailed view of ITU security activities, first of all on approved, new and revised security Recommendations (as Part 1), as well as approved, new and amended definitions and abbreviations of security related Recommendations (as Part 2)

- Part 1: Catalogue of approved Recommendations related to telecommunication security

- Part 2: List of security definitions extracted from approved ITU-T Recommendations

Further more security activities of ITU-T are summarized on the ICT Security Standards Roadmap (especially in its Part 2).

16.3 The Security Standards Roadmap

The ICT Security Standards Roadmap is an on-line resource that provides information about existing ICT security standards and work in progress in key standards development organizations. In addition to aiding the process of standards development, the Roadmap will provide information that will help potential users of security standards, and other standards stakeholders, gain an understanding of what standards are available or under development as well as the key organizations that are working on these standards

The Roadmap is in six parts and the information is directly accessible on-line:

Part 1 *ICT Standards Development Organizations and Their Work*, which contains information about the Roadmap structure and about each of the listed standards organizations. Part 1 also provides links to existing security glossaries and vocabularies;

Part 2 *Approved ICT Security Standards*, which contains a searchable database of approved security standards with direct links to most of the standards; In addition to information about the ITU-T security work, the Roadmap includes information on the security standards work of ATIS, ETSI, IEEE, ISO, ISO/IEC JTC 1, OASIS, oneM2M, 3D@home, 3GPP, and 3GPP2.

Part 3 *Security standards under development*;

Part 4 *Future needs and proposed new security standards*;

Part 5 *Security best practices* and

Part 6 *Identity management (IdM) landscape: IdM standards, organizations and gap analysis*.

It also explains ICT security standards coordination.

Pre-published

16.4 Implementation guidelines for security

Supplement 3 to the ITU-T X-series of Recommendations provides more detailed background on some of the topics discussed in this manual and provides system and network security implementation guidelines that can be used to realize a network security program. These guidelines address four areas: technical security policy; asset identification; threats, vulnerabilities and mitigations; and security assessment. The guidelines indicate key components required to build and manage the technical policy needed to manage networks that potentially span multiple operators and contain products and systems from multiple vendors. It also provides guidelines on regulatory issues.

For more information on X-series implementation can be found at Implementors' Guides. It includes the OSI Implementer's Guide and the Directory Implementers' Guide. The Z-Series Implementers' Guide also is provided.

Pre-published

Annex A – Security definitions

Pre-published

Annex A: Security definitions

The following table contains definitions for terms used in this publication. All definitions are extracted from current ITU-T Recommendations. A more complete list of security definitions is contained in the compendium of ITU-T approved security definitions maintained by Study Group 17.

Term	Definition	Reference
access control	1. The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. 2. Limiting the flow of information from the resources of a system only to authorized persons, programs, processes or other system resources on a network. 3. A security technique used to regulate who can do what to information resources in a computing environment.	ITU-T X.800 ITU-T J.170 ITU-T X.1080.0
access control list	A list of entities, together with their access rights, which are authorized to have access to a resource.	ITU-T X.800
access control policy	The set of rules that define the conditions under which an access may take place.	ITU-T X.812
access management	2) A set of processes to manage the granting or denying of an operation to be performed on a resource. As denoted in Figure 1/X.1093, access management consists of two main processes. The subject to be permitted to access a resource is needed to undergo the authentication process. To implement the authentication process, secure authentication method should be deployed. In this Rec. biometrics-on-card provides the required authentication mechanism. The authorization makes decision to allow or deny access to the resource based on a policy. Authorization is supported by administrative activity which assigns subject privileges in accordance with the access management policy.	ITU-T X.1093
access service	A service provided by a service provider for the execution of a particular transaction.	ITU-T X.1080.0
accidental threats	Threats that exist with no premeditated intent. Examples of realized accidental threats include system malfunctions, operational blunders and software bugs.	ITU-T X.800
accountability	The property that ensures that the actions of an entity may be traced uniquely to the entity.	ITU-T X.800
ACL/DAC access control	An access control model, in which the concept of the access control lists (ACLs)/discretionary access control (DAC) is one where each resource on a system to which access should be controlled, referred to as an object, and has its own associated list of mappings between the set of entities requesting access to the resource and the set of actions that each entity can take on the resource.	ITU-T X.1550
algorithm	A mathematical process which can be used for the scrambling and descrambling of a data stream.	ITU-T J.93
application	A set of functionalities provided by a common entity (the application owner also known as the relying party) and perceived by the user as belonging together.	ITU-T X.1277
attack	1. The activities undertaken to bypass or exploit deficiencies in a system's security mechanisms. By a direct attack on a system they exploit deficiencies in the underlying algorithms, principles, or properties of a security mechanism. Indirect attacks are performed when they bypass the mechanism, or when they make the system use the mechanism incorrectly.	ITU-T H.235 ITU-T X.1361

Pre-published

Term	Definition	Reference
	2. An attempt by an adversary on the device to obtain or modify sensitive information or a service they are not authorized to obtain or modify.	
attack pattern	2) Attack patterns [are STIX 2.0 domain objects (SDOs), and] are a type of TTP that describe ways that adversaries attempt to compromise targets.	ITU-T X.1215
attribute	In the context of message handling, an information item, a component of an attribute list, that describes a user or distribution list and that can also locate it in relation to the physical or organizational structure of message handling system (or the network underlying it). 8) A piece of information of a particular type that is associated with an object. Information associated with an object is composed of attributes.	ITU-T X.400 ITU-T X.1080.0
attribute aggregation	A mechanism for collecting attributes from multiple identity service providers (IdSPs). NOTE – Once the attributes have been collected, they need to be aggregated and asserted for authentication and authorization.	ITU-T X.1258
attribute authority (AA)	1. An authority which assigns privileges by issuing attribute certificates. 2. An entity trusted by one or more entities to create and sign attribute certificates. Note – a CA may also be an AA.	ITU-T X.509 ITU-T X.842
attribute certificate	A data structure, digitally signed by an Attribute Authority, that binds some attribute values with identification information about its holder.	ITU-T X.509
authentication	1. The process of corroborating an identity. Note – See principal and verifier and the two distinguished form of authentication (data origin auth. + entity auth.). Authentication can be unilateral or mutual. Unilateral authentication provides assurance of the identity of only one principal. Mutual authentication provides assurance of the identities of both principals. 2. The provision of assurance of the claimed identity of an entity. 3. See data origin authentication, and peer entity authentication. The term "authentication" is not used in connection with data integrity; the term "data integrity" is used instead. 4. The corroboration of the identity of objects relevant to the establishment of an association. For example, these can include the AEs, APs, and the human users of applications. Note – This term has been defined to make it clear that a wider scope of authentication is being addressed than is covered by peer-entity authentication in CCITT Recommendation ITU-T X.800. 5. The process of verifying the claimed identity of an entity to another entity. 6. The process intended to allow the system to check with certainty the identification of a party. 7. Provision of assurance in the identity of an entity. 8. The process in which a user employs their FIDO authenticator to prove possession of a registered key to a relying party.	ITU-T X.811 ITU-T X.811 ITU-T X.800 ITU-T X.217 ITU-T J.170 ITU-T J.93 ITU-T X.1038 ITU-T X.1277
authentication exchange	1. A mechanism intended to ensure the identity of an entity by means of information exchange. 2. A sequence of one or more transfers of exchange authentication information for the purposes of performing an authentication.	ITU-T X.800 ITU-T X.811
authentication service	The authentication service delivers proof that the identity of an object or subject has indeed the identity it claims to have. Depending on the	ITU-T M.3016.2

Pre-published

Term	Definition	Reference
	type of actor and on the purpose of identification, the following kinds of authentication may be required: user authentication, peer entity authentication, data origin authentication. Examples of mechanisms used to implement the authentication service are passwords and Personal Identification Numbers (PINs) (simple authentication) and cryptographic-based methods (strong authentication).	
authority	An entity, responsible for the issuance of certificates. Two types are defined; certification authority which issues public-key certificates and attribute authority which issues attribute certificates.	ITU-T X.509
authorization	1. The granting of rights, which includes the granting of access based on access rights. Note – This definition implies the rights to perform some activity (such as to access data); and that they have been granted to some process, entity, or human agent. 2. The granting of permission on the basis of authenticated identification. 3. The act of giving access to a service or device if one has the permission to have the access.	ITU-T X.800 ITU-T H.235 ITU-T J.170
availability	The property of being accessible and useable upon demand by an authorized entity.	ITU-T X.800
biometric (adjective)	Pertaining to the field of biometrics.	ITU-T X.1087
biometrics (noun)	1)c Automated recognition of individuals based on their behavioural and biological characteristics.	ITU-T X.1087
biosignal	Any measureable signal in living beings (physical, chemical or electrical) that can be measured or monitored, such as a ballistocardiogram (BCG), electroencephalogram (EEG), electrocardiogram (ECG) and photoplethysmogram (PPG).	ITU-T X.1094
biosignal sensor	An analytical device for detection of biosignals. It can measure a physical quantity and converts it into a signal.	ITU-T X.1094
biometrics (noun)	1)c Automated recognition of individuals based on their behavioural and biological characteristics.	ITU-T X.1087
blacklists\whitelists	Blacklists [for countering mobile in-application advertising spam] are based on the principle of maintaining Internet protocol (IP) addresses or domains that are suspected of sending ad spam. These lists can also include device identity (ID), URLs or sender accounts in the service platform. They can be implemented by an entity for shared use, or introduced and maintained by the service platform using it for its own requirements. Whitelists [for countering mobile in-application advertising spam] are based on the principle of listing sources/entities of approved or recognized ads. These lists can include device ID or sender accounts in service platform. Similar to keywords, although blacklists and whitelists inevitably contain inaccuracies and blacklists can possibly prevent some legitimate ads from getting through filtering engines, both blacklists and whitelists are an effective solution for filtering ad spam.	ITU-T X.1249
blockchain	A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.	ITU-T X.1400
blockchain as a service (BaaS)	A cloud service category in which the capabilities provided to the cloud service customer are to deploy and manage a blockchain network in order to enable the abilities of consensus, smart contract,	ITU-T X.1400

Pre-published

Term	Definition	Reference
	transaction, crypto engine, block record storage, peer-to-peer connectivity and management using blockchain.	
capability	A token used as an identifier for a resource such that possession of the token confers access rights for the resource. 6)b Quality of being able to perform a given activity. 10) Construct that represents the collection of capability characteristics (expressed as capability attributes) of either a Resource (its provided Capability) or an Enterprise Activity (its required Capability) NOTE – Capabilities can be aggregated.	ITU-T X.800 ITU-T X.1631 ITU-T X.1361
centralized DDoS-attack mitigation service	A service that can establish and distribute access control policy rules into network resources for efficient distributed denial-of-service (DDoS) attack mitigation. These rules can be managed dynamically by a centralized server. Software-defined networking (SDN) can work as a centralized DDoS attack mitigation service through a standard interface between DDoS attack mitigation applications and network resources.	ITU-T X.1042
centralized firewall service	A service that can establish and distribute access control policy rules into network resources for efficient firewall management. These rules can be managed dynamically by a centralized server. Software-defined networking (SDN) can work as a centralized firewall service through a standard interface between firewall applications and network resources.	ITU-T X.1042
centralized honeypot service	A service that can establish and distribute access control policy rules into network resources for the dynamic honeypot configuration. These rules can be managed dynamically by a centralized server. Software-defined networking (SDN) can work as a centralized honeypot service through a standard interface between honeypot applications and network resources. The honeypot can dynamically manage honeypot places. The centralized honeypot manages switches and new routing paths to attract attackers to a place used as a trap, i.e., a honeypot. The honeypot is configured as the intended attack target and reports the collected information to the centralized honeypot service.	ITU-T X.1042
centralized illegal device management service	A service that can establish and distribute access control policy rules into network resources for the blacklist of illegal devices. These rules can be managed dynamically and globally by a centralized server. Software-defined networking (SDN) can work as network-based illegal device management through a standard interface between illegal device management applications and network resources. NOTE – A criterion for an illegal device lies outside the scope of this Recommendation. An example of the illegal device may be determined according to usage of the global unique identification system.	ITU-T X.1042
certificate	A set of security-relevant data issued by a security authority or trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data (security certificate – ITU-T X.810). The term refers to "public key" certificates which are values that represent an owner's public key (and other optional information) as verified and signed by a trusted authority in an unforgeable format. 4) An X.509v3 certificate defined by the profile specified in IETF RFC 5280 and its successors.	ITU-T H.235 ITU-T X.1277

Pre-published

Term	Definition	Reference
certificate policy	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.	ITU-T X.509
certificate revocation list (CRL)	1. A signed list indicating a set of certificates that are no longer considered valid by the certificate issuer. In addition to the generic term CRL, some specific CRL types are defined for CRLs that cover particular scopes. 2. A CRL includes the serial numbers of certificates that have been revoked (for example, because the key has been compromised or because the subject is no longer with the company) and whose validity period has not yet expired.	ITU-T X.509 ITU-T Q.817
certification authority (CA)	1. An authority trusted by one or more users to create and assign public-key certificates. Optionally the certification authority may create the users' keys. 2. An entity that is trusted (in the context of a security policy) to create security certificates containing one or more classes of security-relevant data.	ITU-T X.509 ITU-T X.810
ciphertext	Data produced through the use of encipherment. The semantic content of the resulting data is not available. Note – Ciphertext may itself be input to encipherment, such that super-enciphered output is produced.	ITU-T X.800
classification	Locally instantiated matching of traffic flows against policy for subsequent application of the required set of network service functions. The policy may be customer/network/ service specific.	ITU-T X.1043
classifier	An element that performs classification.	ITU-T X.1043
compare-on-card	Compare-on-card refers to a card that is designed to perform a comparison of biometric reference within a smart IC card, and thus the IC card requires an additional computational capability of comparing in addition to storing the biometric reference. For the on-card comparison, the biometric processing unit acquires live biometrics, extracts feature information from the biometric information, and transmits it to the card. This can be divided into two types as shown in Figure 5/X.1093 and Figure 6/X.1093, depending on whether or not there is a digital signature function with an ITU-T X.509 certificate.	ITU-T X.1093
confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.	ITU-T X.800
confidentiality service	The confidentiality service provides protection against unauthorized disclosure of exchanged data. The following kinds of confidentiality services are distinguished: selective field confidentiality; connection confidentiality; data flow confidentiality.	ITU-T M.3016.2
consensus mechanism	Rules and procedures by which consensus is reached.	ITU-T X.1400
credentials	Data that is transferred to establish the claimed identity of an entity.	ITU-T X.800
cryptanalysis	1. Analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext. 2. The process of recovering the plaintext of a message or the encryption key without access to the key.	ITU-T X.800

Pre-published

Term	Definition	Reference
	3. The science of recovering the plaintext of a message without access to the key (to the electronic key in electronic cryptographic systems).	ITU-T J.170 ITU-T J.93
cryptographic algorithm	1. Mathematical function that computes a result from one or several input values. 2. A well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output.	ITU-T H.235 ITU-T X.1361
cryptographic system, cryptosystem	1. A collection of transformations from plain text into ciphertext and vice versa, the particular transformation(s) to be used being selected by keys. The transformations are normally defined by a mathematical algorithm. 2. A cryptosystem is simply an algorithm that can convert input data into something unrecognizable (encryption), and convert the unrecognizable data back to its original form (decryption). RSA encryption techniques are described in ITU-T X.509. 3. A set of cryptographic primitives used to provide information security services.	ITU-T X.509 ITU-T Q.815 ITU-T X.1361
cryptography	The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. Note – Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or method is cryptanalysis.	ITU-T X.800
data breach	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed.	ITU-T X.1631
data confidentiality	This service can be used to provide for protection of data from unauthorized disclosure. The data confidentiality service is supported by the authentication framework. It can be used to protect against data interception.	ITU-T X.509
data integrity	The property that data has not been altered or destroyed in an unauthorized manner.	ITU-T X.800
data origin authentication	1. The corroboration that the source of data received is as claimed. 2. The corroboration of the identity of the principal that is responsible for a specific data unit.	ITU-T X.800 ITU-T X.811
data protection domain	A domain where the information to be protected is under a single management component.	ITU-T X.1080.0
decentralized application	Application that runs in a distributed and decentralized computing environment.	ITU-T X.1400
decentralized autonomous organization (DAO)	A digital entity that manages assets and operates autonomously in a decentralized system, but that also relies on individuals tasked to perform certain functions that the automaton itself cannot perform.	ITU-T X.1400
decipherment	The reversal of a corresponding reversible encipherment.	ITU-T X.800
decryption	See decipherment.	ITU-T X.800
delegation	Conveyance of privilege from one entity that holds such privilege, to another entity.	ITU-T X.509

Pre-published

Term	Definition	Reference
denial of service	The prevention of authorized access to resources or the delaying of time-critical operations.	ITU-T X.800
digital signature	1. Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. 2. A cryptographic transformation of a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties, and the sender against forgery by the recipient.	ITU-T X.800 ITU-T X.843
directory service	A service to search and retrieve information from a catalogue of well defined objects, which may contain information about certificates, telephone numbers, access conditions, addresses etc. An example is provided by a directory service conforming to the ITU-T ITU-T X.500.	ITU-T X.843
distributed ledger	A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.	ITU-T X.1400
distributed ledger technology (DLT)	Technology that enables the operation and use of distributed ledgers.	ITU-T X.1400
eavesdropping	A breach of confidentiality by monitoring communication. 5) (Threat in SDN resource layer:) An attacker may eavesdrop on flows between SDN switches to see what flows are in use, what traffic is being permitted across the network and what data contents are being transported. 6) (Threat in SDN to the application-control interface:) An attacker can use information gathered through eavesdropping of messages to deduce network policies and to use them to elevate the attack. 7) (Threat in SDN to the resource-control interface:) An attacker can use information gathered through eavesdropping of control messages to map out the network routing policies and to use this to elevate the attack.	ITU-T M.3016.0 ITU-T X.1038
electrocardiogram	An electrophysiological monitoring method to record the electrical activity of the heart over a period of time using electrodes placed on the skin. These electrodes detect the tiny electrical changes on the skin that arise from the electrophysiological depolarization pattern of the heart muscle during each heartbeat.	ITU-T X.1094
encipherment	1. The cryptographic transformation of data (see cryptography) to produce ciphertext. Note – Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed. 2. Encipherment (encryption) is the process of making data unreadable to unauthorized entities by applying a cryptographic algorithm (an encryption algorithm). Decipherment (decryption) is the reverse operation by which the ciphertext is transformed to the plaintext.	ITU-T X.800 ITU-T H.235
encryption	1. A method used to translate information in plaintext into ciphertext. 2. The process of scrambling signals to avoid unauthorized access. (See also encipherment)	ITU-T J.170 ITU-T J.93
end-to-end encipherment	Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system.	ITU-T X.800

Pre-published

Pre-published

Term	Definition	Reference
entity	1. A human being, an organization, a hardware component or a piece of software. 2. Any concrete or abstract thing of interest. While in general the word entity can be used to refer to anything, in the context of modelling it is reserved to refer to things in the universe of discourse being modelled. 3. Anything that has a separately identifiable existence (e.g., organization, person, group, etc.).	ITU-T X.842 ITU-T X.902 ITU-T X.1215
entity authentication	Corroboration of the identity of a principal, within the context of a communication relationship. Note – The principal's authenticated identity is assured only when this service is invoked. Assurance of continuity of authentication can be obtained by methods described in 5.2.7/ITU-T X.811.	ITU-T X.811
evidence	Information that, either by itself or when used in conjunction with other information, may be used to resolve a dispute. Note – Particular forms of evidence are digital signatures, secure envelopes and security tokens. Digital signatures are used with public-key techniques while secure envelopes and security tokens are used with secret key techniques.	ITU-T X.813
firewall	1. Type of security barrier placed between network environments – consisting of a dedicated device or a composite of several components and techniques – through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic, as defined by the local security policy, is allowed to pass. 2. A device or service at the junction of two network segments that inspects every packet that attempts to cross the boundary. It also rejects any packet that is disqualified by certain criteria, such as the presence of disallowed port numbers or IP addresses. NOTE – Firewall services can be separated from physical devices and work as an application.	ITU-T X.1038 ITU-T X.1042
forgery	An entity fabricates information and claims that such information was received from another entity or sent to another entity.	ITU-T M.3016.0
fork	Creation of two or more different versions of a distributed ledger. NOTE – There are two types of forks: hard fork (see 6.28 and Figure 1) and soft fork (see 6.56 and Figure 3)	ITU-T X.1400
hash function	A (mathematical) function that maps values from a (possibly very) large set of values into a smaller range of values.	ITU-T X.810
hub-spokes	An incident information exchange model, which often has a central hub that receives data from the participating members (i.e., spokes). Either the hub can redistribute the incoming data directly to other members, or it can provide value-added services and send the new (and presumably more useful) information to the members. With this approach, the hub acts as a clearinghouse that can facilitate information sharing while protecting the identities of the members. A related challenge is that sharing information in this model requires a high degree of trust in the hub.	ITU-T X.1550
information disclosure	1. (Threat in SDN application layer:) It is possible for attackers to get user's credentials and then to masquerade as a legitimate user to inject forged flows into network through SDN application. 2. (Threat in SDN control layer:) It is possible for attackers to get sensitive system information (e.g., configuration data, user credentials) for a future attack. 3. (Threat in SDN resource layer:) It is possible for attackers to get sensitive system information (e.g., flow table, configuration data) for a future attack.	ITU-T X.1038

Term	Definition	Reference
instant messaging	An exchange of content between a set of participants in near real time. Generally, the content is short text messages, although that need not be the case.	ITU-T X.1248
integrity	The property that data has not been altered in an unauthorized manner. (See also data integrity)	ITU-T H.235
integrity service	The integrity service provides means to ensure the correctness of exchanged data, protecting against modification, deletion, creation (insertion) and replay of exchanged data. The following kinds of integrity services are distinguished: selective field integrity; connection integrity without recovery; connection integrity with recovery.	ITU-T M.3016.2
intentional threats	Threats that may range from casual examination using easily available monitoring tools to sophisticated attacks using special system knowledge. An intentional threat, if realized, may be considered to be an "attack".	ITU-T X.800
intrusion detection system	Information systems used to identify that an intrusion has been attempted, is occurring, or has occurred.	ITU-T X.1038
IP-based network	A network in which the Internet Protocol is used as the ISO layer 3 protocol (OSI Reference Model).	ITU-T X.1246
IPCablecom	An ITU-T project that includes an architecture and a series of Recommendations that enable the delivery of real-time services over the cable television networks using cable modems.	ITU-T J.160
Kerberos	A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.	ITU-T J.170
key	1. A sequence of symbols that controls the operations of encipherment and decipherment. 2. A mathematical value input into the selected cryptographic algorithm.	ITU-T X.800 ITU-T J.170
key exchange	The swapping of public keys between entities to be used to encrypt communication between the entities.	ITU-T J.170
key management	The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.	ITU-T X.800
ledger	Information store that keeps final and definitive (immutable) records of transactions.	ITU-T X.1400
logical access control	A mechanism that performs the granting or denying of access for computers, programs, processes, and information systems.	ITU-T X.1093
malware	1. Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability. firewaNOTE – Viruses, Trojan horses, worms, spyware, adware, rootkits are examples of malware. 2. Malware [is a STIX 2.0 domain object (SDO) and] is a type of TTP that is also known as malicious code and malicious software, and refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim.	ITU-T X.Sup29 ITU-T X.1215
man-in-the-middle attack	An attack in which an attacker is able to read, insert and modify at will messages between two parties without either party knowing that the link between them has been compromised.	ITU-T X.1151

Pre-published

Term	Definition	Reference
mandatory access control	An access control model, which is most often used in systems where priority is placed on data confidentiality. MAC works by assigning a classification label to each file resource. Classifications include a category of information and a sensitivity level, for example: confidential, secret or top secret. Each subject is assigned a similar classification, called a clearance. When a subject tries to access a specific resource, the system checks the subject's privileges to determine whether access will be granted, as well as compares the clearance of the subject against the classification of the resource.	ITU-T X.1550
masquerade	The pretence by an entity to be a different entity.	ITU-T X.800
mobile in-application advertising	An advertisement displayed within a mobile application. It can be displayed on the mobile device's screen as a banner at the top or bottom of the screen, mobile interstitial, or as an overlay, etc.	ITU-T X.1249
mobile in-application advertising spam	Mobile in-application advertising which is usually unsolicited, unwanted, and harmful for recipients. NOTE 1: "unsolicited" herein means "user not asked for", and "unwanted" means that users have done something to clearly express his rejection, such as turning off the option of receiving some kinds of advertising. NOTE 2 -- Mobile in-application advertising spam is usually sent indiscriminately, in bulk and repetitively. Examples of actual and tangible harm include fraud or conveyance of malicious code.	ITU-T X.1249
mobile in-application advertising spam database	This database is used for storing mobile in-application advertising spam characteristics. It is a logical database and could be maintained by each service provider or shared by several service providers. Mobile in-application advertising spam characteristics from the database can be used for comparing and filtering. Enriching the mobile in-application advertising spam database can help to improve the performance of the rules engine. The mobile in-application advertising spam database can be enriched by the feedback platform extracting characteristics from newly identified mobile in-application advertising spam.	ITU-T X.1249
mobile messaging spam	1)a Unsolicited electronic communications over mobile messaging services, typically consisting of short message service (SMS) spam and multimedia message service (MMS) spam. 1)b Unsolicited electronic communications over mobile messaging services, typically consisting of SMS spam and MMS spam.	ITU-T X.1247 ITU-T X.Sup12
multimedia message spam	Spam sent via MMS.	ITU-T X.1247
mutual authentication	The assurance of the identities of both principals.	ITU-T X.811
network monitoring	Process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis.	ITU-T X.1361
network resources	1) Network devices that can perform packet forwarding in a network system. The network resources include network switch, router, gateway, WiFi access points, and similar devices. 2) A device that performs packet forwarding in a network system. Note -- Network resources include network switches, routers, gateways, and WiFi access points.	ITU-T X.1038 ITU-T X.1042
non-repudiation	1. The ability to prevent a sender from denying later that he or she sent a message or performed an action.	ITU-T J.170 ITU-T H.235

Pre-published

Term	Definition	Reference
	2. Protection from denial by one of the entities involved in a communication of having participated in all or part of the communication. 3. A process by which the sender of a message (e.g. a request on a pay-per-view) cannot deny having sent the message.	ITU-T J.93
notarization	The registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery.	ITU-T X.800
object	A person, a department, a professional or some other type of object about which there is information and which is identifiable by a distinguished name.	ITU-T X.1080.0
passive threat	The threat of unauthorized disclosure of information without changing the state of the system.	ITU-T X.800
password	1. Confidential authentication information, usually composed of a string of characters. 2. Referring to a user-entered password string: is understood to be the assigned security key, which the mobile user shares with his home domain. This user password and derived user shared secret shall be applied for the purpose of user authentication.	ITU-T X.800 ITU-T H.530
permissioned distributed ledger system	Distributed ledger system in which permissions are required to maintain and operate a node.	ITU-T X.1400
permissionless distributed ledger system	Distributed ledger system where permissions are not required to maintain and operate a node.	ITU-T X.1400
personally identifiable information	Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal. NOTE – To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.	ITU-T X.1361
phishing	An attack to acquire sensitive information such as usernames, passwords, and credit card details for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.	ITU-T X.Sup29
photoplethysmogram	An optical measurement signal of heart rate or skin blood pulse wave by means that illuminate the skin and measure changes in light absorption.	ITU-T X.1094
physical access control	Electro-mechanical suite that performs the granting or denying of access at controlled entry points of a facility.	ITU-T X.1093
physical security	The measures used to provide physical protection of resources against deliberate and accidental threats.	ITU-T X.800
PII breach	Situation where personally identifiable information is processed in violation of one or more relevant PII protection requirements.	ITU-T X.1361
platform or software security	The vulnerabilities of software platforms and third-party components, generally used in the development of value-added services, directly affect service security.	ITU-T X.1146
post-to-all	An incident information exchange model, which enables any participant to share with the entire membership roster, rather than going through a central hub. Because members share directly with one another, information dissemination is quick and can be easily scaled to many participants.	ITU-T X.1550
preprocessing component	The preprocessing component [to counter mobile in-application advertising spam] is used to pre-process the original ad files to convert them to the format required by the filtering engines, such as	ITU-T X.1249

Pre-published

Term	Definition	Reference
	separating the contents of text, image, uniform resource locator (URL), audio and video, etc.	
principal	An entity whose identity can be authenticated.	ITU-T X.811
privacy	1. The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. Note – Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security. 2. A mode of communication in which only the explicitly enabled parties can interpret the communication. This is typically achieved by encryption and shared key(s) for the cipher.	ITU-T X.800 ITU-T H.235
private DLT system	A distributed ledger technology (DLT) system which is accessible for use only to a limited group of DLT users.	ITU-T X.1400
private key	1. (In a public-key cryptosystem) that key of a user's key pair which is known only by that user. 2. A key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity). 3. The key used in public-key cryptography that belongs to an individual entity and must be kept secret.	ITU-T X.509 ITU-T X.810 ITU-T J.170
privilege	An attribute or property assigned to an entity by an authority.	ITU-T X.509
privilege management infrastructure (PMI)	The infrastructure able to support the management of privileges in support of a comprehensive authorization service and in relationship with a public-key infrastructure.	ITU-T X.509
proof of work	Consensus process to solve a difficult (costly, time-consuming) problem that produces a result that is easy for others to verify. NOTE – Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. Bitcoin uses the Hash cash proof of work system.	ITU-T X.1400
proof of stake	Consensus process, where an existing stake in the distributed ledger system (e.g., the amount of that currency that you hold) is used to reach consensus.	ITU-T X.1400
public DLT system	A distributed ledger technology (DLT) system which is accessible to the public for use.	ITU-T X.1400
public key	1. (In a public-key cryptosystem) that key of a user's key pair which is publicly known. 2. A key that is used with an asymmetric cryptographic algorithm and that can be made publicly available. 3. The key used in public-key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.	ITU-T X.509 ITU-T X.810 ITU-T J.170
public-key certificate	1. The public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it. 2. Values that represent an owner's public key (and other optional information) as verified and signed by a trusted authority in an unforgeable format. 3. A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.	ITU-T X.509 ITU-T H.235 ITU-T J.170

Pre-published

Term	Definition	Reference
public-key cryptography	A cryptographic technique based upon a two-key algorithm, private and public, wherein a message is encrypted with the public key but can only be decrypted with the private key. Also known as a Private-Public Key (PPK) system. Note – Knowing the public key does not reveal the private key. Example: Party A would devise such a private and public key, and send the public key openly to all who might wish to communicate with Party A, but retain the private key in secret. Then, while any who have the public key can encrypt a message for Party A, only Party A with the private key can decrypt the messages.	ITU-T J.93
public-key infrastructure (PKI)	The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.	ITU-T X.509
relying party	A user or agent that relies on the data in a certificate in making decisions.	ITU-T X.509
replay	A message, or part of a message, is repeated to produce unauthorized effect. For example, a valid message containing authentication information may be replayed by another entity in order to authenticate itself (as something that it is not).	ITU-T X.800
repudiation	1. Denial by one of the entities involved in a communication of having participated in all or part of the communication. 2. An entity involved in a communication exchange subsequently denies the fact. 3. (In an MHS the case) when an MTS-user or the MTS may later deny submitting, receiving, or originating a message, and include: denial of origin, denial of submission, denial of delivery. 5. (Threat in SDN application layer:) A user or an administrator, enforcing a malicious network policy (e.g., copying and forwarding specific traffic flows to a malicious server), may claim that he/she did not make such network policy enforcement. 6. (Threat in SDN control layer:) An administrator or a SDN application, inserting malicious flow rules into the flow table to make inside attacks, may claim that he/she did not insert such malicious flow rules into the flow table. 7) (Threat in SDN resource layer:) An administrator or a SDN controller may make incorrect configuration and later claim that he/she did not do such attacks.	ITU-T X.800 ITU-T M.3016.0 ITU-T X.402 ITU-T X.1038
revocation list certificate	A security certificate that identifies a list of security certificates that have been revoked.	ITU-T X.810
risk-adaptive access control	An access control model, which was devised to bring real-time, adaptable, risk-aware access control. It extends other earlier access control models by introducing environmental conditions and risk levels into the access control decision process. It combines information about a person's (or a machine's) trustworthiness, information about the corporate information technology (IT) infrastructure, and environmental risk factors, and uses all of this information to create an overall quantifiable risk metric. RAdAC also uses situational factors as input for the decision-making process. These situational inputs could include information on the current threat level an organization faces based on data gathered from other sources, such as computer emergency response teams (CERTs), computer security incident response teams (CSIRTs) or security vendors.	ITU-T X.1550
role-based access control	An access control model, in which the access to a resource is determined based on the relationship between the requester and the organization or owner in control of the resource; the requester's role or function will determine whether access will be granted or denied.	ITU-T X.1550

Pre-published

Term	Definition	Reference
SDN application	1. A service that explicitly, directly and programmatically communicates its network requirements and desired network behaviour to the SDN controller via a northbound interface such as the ACI in Figure 6-2/X.1042. In addition, they may consume an abstracted view of the network for their internal decision-making purposes. For example, firewall, honeypot, DDoS mitigation and illegal device management services can be provided as applications. These SDN applications are required to interact with the ALM through the AL-MSO for fault, configuration, accounting, performance and security management. And these applications make access rules, thus they are also required to interact with the SDN-CL via ACIs so that access rules are implemented. 2. SDN applications are programs that explicitly, directly, and programmatically communicate their network requirements and desired network behaviour (i.e., network policies) to the SDN controller via application-controller interfaces. The controller converts these network policies into flow entries and inserts them into the flow table. However, currently a flow entry in OpenFlow flow table does not distinguish the application generating the new flow entry from another application generating the old flow entry. So, it is possible that a new network policy generated by a general application can replace a non-bypass security policy predefined by the security administrator.	ITU-T X.1042 ITU-T X.1038
SDN controller	A logically centralized entity in charge of (i) translating the requirements from SDN applications to SDN switches and (ii) providing abstract network views to applications with useful network information such as traffic statistics and events. That is, SDN controller makes flow entries based on access rules it gets from SDN applications. Therefore, the SDN controller is required to interact with the CLM, SDN applications and the SDN-RL.	ITU-T X.1042
SDN switch	A software program or hardware device that forwards packets in a SDN environment. SDN switches are capable of storing packet forwarding rules managed by a SDN controller via a southbound interface such as RCI in Figure 6-2/X.1042. So, the SDN switch is required to interact with the resource layer management (RLM) and the SDN-CL.	ITU-T X.1042
secret key	A key that is used with a symmetric cryptographic algorithm. Possession of a secret key is restricted (usually to two entities).	ITU-T X.810
security	The term "security" is used in the sense of minimizing the vulnerabilities of assets and resources. An asset is anything of value. A vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential violation of security.	ITU-T X.800
security alarm	A message generated when a security-related event that is defined by security policy as being an alarm condition has been detected. A security alarm is intended to come to the attention of appropriate entities in a timely manner.	ITU-T X.816
security audit	An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.	ITU-T X.800
security audit trail	Data collected and potentially used to facilitate a security audit.	ITU-T X.800

Pre-published

Term	Definition	Reference
security certificate	A set of security-relevant data issued by a security authority or trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data. Note – All certificates are deemed to be security certificates. The term security certificate in the ITU-T X.800 series is adopted in order to avoid terminology conflicts with ITU-T X.509.	ITU-T X.810
security domain	1. A collection of users and systems subject to a common security policy. 2. The set of resources subject to a single security policy.	ITU-T X.841 ITU-T X.411
security gateway	Point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy in the IoT environment. NOTE – It is adapted from ISO/IEC 27033-1 and referred as 'gateway' in this Recommendation.	ITU-T X.1361
security information (SI)	Information needed to implement security services.	ITU-T X.810
security management	Security management comprises all activities to establish, maintain and terminate the security aspects of a system. Topics covered are: management of security services; installation of security mechanisms; key management (management part); establishment of identities, keys, access control information, etc.; management of security audit trail and security alarms.	ITU-T M.3016.0
security manager	An ALM function which transfers security policies to SDN application. So the SM is required to interact with SDN applications through the AL-MSO.	ITU-T X.1042
security model	A framework for describing the security services that counter potential threats to the MTS and the security elements that support those services.	ITU-T X.402
security policy	1. The set of rules laid down by the security authority governing the use and provision of security services and facilities. 2. The set of criteria for the provision of security services. Note – See identity-based and rule-based security policy. A complete security policy will necessarily address many concerns which are outside of the scope of OSI.	ITU-T X.509 ITU-T X.800
security service	A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.	ITU-T X.800
security threat (threat)	A potential violation of security	ITU-T X.800
security token	A set of data protected by one or more security services, together with security information used in the provision of those security services, that is transferred between communicating entities.	ITU-T X.810
sensitivity	Characteristic of a resource that implies its value or importance.	ITU-T X.509
sensor-on-card	Sensor-on-card refers to a card that is designed to perform the entire biometric recognition process inside the IC card. Therefore, the IC card can process live biometrics, extract features and compare the stored biometric references, and so additional computational power is required. When this sensor-on-card is adopted, not only the registered biometric reference but also the acquired biometric information is not transmitted outside of the card, which is a useful method for securing the biometric security of the user. This can be divided into two types as shown in Figure 7/X.1093 and Figure 8/X.1093, depending on	ITU-T X.1093

Pre-published

Term	Definition	Reference
	whether or not there is a digital signature function with an ITU-T X.509 certificate.	
service function	A function that is responsible for specific treatment of received packets. A service function can act at various layers of a protocol stack (e.g., at the network layer or other OSI layers). As a logical component, a service function can be realized as a virtual element or be embedded in a physical network element. One or more service functions can be embedded in the same network element. Multiple occurrences of the service function can exist in the same administrative domain.	ITU-T X.1043
service function chain	A service function chain defines an ordered set of abstract service functions and ordering constraints that must be applied to packets and/or frames and/or flows selected as a result of classification.	ITU-T X.1043
service provider	An entity that provides services to the clients or to the other service providers.	ITU-T X.1258
shared secret	Refers to the security key for the cryptographic algorithms; it may be derived from a password.	ITU-T H.530
signature	See digital signature.	ITU-T X.800
simple authentication	Authentication by means of simple password arrangements.	ITU-T X.509
smart contract	A program written on a distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that can be validated and triggered by specific conditions.	ITU-T X.1400
smart grid	Intelligent power grid equipped with information communication technologies. With a smart grid, electricity utilities can estimate electricity demand based on customer electricity usage information collected from smart meters. Consequently, utilities might then control the peak load situation based on the estimation. Before an electrical peak load occurs, a utility reduces customer usage or makes the customer switch to alternative sources generated by a distributed electricity resource (DER) in the customer premises, such as polar voltaic devices on the roof, electricity stores or electric vehicles (EVs). Moreover, the customer can delay or bring forward electricity usage based on peak load time information from the utility.	ITU-T X.1331
smart ID card	A contact or contactless type of any pocket sized card that has embedded integrated circuits that hold a user's identity information. This can employs a PKI, which stores an encrypted digital certificate issued from the PKI provider with other relevant identity information.	ITU-T X.1093
soft fork	Change to the protocol or rules that result in a fork that is backward compatible.	ITU-T X.1400
software-defined networking	1)c A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.	ITU-T Y.3302
source of authority (SOA)	An Attribute Authority that a privilege verifier for a particular resource trusts as the ultimate authority to assign a set of privileges.	ITU-T X.509
spam	Unsolicited and unwanted e-mail	ITU-T H.235
specification	An ITU-T Recommendation, an International Standard or any specification developed by a recognized Standards Developing Organization (SDO).	ITU-T X.1080.0

Pre-published

Term	Definition	Reference
spoofed call	Spoofed calls are a type of call that exists in the telecommunication voice service. Spoofed calls are identity faked or identity modified of unwanted and unsolicited calls with the objective of fraud, vishing, identity (ID) theft, etc. Note: Both in the traditional network and in the fourth generation (4G) network, spoofed calls are generated due to protocol and management vulnerabilities. However, in the traditional network, once a spoofed call arrives at the terminated network, operators can scarcely identify whether an incoming call user identity (mostly from other networks) is spoofed or not.	ITU-T X.Sup28
spoofing	Impersonating a legitimate resource or user 2) (Threat in SDN application layer:) An attacker masquerades as a SDN controller to get the service level agreement (SLA) or users' data (e.g., user identification, credentials) or service logic and use it for the future attack. 3) (Threat in SDN control layer:) An attacker may impersonate an administrator or a SDN application to remove or modify sensitive data (e.g., configuration data, user data) from the SDN controller or to obtain network topology information and routing information or even to have complete control of the SDN controller. By spoofing the address of a SDN controller, an attacker can take the control of the entire network by creating a fake SDN controller. Moreover, an attacker may create a fake SDN switch to perform network reconnaissance by observing how the controller responds to different packets which are generated by the fake SDN switch. 4) (Threat in SDN resource layer:) An attacker may impersonate an administrator or a SDN controller to remove or modify sensitive data (e.g., configuration data, flow table) from the SDN switch or to obtain sensitive information such as flow entries in the flow table.	ITU-T X.509 ITU-T X.1038
store-on-card	Store-on-card refers to a card that is designed to perform a comparison of biometric information outside the smart IC card, and thus the IC card is used only as a storage medium for storing biometric references. This can be divided into two types as shown in Figure 3/X.1093 and Figure 4/X.1093, depending on whether or not there is a digital signature function with an ITU-T X.509 certificate.	ITU-T X.1093
strong authentication	Authentication by means of cryptographically derived credentials.	ITU-T X.811
structured threat information expression (STIX)	A language and serialization format used to exchange cyber threat intelligence (CTI). A structured, expressive, flexible, extensible, automatable, and readable language to describe cyber threat information.	ITU-T X.1215
Sybil attack	An attack in which the reputation system of a peer-to-peer network is subverted by creating a large number of pseudonymous entities and using them to gain a disproportionately large influence.	
task-based access control	An access control model, which is an extension of RBAC based on defining business tasks which allow finer granularity for access control.	ITU-T X.1550
thing	With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.	ITU-T X.1361
threat	A potential violation of security.	ITU-T X.800
token	See security token	

Pre-published

Term	Definition	Reference
	In FIDO U2F, the term "token" is often used to mean what is called an authenticator in UAF. NOTE – Other uses of "token", e.g. KHAccess token, user verification token, etc., are separately distinct. If they are not explicitly defined, their meaning needs to be determined from context.	ITU-T X.1277
Trojan horse	When introduced to the system, the Trojan horse has an unauthorized function in addition to its authorized function. A relay that also copies messages to an unauthorized channel is a Trojan Horse.	ITU-T X.800
trust	Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.	ITU-T X.810
trusted functionality	Functionality perceived to be correct with respect to some criteria, e.g., as established by a security policy.	ITU-T X.800
trusted third party (TTP)	A security authority or its agent that is trusted (by other entities) with respect to some security-relevant activities (in the context of a security policy).	ITU-T X.810
Ubiquitous sensor network (USN)	A network that uses low cost, low power sensors to develop context awareness in order to deliver sensed information and knowledge services to anyone, anywhere and at anytime. A USN may cover a wide geographical area and may support a variety of applications.	
unauthorized access	An entity attempts to access data in violation of the security policy in force.	ITU-T M.3016.0
universal authentication framework	The FIDO protocol and family of authenticators which enable a service to offer its users flexible and interoperable authentication. NOTE – This protocol allows triggering the authentication before the server knows the user.	ITU-T X.1277
user authentication	Establishing proof of the identity of the human user or application process.	ITU-T M.3016.0
user identity authentication	A method of confirming the user's identity. According to the verification result, the value-added service reacts appropriately. Generally speaking, there are mainly three ways of verifying a user's identity, based on: – what the user knows, e.g., a password (static); – what the user has possession of, for example, a smart card, a SMS password, a universal serial bus key or a dynamic password; – who the user is, based on unique physical characteristics, e.g., fingerprints, handwriting, DNA, retinal imaging and body biometrics.	ITU-T X.1146
value-added service	A service that is offered in addition to or in conjunction with basic telecommunication services such as voice call, short message service (SMS), multimedia messaging service (MMS) and data access. These value-added services allow operators to drive up their average revenue per user (ARPU). The scope of value-added services in this Recommendation is limited to those provided by telecommunication operators and the servers hosting such services reside in operators' networks. Typical value-added services include mobile office automation, e-reading and e-commerce.	ITU-T X.1146
verifier	An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.	ITU-T X.811
virtual machine	The complete environment that supports the execution of guest software. NOTE – A virtual machine is a full encapsulation of the virtual hardware, virtual disks, and the metadata associated with it. Virtual machines allow multiplexing of the underlying physical machine through a software layer called a hypervisor.	ITU-T X.1631

Pre-published

Term	Definition	Reference
voice spam	Unsolicited, automatically dialled, pre-recorded phone calls, usually with the objective of marketing commercial products or services. The content of voice spam ranges from advertisement of goods to offensive pornographic materials. Voice spam may have various kinds of harmful effects on users and operators.	ITU-T X.1246
vulnerability	1. Any weakness that could be exploited to violate a system or the information it contains. 2. Weakness of an asset or control that can be exploited by one or more threats. 3. A vulnerability [is a STIX 2.0 domain object (SDO) and] is "a mistake in software that can be directly used by a hacker to gain access to a system or network".	ITU-T X.800 ITU-T X.1361 ITU-T X.1215
vulnerability management	The process that consists of identifying, classifying, remediating, and mitigating vulnerabilities.	ITU-T X.1361
wallet	Software and/or hardware used to generate, manage and store both private and public keys and addresses, which enable distributed ledger technology (DLT) users to transact. Some wallets may interact with smart contracts and allow single and/or multi-signature.	ITU-T X.1400
whitelist	see blacklists\whitelists	ITU-T X.1249
ITU-T X.509 certificate	A public-key certificate specification developed as part of the ITU-T X.500 standards directory.	ITU-T J.170

Pre-published

Annex B

Acronyms and abbreviations

Pre-published

Annex B: Acronyms and abbreviations

Acronym	Meaning
ABAC	Attribute-Based Access Control
ACI	Access Control Information *Application Control Interface (Y.3302)*
ACM	Access Control Management
AES	Advanced Encryption Standard Algorithm
AL	Application Layer
ALM	Application Layer Management
AL-MSO	Application Layer Management Support and Orchestration
ARPU	Average Revenue Per User
ASM	Application-specific Module Authenticator Specific Module
ASN.1	Abstract Syntax Notation One
ASP	Application Service Provider
ATIS	Alliance for Telecommunications Industry Solutions
Authnr	authenticator
A/V	Audio-visual
B2C	Business-to-Customer
BaaS	Blockchain as a Service
BCG	Ballistocardiogram
BioAPI	Biometric Application Program/programming Interface
BPON	Broadband Passive Optical Network
CA	Certification Authority
CASF	Core anti-spam functions
CCTV	closed-circuit television
CDC	Cyber Defence Centre
CDMA	Code Division Multiple Access
CISO	Chief Information Security Officer
CIRT	Computer Incident Response Team
CL	Control Layer
CL-AS	Control Layer Application Support
CLM	Control Layer Management
CL-MSO	Control Layer Management Support and Orchestration
CL-RA	Control Layer Resource Abstraction
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSO	Chief Security Officer
CVE	Common vulnerabilities and exposures

Pre-published

Acronym	Meaning
CVSS	Common vulnerability scoring system
CYBEX	Cybersecurity information exchange
DAO	Decentralized Autonomous Organization
DLT	Distributed Ledger Technology
DNS	Domain Name Server/System/Service
DPoS	Delegated Proof of Stake
DSL	Digital Subscriber Loop
EAP	Extensible Authentication Protocol
ECU	Electronic Control Unit
EEG	Electroencephalogram
ENISA	European Network and Information Security Agency
ETC	Electronic Toll Collection
ETSI	European Telecommunications Standards Institute
FIDO	Fast IDentity On-line
FMC	Fixed Mobile Convergence
FW	Firewall
GK	Gatekeeper
GPRS	General Packet Radio System
GSM	Global System for Mobile communications
GW	Gateway
HAN	Home Area Network
HFX	Hawthorne Facsimile Cipher
HKM	Hawthorne Key Management algorithm
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
ID	Identifier Identity (X.Sup28)
IdM	Identity Management
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IJCSIT	International Journal of Computer Science and Information Technology
IKE	Internet Key Exchange is a key management mechanism used to negotiate and derive keys for SAs in IPSec.
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IMT-2000	International Mobile Telecommunications 2000
IODEF	incident object description exchange format
IoT	Internet of things
IP	Internet Protocol
IPSec	Internet Protocol Security

Pre-published

Acronym	Meaning
IPTV	Internet Protocol TeleVision
IPX	Internet Packet Exchange
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITU-T	Telecommunication Standardization Sector of the International Telecommunication Union
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest No. 5 (a secure hash algorithm)
MIKEY	Multimedia Internet Keying
MMF	Multi-layer Management Function
MMFA	Multi-layer Management Function Application layer
MMFC	Multi-layer Management Function Control layer
MMFR	Multi-layer Management Function Resource layer
MMS	Multimedia Messaging Service
MTA	Message Transfer Agent (In messaging) Media Terminal Adapter (In cable technology)
MWSSG	Mobile Web Services Security Gateway
NAT	Network Address Translation
NFT	Non Fungible Token
NGN	Next Generation Network
OASIS	Organization for the Advancement of Structured Information Standards
OMG	Object Management Group
ONF	Open Networking Foundation
OSI	Open Systems Interconnection
P2P	Peer-to-peer
PC	Personal Computer
PDA	Personal Data Assistant personal digital assistants (X.1058)
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public-key Infrastructure
PKINIT	Public-key Cryptography Initial Authentication
PMI	Privilege Management Infrastructure
PPG	Photoplethysmogram
PSTN	Public Switched Telephone Network
PUCI	Protection against Unsolicited Communication for IMS
RASF	Recipient-side anti-spam functions
RBAC	Role-Based Access Control
RBL	Real-time blocking list
RCI	Resource Control Interface
RFID	Radio frequency identification

Pre-published

Acronym	Meaning
RII	Rights information interoperability
RL-MS	Resource Layer Management Support
RSA	Rivest, Shamir and Adleman (public-key algorithm)
RTP	Real time protocol
SAML	Security Assertion Mark-up Language Secure Authentication Markup Language (X.1277)
SASF	Sender-side anti-spam functions
SDES	SDP Security Descriptions
SDN	Software-Defined Networking
SDN-AL	Software-Defined Networking - Application Layer
SDN-CL	Software-Defined Networking - Control Layer
SDN-RL	Software-Defined Networking - Resource Layer
SDO	Standards Development Organization
SFC	Service Function Chain
SFF	Service Function Forwarder
SFP	Service Function Path
SG	Study Group
SHA1	Secure Hash Algorithm 1
SIP	Session Initiation Protocol. An application-layer control (signalling) protocol for creating, modifying, and terminating sessions with one or more participants.
SLRTP	Signalling Link Release Time Point
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SoA	Source of Authority
SOA	Service Oriented Architecture
SP	Service provider
SPAK	Secure Password-based Authentication protocol with Key exchange
SRTP	Secure Real-Time Protocol
SSL	Secure Socket Layer
SSO	Single Sign-On
STB	Set-top box
STIX	Structured Threat Information Expression
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TMN	Telecommunication Management Network
TNSS	Telecommunication IP-based network security system
TSP	Token Service Provider
TTP	Trusted Third Party
UAF	Universal Authentication Framework
UE	User Equipment

Pre-published

Acronym	Meaning
UICC	Universal Integrated Circuit Card
URS	User reputation system
USB	universal serial bus
USN	UbiquitousSensor Network
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-X (vehicle/infrastructure)
VMS	Voice Mail Server
VoIP	Voice over IP
VoLTE	Voice over Long-Term Evolution
VPN	Virtual Private Network
VSPPS	VoIP spam prevention policy server
VSPS	VoIP spam prevention system
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity (trademark of the Wi-Fi Alliance for certified products based on the IEEE 802.11 standards)
WPA	Wi-Fi Protected Access
WTSA	World Telecommunication Standardization Assembly
XACML	eXtensible Access Control Mark-up Language
XML	eXtensible Mark-up Language
3G	3rd Generation
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
5G	fifth Generation

Pre-published

Annex C

Summary of security-related ITU-T Study Groups

Pre-published

Annex C: Summary of security-related ITU-T Study Groups

The work of most Study Groups includes at least some aspects of telecommunications and/or ICT security. Each Study Group is responsible for addressing security issues within its own area of responsibility, but SG17, which has security as its primary focus, has been designated the Lead Study Group on security. The table below summarizes the roles of Study Groups with security-related responsibilities and lists their respective Lead Study Group responsibilities during the 2017-2020 Study Period.

Study Group	Title	Responsibilities/Security role
SG2	Operational aspects	Lead study group on numbering, naming, addressing, identification and routing Lead Study Group for service definition Lead Study Group on telecommunications for disaster relief/early warning, network resilience and recovery Lead Study Group on telecommunication management
SG3	Tariff and accounting principles and international telecommunication/ICT economic and policy issues	Lead study group on tariff and accounting principles relating to international telecommunications/ICT Lead study group on economic issues relating to international telecommunications/ICT Lead study group on policy issues relating to international telecommunications/ICT
SG5	Environment, climate change and circular economy	Lead Study Group on electromagnetic compatibility, lightning protection, and electromagnetic effects Lead Study Group on ICTs related to the environment, climate change, energy efficiency and clean energy Lead study group on circular economy, including e-waste
SG9	Broadband cable and TV	Lead Study Group on integrated broadband cable and television networks
SG11	Signalling requirements, protocols, test specifications and combating counterfeit products	Lead Study Group on signalling and protocols, including for IMT-2020 technologies Lead Study Group on test specifications, conformance and interoperability testing for all types of networks, technologies and services that are the subject of study and standardization by all ITU-T study groups Lead study group on combating counterfeiting of ICT devices Lead study group on combating the use of stolen ICT devices
SG12	Performance, QoS and QoE	Lead Study Group on quality of service and quality of experience Lead Study Group on driver distraction and voice aspects of car communications Lead study group on quality assessment of video communications and applications
SG13	Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures	Lead Study Group on future networks such as IMT-2020 networks (non-radio related parts) Lead Study Group on mobility management Lead Study Group on cloud computing Lead Study Group on software-defined network infrastructure
SG15	Transport, access and home	Lead Study Group on access network transport Lead study group on home networking Lead Study Group on optical technology Lead Study Group on smart grid
SG16	Multimedia coding, systems and applications	Lead study group on multimedia coding, systems and applications Lead study group on ubiquitous multimedia applications Lead study group on telecommunication/ICT accessibility for persons with disabilities Lead study group on human factors Lead study group on multimedia aspects of intelligent transport system (ITS) communications Lead study group on Internet Protocol television (IPTV) and digital signage Lead study group on multimedia aspects of e-services

Pre-published

SG17	Security	Lead Study Group on telecommunication security Lead Study Group on identity management Lead Study Group on languages and description techniques
SG20	Internet of Things (IoT) and its applications including smart cities and communities (SC&C)	Lead study group on Internet of things (IoT) and its applications Lead study group on smart cities and communities, including its e-services and smart services Lead study group for Internet of things identification

Pre-published

Annex D

Security Recommendations and other publications referenced in this manual

Pre-published

Annex D: Security Recommendations and other publications referenced in this manual

This annex contains a complete listing of all ITU-T Recommendations referenced in this manual along with hyperlinks so that those readers who are using an electronic version of the text can link directly to download the Recommendations. As noted in the text, ITU-T has developed many security-related standards in collaboration with other standards development organizations. Currently published, common/twin text Recommendations relating to ICT security are also included in this table. The complete set of ITU-T Recommendations is accessible on line at: http://www.itu.int/en/ITU-T/publications/Pages/recs.aspx. ITU-T security-related Recommendations are available via Part 2 (Database) of the Security Standards Roadmap (https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/default.aspx).

Recommendation	Title	Equivalent text
ITU-T E.408	Telecommunication networks security requirements	
ITU-T E.409	Incident organization and security incident handling: Guidelines for telecommunication organizations	
ITU-T F.744	Service description and requirements for ubiquitous sensor network middleware	
ITU-T G.827	Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths	
ITU-T G.1000	Communications Quality of Service: A framework and definitions	
ITU-T G.1030	Estimating end-to-end performance in IP networks for data applications	
ITU-T G.1050	Network model for evaluating multimedia transmission performance over Internet Protocol	
ITU-T G.1081	Performance monitoring points for IPTV	
ITU-T H.235.0	H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems	
ITU-T H.235.1	H.323 security: Baseline security profile	
ITU-T H.235.2	H.323 security: Signature security profile	
ITU-T H.235.3	H.323 security: Hybrid security profile	
ITU-T H.235.4	H.323 security: Direct and selective routed call security	
ITU-T H.235.5	H.323 security: Framework for secure authentication in RAS using weak shared secrets	
ITU-T H.235.6	H.323 security: Voice encryption profile with native H.235/H.245 key management	
ITU-T H.235.7	H.323 security: Usage of the MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235	
ITU-T H.235.8	H.323 security: Key exchange for SRTP using secure signalling channels	
ITU-T H.235.9	H.323 security: Security gateway support for H.323	
ITU-T H.235 Implementers' Guide	Implementors Guide for ITU-T H.235 V3: "Security and encryption for H-series (ITU-T H.323 and other ITU-T H.245-based) multimedia terminals"	
ITU-T H.323	Packet-based multimedia communications systems	
ITU-T H.350	Directory services architecture for multimedia conferencing	
ITU-T H.460.17	Using H.225.0 call signalling connection as transport for H.323 RAS messages	

Pre-published

Recommendation	Title	Equivalent text
ITU-T H.460.18	Traversal of H.323 signalling across network address translators and firewalls	
ITU-T H.460.19	Traversal of H.323 media across network address translators and firewalls	
ITU-T H.460.22	Negotiation of security protocols to protect H.225.0 call signalling messages	
ITU-T H.460.23	Network address translator and firewall device determination in ITU-T H.323 systems	
ITU-T H.460.24	Point-to-point media through network address translators and firewalls within ITU-T H.323 systems	
ITU-T H.460.26	Using ITU-T H.225.0 call signalling connection as transport for media	
ITU-T H.510	Mobility for H.323 multimedia systems and services	
ITU-T H.530	Symmetric security procedures for H.323 mobility in H.510	
ITU-T H.750	High-level specification of metadata for IPTV services	
ITU-T H.751	Metadata for rights information interoperability in IPTV services	
ITU-T J.160	Architectural framework for the delivery of time-critical services over cable television networks using cable modems	
ITU-T J.170	IPCablecom security specification	
ITU-T J.360	IPCablecom2 architecture framework	
ITU-T K.81	High-power electromagnetic immunity guide for telecommunication systems	
ITU-T K.84	Test methods and guide against information leaks through unintentional electromagnetic emissions	
ITU-T K.87	Guide for the application of electromagnetic security requirements - Overview	
ITU-T M.3010	Principles for a telecommunications management network	
ITU-T M.3016.0	Security for the management plane: Overview	
ITU-T M.3016.1	Security for the management plane: Security requirements	
ITU-T M.3016.2	Security for the management plane: Security services	
ITU-T M.3016.3	Security for the management plane: Security mechanism	
ITU-T M.3016.4	Security for the management plane: Profile proforma	
ITU-T M.3208.2	TMN management services for dedicated and reconfigurable circuits network: Connection management of pre-provisioned service link connections to form a leased circuit service	
ITU-T M.3210.1	TMN management services for IMT-2000 security management	
ITU-T M.3410	Guidelines and requirements for security management systems to support telecommunications management	
ITU-T Q.816	CORBA-based TMN services	
ITU-T Q.816.1	CORBA-based TMN services: Extensions to support coarse-grained interfaces	
ITU-T Q.816.2	CORBA-based TMN services: Extensions to support service-oriented interfaces	
ITU-T Q.834.3	A UML description for management interface requirements for Broadband Passive Optical Networks	

Prepublished

Recommendation	Title	Equivalent text
ITU-T Q.834.4	A CORBA interface specification for Broadband Passive Optical Networks based on UML interface requirements	
ITU-T Q.1701	Framework for IMT-2000 networks	
ITU-T Q.1702	Long-term vision of network aspects for systems beyond IMT-2000	
ITU-T Q.1703	Service and network capabilities framework of network aspects for systems beyond IMT-2000	
ITU-T Q.1741.1	IMT-2000 references to release 1999 of GSM evolved UMTS core network with UTRAN access network	Identifies 3GPP documents
ITU-T Q.1742.1	IMT-2000 references to ANSI-41 evolved core network with cdma2000 access network	Identifies 3GPP2 documents
ITU-T T.4	Standardization of Group 3 facsimile terminals for document transmission	
ITU-T T.36	Security capabilities for use with Group 3 facsimile terminals	
ITU-T T.37	Procedures for the transfer of facsimile data via store-and-forward on the Internet	
ITU-T T.38	Procedures for real-time Group 3 facsimile communication over IP networks	
ITU-T T.563	Terminal characteristics for Group 4 facsimile apparatus	
ITU-T X.500	The Directory: Overview of concepts, models and services	ISO/IEC 9594-1
ITU-T X.501	The Directory: Models	ISO/IEC 9594-2
ITU-T X.509	The Directory: Public-key and attribute certificate frameworks	ISO/IEC 9594-8
ITU-T X.510	Information technology — Open systems interconnection — The directory — Part 11: Protocol specifications for secure operations	ISO/IEC 9594-11
ITU-T X.511	The Directory: Abstract service definition	ISO/IEC 9594-3
ITU-T X.518	The Directory: Procedures for distributed operation	ISO/IEC 9594-4
ITU-T X.519	The Directory: Protocol specifications	ISO/IEC 9594-5
ITU-T X.520	The Directory: Selected attribute types	ISO/IEC 9594-6
ITU-T X.521	The Directory: Selected object classes	ISO/IEC 9594-7
ITU-T X.525	The Directory: Replication	ISO/IEC 9594-9
ITU-T X.530	The Directory: Use of systems management for administration of the Directory	ISO/IEC 9594-10
ITU-T X.711	Common management information protocol: Specification	ISO/IEC 9596-1
ITU-T X.736	Systems Management: Security alarm reporting function	ISO/IEC 10164-7
ITU-T X.740	Systems Management: Security audit trail function	ISO/IEC 10164-8
ITU-T X.741	Systems Management: Objects and attributes for access control	ISO/IEC 10164-9
ITU-T X.780	TMN guidelines for defining CORBA managed objects	
ITU-T X.780.1	TMN guidelines for defining coarse-grained CORBA managed object interfaces	
ITU-T X.780.2	TMN guidelines for defining service-oriented CORBA managed objects and façade objects	
ITU-T X.781	Requirements and guidelines for Implementation Conformance Statements proformas associated with CORBA-based systems	
ITU-T X.790	Trouble management function for ITU-T applications	

Pre-published

Recommendation	Title	Equivalent text
ITU-T X.800	Security architecture for Open Systems Interconnection for CCITT applications	ISO/IEC 7498-2
ITU-T X.802	Lower layers security model	ISO/IEC TR 13594
ITU-T X.803	Upper layers security model	ISO/IEC 10745
ITU-T X.805	Security architecture for systems providing end-to-end communications	ISO/IEC 18028-2
ITU-T X.810	Security frameworks for open systems: Overview	ISO/IEC 10181-1
ITU-T X.811	Security frameworks for open systems: Authentication framework	ISO/IEC 10181-2
ITU-T X.812	Security frameworks for open systems: Access control framework	ISO/IEC 10181-3
ITU-T X.813	Security frameworks for open systems: Non-repudiation framework	ISO/IEC 10181-4
ITU-T X.814	Security frameworks for open systems: Confidentiality framework	ISO/IEC 10181-5
ITU-T X.815	Security frameworks for open systems: Integrity framework	ISO/IEC 10181-6
ITU-T X.816	Security Frameworks for open systems: Security audit and alarms framework	ISO/IEC 10181-7
ITU-T X.830	Generic upper layers security: Overview, models and notation	ISO/IEC 11586-1
ITU-T X.831	Generic upper layers security: Security Exchange Service Element (SESE) service definition	ISO/IEC 11586-2
ITU-T X.832	Generic upper layers security: Security Exchange Service Element (SESE) protocol specification	ISO/IEC 11586-3
ITU-T X.833	Generic upper layers security: Protecting transfer syntax specification	ISO/IEC 11586-4
ITU-T X.834	Generic upper layers security: Security Exchange Service Element (SESE) Protocol Implementation Conformance Statement (PICS) proforma	ISO/IEC 11586-5
ITU-T X.835	Generic upper layers security: Protecting transfer syntax Protocol Implementation Conformance Statement (PICS) proforma	ISO/IEC 11586-6
ITU-T X.841	Security techniques – Security information objects for access control	ISO/IEC 15816
ITU-T X.842	Security techniques – Guidelines for the use and management of trusted third party services	ISO/IEC TR 14516
ITU-T X.843	Security techniques – Specification of TTP services to support the application of digital signatures	ISO/IEC 15945
ITU-T X.1031	Roles of end users and telecommunications networks within security architecture	
ITU-T X.1032	Architecture of external interrelationships for a telecommunication IP-based network security system	
ITU-T X.1034	Guidelines on extensible authentication protocol based authentication and key management in a data communication network	
ITU-T X.1035	Password-authenticated key exchange (PAK) protocol	
ITU-T X.1036	Framework for creation, storage, distribution and enforcement of policies for network security	
ITU-T X.1038	Security requirements and reference architecture for software-defined networking	
ITU-T X.1042	Security services using software-defined networking	
ITU-T X.1043	Security framework and requirements for service function chaining based on software-defined networking	
ITU-T X.1045	Security service chain architecture for networks and applications	

Pre-published

Recommendation	Title	Equivalent text
ITU-T X.1051	Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	ISO/IEC 27011
ITU-T X.1052	Information security management framework	
ITU-T X.1054	Governance of information security	ISO/IEC 27014
ITU-T X.1055	Risk management and risk profile guidelines for telecommunication organizations	
ITU-T X.1056	Security incident management guidelines for telecommunications organizations	
ITU-T X.1057	Asset management guidelines in telecommunication organizations	
ITU-T X.1058	Information technology - Security techniques - Code of practice for personally identifiable information protection	ISO/IEC 29151
ITU-T X.1059	Implementation guidance for telecommunication organizations on risk management of their assets globally accessible in IP-based networks	
ITU-T X.1060	Framework for the creation and operation of a cyber defence centre	
ITU-T X.1080.0	Access control for telebiometrics data protection	
ITU-T X.1081	A framework for the specification of security and safety aspects of telebiometrics	
ITU-T X.1080.1	e-Health and world-wide telemedicines – Generic telecommunication protocol	
ITU-T X.1082	Telebiometrics related to human physiology	ISO/IEC 80000-14
ITU-T X.1083	Biometrics – BioAPI interworking protocol	ISO/IEC 24708
ITU-T X.1084	Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems	
ITU-T X.1086	Telebiometrics protection procedures – A guideline to technical and managerial countermeasures for biometric data security	
ITU-T X.1087	Technical and operational countermeasures for telebiometric applications using mobile devices	
ITU-T X.1088	Telebiometrics digital key framework (TDK) – A framework for biometric digital key generation and protection	
ITU-T X.1089	Telebiometrics authentication infrastructure (TAI)	
ITU-T X.1090	Authentication framework with one-time telebiometric templates	
ITU-T X.1091	A guideline for evaluating telebiometric template protection techniques	
ITU-T X.1092	Integrated framework for telebiometric data protection in e-health and telemedicine	
ITU-T X.1093	Telebiometric access control with smart ID cards	
ITU-T X.1094	Telebiometric authentication using biosignals	
ITU-T X.1095	Entity authentication service for pet animals using telebiometrics	
ITU-T X.1101	Security requirements and framework for multicast communication	
ITU-T X.1111	Framework for security technologies for home network	
ITU-T X.1112	Device certificate profile for the home network	
ITU-T X.1113	Guideline on user authentication mechanisms for home network services	

Prepublished

Recommendation	Title	Equivalent text
ITU-T X.1114	Authorization framework for home network	
ITU-T X.1121	Framework of security technologies for mobile end-to-end data communications	
ITU-T X.1122	Guideline for implementing secure mobile systems based on PKI	
ITU-T X.1123	Differentiated security service for secure mobile end-to-end data communication	
ITU-T X.1124	Authentication architecture for mobile end-to-end communication	
ITU-T X.1125	Correlative Reacting System in mobile data communication	
ITU-T X.1141	Security Assertion Markup Language (SAML 2.0)	OASIS SAML 2.0
ITU-T X.1142	eXtensible Access Control Markup Language (XACML 2.0)	OASIS XACML 2.0
ITU-T X.1143	Security architecture for message security in mobile web services	
ITU-T X.1146	Secure protection guidelines for value-added services provided by telecommunication operators	
ITU-T X.1151	Guideline on secure password-based authentication protocol with key exchange	
ITU-T X.1148	Framework of de-identification process for telecommunication service providers	
ITU-T X.1149	Security framework of an open platform for FinTech services	
ITU-T X.1150	Security assurance framework for digital financial services	
ITU-T X.1152	Secure end-to-end data communication techniques using trusted third party services	
ITU-T X.1153	Management framework of a one-time password-based authentication service	
ITU-T X.1154	General framework of combined authentication on multiple identity service provider environments	
ITU-T X.1156	Non-repudiation framework based on a one time password	
ITU-T X.1157	Technical capabilities of fraud detection and response for services with high assurance level requirements	
ITU-T X.1158	Multi-factor authentication mechanisms using a mobile device	
ITU-T X.1159	Delegated non-repudiation architecture based on ITU-T X.813	
ITU-T X.1161	Framework for secure peer-to-peer communications	
ITU-T X.1162	Security architecture and operations for peer-to-peer networks	
ITU-T X.1164	Use of service providers' user authentication infrastructure to implement public key infrastructure for peer-to-peer networks	
ITU-T X.1171	Threats and requirements for protection of personally-identifiable information in applications using tag-based identification	
ITU-T X.1191	Functional requirements and architecture for IPTV security aspects	
ITU-T X.1192	Functional requirements and mechanisms for the secure transcodable scheme of IPTV	
ITU-T X.1193	Key management framework for secure Internet protocol television (IPTV) services	
ITU-T X.1195	Service and content protection interoperability scheme	
ITU-T X.1196	Framework for the downloadable service and content protection system in the mobile Internet Protocol television environment	

Pre-published

Recommendation	Title	Equivalent text
ITU-T X.1197	Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection	
ITU-T X.1198	Virtual machine-based security platform for renewable IPTV service and content protection	
ITU-T X.1205	Overview of cybersecurity	
ITU-T X.1206	A vendor-neutral framework for automatic notification of security related information and dissemination of updates	
ITU-T X.1207	Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software	
ITU-T X.1209	Capabilities and their context scenarios for cybersecurity information sharing and exchange	
ITU-T X.1215	Use cases for structured threat information expression	
ITU-T X.1231	Technical strategies on countering spam	
ITU-T X.1240	Technologies involved in countering e-mail spam	
ITU-T X.1241	Technical framework for countering e-mail spam	
ITU-T X.1242	Short message service (SMS) spam filtering system based on user-specified rules	
ITU-T X.1243	Interactive gateway system for countering spam	
ITU-T X.1244	Overall aspects of countering spam in IP-based multimedia applications	
ITU-T X.1245	Framework for countering spam in IP-based multimedia applications	
ITU-T X.1246	Technologies involved in countering voice spam in telecommunication organizations	
ITU-T X.1247	Technical framework for countering mobile messaging spam	
ITU-T X.1248	Technical requirements for countering instant messaging spam	
ITU-T X.1249	Technical framework for countering mobile in-application advertising spam	
ITU-T X.1250	Baseline capabilities for enhanced global identity management and interoperability	
ITU-T X.1251	A framework for user control of digital identity	
ITU-T X.1252	Baseline identity management terms and definitions	
ITU-T X.1253	Security guidelines for identity management systems	
ITU-T X.1254	Entity authentication assurance framework	ISO/IEC 29115
ITU-T X.1255	Framework for discovery of identity management information	
ITU-T X.1258	Enhanced entity authentication based on aggregated attributes	
ITU-T X.1275	Guidelines on protection of personally identifiable information in the application of RFID technology	
ITU-T X.1277	Universal authentication framework	
ITU-T X.1277.2	Universal authentication framework protocol specification	
ITU-T X.1278	Client to authenticator protocol/Universal 2-factor framework	
ITU-T X.1278.2	Client to authenticator protocol	
ITU-T X.1280	Framework for out-of-band server authentication using mobile devices	
ITU-T X.1303	Common alerting protocol (CAP 1.1)	OASIS CAP v1.1

Pre-published

Recommendation	Title	Equivalent text
ITU-T X.1311	Security framework for ubiquitous sensor network	ISO/IEC 29180
ITU-T X.1312	Ubiquitous sensor network middleware security guidelines	
ITU-T X.1331	Security guidelines for home area network (HAN) devices in smart grid systems	
ITU-T X.1352	Security requirements for Internet of things devices and gateways	
ITU-T X.1361	Security framework for the Internet of things based on the gateway model	
ITU-T X.1363	Technical framework of personally identifiable information (PII) handling in Internet of things (IoT) environment	
ITU-T X.1364	Security requirements and framework for narrow band Internet of things	
ITU-T X.1366	Aggregate message authentication schemes for Internet of things environment	
ITU-T X.1367	Standard format for Internet of things error logs for security incident operations	
ITU-T X.1368	Secure firmware or software update for Internet of things devices	
ITU-T X.1369	Security requirements for IoT service platform	
ITU-T X.1371	Security threats to connected vehicles	
ITU-T X.1372	Security guidelines for Vehicle-to-Everything (V2X) communication systems	
ITU-T X.1373	Secure software update capability for intelligent transportation system communication devices	
ITU-T X.1400	Terms and definitions for distributed ledger technology	
ITU-T X.1401	Security threats of distributed ledger technology	
ITU-T X.1402	Security framework for distributed ledger technology	
ITU-T X.1403	Security guidelines for using DLT for decentralized identity management	
ITU-T X.1404	Security assurance for distributed ledger technology	
ITU-T X.1405	Security threats and requirements for digital payment services based on distributed ledger technology	
ITU-T X.1408	Security threats and requirements for data access and sharing based on the distributed ledger technology	
ITU-T X.1410	Security architecture of data sharing management based on the distributed ledger technology	
ITU-T X.1411	Guideline on blockchain as a service (BaaS) security	
ITU-T X.1412	Security requirements for smart contract management based on the distributed ledger technology	
ITU-T X.1500	Overview of cybersecurity information exchange	
ITU-T X.1520	Common vulnerabilities and exposures	
ITU-T X.1521	Common vulnerability scoring system	
ITU-T X.1550	Access control models for incident exchange networks	
ITU-T X.1570	Discovery mechanisms in the exchange of cybersecurity information	
ITU-T X.1601	Security framework for cloud computing	
ITU-T X.1602	Security requirements for software as a service application environments	

Pre-published

Recommendation	Title	Equivalent text
ITU-T X.1603	Data security requirements for the monitoring service of cloud computing	
ITU-T X.1604	Security requirements of Network as a Service (NaaS) in cloud computing	
ITU-T X.1605	Security requirements of public Infrastructure as a Service (IaaS) in cloud computing	
ITU-T X.1606	Security requirements for communications as a service application environments	
ITU-T X.1631	Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services	ISO/IEC 27017
ITU-T X.1641	Guidelines for cloud service customer data security	
ITU-T X.1642	Guidelines for the operational security of cloud computing	
ITU-T X.1643	Security requirements and guidelines for virtualization containers in cloud computing environments	
ITU-T X.1644	Security guidelines for distributed cloud	
ITU-T X.1645	Requirements of network security situational awareness platform for cloud computing	
ITU-T X.1702	Quantum noise random number generator architecture	
ITU-T X.1750	Guidelines on security of big data as a service for big data service providers	
ITU-T X.1751	Security guidelines for big data lifecycle management by telecommunication operators	
ITU-T X.1771	Security guidelines for combining de-identified data using trusted third party	
ITU-T X.1752	Security guidelines for big data infrastructure and platform	
ITU-T X.1811	Security guidelines for applying quantum-safe algorithms in IMT-2020 systems	
ITU-T X.1812	Security framework based on trust relationships for the IMT-2020 ecosystem	
ITU-T X.1813	Security and monitoring requirements for operation of vertical services supporting ultra-reliability and low latency communication (URLLC) in IMT-2020 private networks	
ITU-T X.1814	Security guidelines for IMT-2020 communication system s	
ITU-T Y.1271	Framework(s) on network requirements and capabilities to support emergency communications over evolving circuit-switched and packed-switched networks	
ITU-T Y.1550	Considerations for realizing virtual measurement systems	
ITU-T Y.2001	General overview of NGN	
ITU-T Y.2066	Common requirements of the Internet of things	
ITU-T Y.2074	Requirements for Internet of things devices and operation of Internet of things applications during disasters	
ITU-T Y.2205	Emergency Telecommunications – Technical Considerations	
ITU-T Y.2701	Security requirements for NGN release 1	
ITU-T Y.2702	Authentication and authorization requirements for NGN release 1	
ITU-T Y.2703	The application of AAA service in NGN	

Pre-published

Recommendation	Title	Equivalent text
ITU-T Y.2704	Security mechanisms and procedures for NGN	
ITU-T Y.2705	Minimum security requirements for interconnection of emergency telecommunications service (ETS)	
ITU-T Y.2720	NGN identity management framework	
ITU-T Y.2721	NGN identity management requirements and use cases	
ITU-T Y.2722	NGN identity management mechanisms	
ITU-T Y.2740	Security requirements for mobile remote financial transactions in next generation networks	
ITU-T Y.2741	Architecture of secure mobile financial transactions in next generation networks	
ITU-T Y.2760	Mobility security framework in NGN	
ITU-T Y.3300	Framework of software-defined networking	
ITU-T Y.3302	Functional architecture of software-defined networking	
ITU-T Y.3500	Cloud computing – Overview and vocabulary	ISO/IEC 17788
ITU-T Y.3600	Big data - Cloud computing based requirements and capabilities	
ITU-T Y.4100	Common requirements of the Internet of things	

Pre-published

Publication	Title	Equivalent text
Supplements to ITU-T X-series Recommendations		
Supplement 2	ITU-T X.800-X.849 series – Supplement on security baseline for network operators	
Supplement 3	ITU-T X.800-X.849 series – Supplement on guidelines for implementing system and network security	
Supplement 6	ITU-T X.1240 series – Supplement on countering spam and associated threats	
Supplement 7	ITU-T X.1250 series – Supplement on overview of identity management in the context of cybersecurity	
Supplement 8	ITU-T X.1205 – Supplement on best practices against botnet threats	
Supplement 9	ITU-T X.1205 – Guidelines for reducing malware in ICT networks	
Supplement 10	ITU-T X.1205 – Supplement on usability of network traceback	
Supplement 11	ITU-T X.1245 - Supplement on framework based on real-time blocking lists for countering VoIP spam	
Supplement 12	ITU-T X.1240 - Supplement on overall aspects of countering mobile messaging spam	
Supplement 15	ITU-T X.800-X.849 series - Supplement on guidance for creating a national IP-based public network security centre for developing countries	
Supplement 16	ITU-T X.800-X.849 series – Supplement on architectural systems for security controls for preventing fraudulent activities in public carrier networks	
Supplement 23	ITU-T X.1037 - Supplement on security management guidelines for the implementation of an IPv6 environment in telecommunication organizations	
Supplement 28	ITU-T X.1245 - Supplement on technical measures and mechanisms on countering spoofed calls in the terminating network of voice over long term evolution (VoLTE)	
Supplement 29	ITU-T X.1242 - Supplement on guidelines on countermeasures against short message service phishing and smishing attacks	
Supplement 33	ITU-T X.1231 - Supplement on technical framework for countering telephone service scams	
Supplements to ITU-T Y-series Recommendations		
Y.sup 19	Supplement to Y.2222 series on the risk analysis service in next generation networks	
ITU-T Handbooks		
link	Outside plant Technologies for public networks	
link	Application of Computers and Microprocessors to the Construction, Installation and Protection of Telecommunication Cables	

Pre-published