International Telecommunication Union

Security in Telecommunications and Information Technology

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

ITU-T

ITU-T
Telecommunication
Standardization
Sector of ITU

2009

ITU
International
Telecommunication
Union

ITU-T – Telecommunication Standardization Bureau (TSB)
Place des Nations – CH-1211 Geneva 20 – Switzerland
E-mail: tsbmail@itu.int Web: www.itu.int/ITU-T

Security in Telecommunications and Information Technology

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

September 2009

Preface

Malcolm Johnson
Director
ITU Telecommunication Standardization Bureau

Until relatively recently, telecommunications and information technology security was mainly of concern to niche areas such as banking, aerospace and military applications. However, with the rapid and widespread growth in the use of data communications, particularly the Internet, security has become a concern to almost everyone.

The increased profile of information and communication technology (ICT) security may be attributed in part to widely-reported incidents such as viruses, worms, hackers and threats to personal privacy, but the reality is that, as computing and networking are now such an important part of daily life, the need for effective security measures to protect the computer and telecommunication systems of governments, industry, commerce, critical infrastructures and individual consumers is now imperative. In addition, an increasing number of countries now have data protection legislation that requires compliance with demonstrated standards of data confidentiality and integrity.

It is now widely recognized that security should be built into systems, rather than retrofitted and that, to be truly effective, security must be considered throughout all stages of the system lifecycle, from system inception and design through implementation, deployment and, finally, decommissioning. Failure to consider security adequately during the project design phase and during systems development can result in implementation vulnerabilities. Standards committees have a vital role to play in protecting telecommunications and information technology systems by maintaining an awareness of security issues, by ensuring that security considerations are a fundamental part of specifications, and by providing technical standards and guidance to assist implementers and users in the task of making communication systems and services sufficiently robust that they can withstand cyber attacks.

ITU-T has been active in the security work for telecommunications and information technology for many years but, as network use has increased, the workload has grown quite dramatically in response to new and evolving threats and the demands of our members for standards to help counter these threats. This manual presents an overview of some of the key elements of that work and provides an introduction to the extensive resources available from the ITU-T to assist all users in addressing the network security challenges we face.

Standardization is a key building block in constructing a global culture of cybersecurity. We can and will win the war against cyber-threats. We will do so by building on the work of the thousands of dedicated individuals, from public administrations, the private sector and academia, who come together, in organizations like the ITU, to develop security standards and guidelines for best practice. The work is not glamorous, or high profile, but it is nonetheless essential to safeguard our digital future. I would like to express my appreciation to the engineers of the ITU Telecommunication Standardization Bureau who, in conjunction with experts from the ITU membership, have worked, and continue to work, so tirelessly to develop these standards and guidelines.

The manual is intended as a guide for senior executives and managers who have responsibility for, or an interest in, information and telecommunications security, as well as technologists, regulators and others who wish to gain a better understanding of ICT security issues and the corresponding ITU-T Recommendations that address those issues. I trust that this manual will be a useful guide for those looking to address ICT security issues and I welcome feedback from readers for future editions.

Malcolm Johnson

Director
Telecommunication Standardization Bureau, ITU

Contents

Page

Page

Page

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 Rapporteurs, editors, and security coordinators of the ITU Study Groups, to the ITU/TSB counsellors involved in studies on security and in particular to Herb Bertine, the former Chairman of the lead Study Group in ITU-T for work on telecommunications security and Mike Harrop, the former Rapporteur for the security project.

Executive Summary

The purpose of this manual is to provide a broad introduction to the security work of the ITU-T. It is directed towards those who have responsibility for, or an interest in, information and communications security and the related standards, and those who simply need to gain a better understanding of ICT security issues and the corresponding ITU-T Recommendations.

The text begins with an overview of ITU-T security activities. Included in this section are links to some of the key ITU-T security resources and outreach information. In addition, this introductory part of the manual contains a summary table that indicates how the manual can be used by different audiences.

Next, the basic requirements for protection of ICT applications, services and information are introduced in a section that explains the threats and vulnerabilities that drive the requirements, examines the role of standards in meeting the requirements, and describes some of the features that are needed to protect the various parties with a close interest in the use and operation of ICT facilities. In addition, this section provides rationale for ICT security standards and outlines the evolution of the ITU-T work in this area.

The generic security architectures for open systems and end-to-end communications are then introduced together with some 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 provide 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. This section also provides a link to security guidelines relating to critical activities associated with the network security life-cycle.

Selected topics on security management are then addressed in a section that examines information security management, risk management and incident response and handling.

The Directory and its role in supporting security services, together with the related topics of authentication and identity management are then discussed. Topics such as public-key infrastructures, telebiometrics (i.e. personal identification and authentication using biometric devices in telecommunication environments) and privacy are presented in this section which also covers the importance of protecting the Directory information base.

A discussion on securing the network infrastructure then covers topics related to network management and common security management services.

Some specific examples and approaches to network security are described next. The section begins with a look at the security requirements for Next Generation Networks 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. This is followed by an examination of security provisions for home networks and cable television. Lastly, the challenges of security for ubiquitous sensor networks are outlined.

Although 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, applications are still at risk from an evolving threat environment and from inherent vulnerabilities. The section on application security reviews a number of ICT applications, including Voice over IP, IPTV and secure fax, with particular emphasis on the security features that are defined in ITU-T Recommendations.

The next section examines how to counter some common network threats such as spam, malicious code and spyware. It also considers the importance of timely notification and dissemination of updates and the need for organization and consistency in handling security incidents.

In conclusion, there is a short section on the likely future directions of ICT security standardization. This is followed by a review of sources of additional information.

Annexes are included 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.

Introduction to the 4th edition

For this 4th edition of the manual, the structure and contents have been significantly revised. Since the first edition of the manual was published in 2003, the ITU-T has embarked on many new work areas. In addition, a great many new Recommendations have been completed and published and the Study Groups themselves have been restructured following the World Telecommunication Standardization Assembly (WTSA) 2008. Any attempt to cover all this work in detail would have resulted in a large, complex and unwieldy document. After consultation with ITU-T members, some guiding principles were established for this edition. These included:

- 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);
- it should be written to accommodate publication both as a stand-alone printed document and as an electronic document;
- the text should employ web links to Recommendations and other sources of publicly-available material as much as possible. Detailed information, over and above that 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 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 provides web links to additional information.

The manual is published both in hard copy and in electronic format. For readers using an electronic version of the text, direct hyperlinks are provided to the listed Recommendations and to other on-line documentation. For readers using a hard copy of the text, all referenced Recommendations are listed in Annex D. These can be accessed on line at: www.itu.int/rec/T-REC/en.

1. Introduction

1 Introduction

1.1 Purpose and scope of this 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 assembles selected security-related material from ITU-T Recommendations into one publication and explains relationships of various aspects of the work. Results achieved in ITU-T security-related standardization since the second 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 addressed 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 some other Sectors of the ITU. Examples include the work on cybersecurity (www.itu.int/cybersecurity) and the ITU-D Best Practices Report.

1.2 How to use this manual

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 linkages are provided. The manual can be used in several ways. Table 1indicates how it can be used to address the needs of different audiences.

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 standardization efforts High level roadmap to relevant standards	The manual directly addresses these needs
	Design and deployment engineers	Roadmap to relevant standards Technical details associated with specific areas	The manual provides roadmap plus links to detailed explanatory text Recommendations provide technical details
Telecommunication service vendors	Senior executives / managers	Broad overview of scope of standardization efforts High level roadmap to relevant standards	The manual directly addresses these needs
	Product managers	Roadmap to relevant standards	The manual provides 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 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 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 standardization efforts	The manual provides roadmap plus links to detailed explanatory text on specific areas
Government	Senior executives and managers	Broad overview of scope of standardization efforts High level roadmap to relevant standards	The manual directly addresses these needs
	Regulators		
	Policy makers		
Non-government organizations	Senior executives / managers	Broad overview of scope of standardization efforts High level roadmap to relevant standards	The manual directly addresses these needs
	Development and capacity building	Roadmap to relevant standards Technical details associated with specific areas	The manual provides links to detailed explanatory text on specific areas Recommendations provide technical details

2. Overview of ITU-T security activities

2 Overview of ITU-T security activities

2.1 Introduction

The ITU-T work on ICT security has been underway for over two decades, during which time Recommendations and guidance have been developed in a number of key areas by several Study Groups. Study Group 17 (SG 17) now has primary responsibility for the ITU-T 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, SG 17 has developed a number of reference and outreach publications. These publications, which include this manual, aid in the effort to coordinate the ITU-T security work internally as well as help to promote the work to a much wider community and encourage the use of the Recommendations.

This section contains an overview of the ITU-T's reference and outreach publications and provides a graphical summary of the security work currently underway.

2.2 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 SG 17 Lead Study Group on Security website provides a summary of the responsibilities and activities of SG 17. Included on this site are summaries of, and links to documentation and outreach material, information on past workshops, presentations and outreach activities, and links to security guidance, including a tutorial on writing safe and secure programs.

More detailed information on various aspects of the security work along with direct links to further information is contained in Chapter 12.

2.3 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. For readers using an electronic version of the text, direct 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 so that those reading the electronic version of the text will be able to link directly to download the Recommendations.

Table 2 – Overview of some of the key topics and selected Recommendations

Topic	Sub-topics	Examples of relevant Recommendations & publications
3. Security requirements	3.2 Threats, risks and vulnerabilities 3.3 Security objectives 3.4 Rationale for security standards 3.6 Personnel and physical security requirements	X.1205: Overview of cybersecurity E.408: Telecommunication networks security requirements X.1051: Information security management guidelines for telecommunications organizations Outside plant technologies for public networks Application of computers and microprocessors to the construction, installation and protection of telecommunication cables
4. Security architectures	4.1 Open systems security architecture 4.2 Security services 4.3 Security architecture for systems providing end-to-end communications 4.3.2 Availability of the network and its components 4.4 Implementation guidance 4.5 Application-specific architectures	X.800: Open systems security architecture X.805: Security architecture for systems providing end-to-end communications X.810: Security framework overview X.Sup3: ITU-T X.800-X.849 series - Supplement on guidelines for implementing system and network security X.1162: Security architecture and operations for peer-to-peer networks X.1161: Framework for secure peer-to-peer communications X.1143: Security architecture for message security in mobile web services.
5. Security management	5.1 Information security management 5.2 Risk management 5.3 Incident handling	X.1051: Information security management guidelines for telecommunications organizations X.1055: Risk management and risk profile guidelines for telecommunication organizations E.409: Incident organization and security incident handling
6. The Directory, authentication and Identity management	6.1 Protection of Directory information 6.1.4 Privacy protection 6.2 Public-key security mechanisms 6.2.3 Public-key infrastructures 6.4 Identity management 6.5 Telebiometrics	X.500: Overview of concepts, models and services X.509: The Directory: Public-Key and attribute certificate frameworks X.1171: Threats and requirements for protection of personally-identifiable information in applications using tag-based identification Y.2720: An NGN identity management framework X.1081: A framework for the specification of security and safety aspects of telebiometrics, X.1089: Telebiometrics authentication infrastructure
7. Securing the network infrastructure	7.1 The telecommunications management network 7.2 Network management architecture 7.4 Securing monitoring and control activities 7.5 Securing network-based applications 7.6 Common security management services 7.6.4 CORBA-based security services	M.3010: Principles for a telecommunications management network X.790: Trouble management function for ITU-T applications X.711: Common Management Information Protocol X.736: Security alarm reporting function X.740: Security audit trail function X.780: TMN Guidelines for defining CORBA managed objects
8. Some specific approaches to network security	8.1 Next Generation Network (NGN) security 8.2 Mobile communications security 8.3 Security for home networks 8.4 Security requirements for IPCablecom 8.6 Security for Ubiquitous Sensor Networks	Y.2001: General overview of NGN Y.2701: Security requirements for NGN release 1 X.1121: Framework of security technologies for mobile end-to-end data communications X.1111: Framework for security technologies for home network J.170: IPCablecom security specification
9. Application security	9.1 Voice over IP (VoIP) and multimedia 9.2 IPTV 9.3 Secure fax 9.4 Web services 9.5 Tag-based services	H.235: Framework for security in H-series multimedia systems X.1191: Functional requirements and architecture for IPTV security aspects T.36: Security capabilities for use with Group 3 facsimile terminals X.1141: Security Assertion Markup Language (SAML 2.0)
10. Countering common network threats	10.1 Countering spam 10.2 Malicious code, spyware and deceptive software 10.3 Notification and dissemination of software updates	X.1231: Technical strategies on countering spam X.1240: Technologies involved in countering email spam X.1244: Overall aspects of countering spam in IP-based multimedia applications X.1207: Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software X.1206: A vendor-neutral framework for automatic notification of security related information and dissemination of updates
For a complete set of ITU-T security Recommendations see http://www.itu.int/ITU-T/recommendations/		

3. Security requirements

3 Security requirements

3.1 Introduction

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 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 a changing threat environment. For the most part, the discussion in this section is generic. Requirements for particular applications and environments are discussed in later sections.

3.2 Threats, risks and vulnerabilities

In general terms, in ICT security, we may need to protect assets for the following parties:

- *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, fair competition and privacy protection; and
- *network operators/service providers* themselves who need security to safeguard their operation and business interests and to meet their obligations to the customers and the public, at the national and international level.

The assets to be protected include:

- communications 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* 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.

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.

ITU-T Recommendations recognize four types of vulnerability:

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

A *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 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, any 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 address 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 the relevant policies. The 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, *Telecommunication networks security requirements*, 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, national implementation of the requirements for the national components of the network is essential.

Recommendation ITU-T X.1205, *Overview of cybersecurity*, 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.

3.3 General security objectives for ICT networks

The general security objectives for telecommunication networks are:

a) only authorized users should be able to access and use telecommunication networks;

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

c) telecommunication networks should provide privacy at the level set by the security policies of the network;

d) all users should be held accountable for their own, but only their own, actions in telecommunication networks;

e) in order to ensure availability, telecommunication networks should be protected against unsolicited access or operations;

f) it should be possible to retrieve security-related information from telecommunication networks (but only authorized users should be able to retrieve such information);

g) if security violations are detected, they should be handled in a controlled way, in accordance with a pre-defined plan, to minimize potential damage;

h) after a security breach is detected, it should be possible to restore normal security levels; and

i) the security architecture of telecommunication networks should provide a degree of flexibility in order to support different security policies and security mechanisms of different strengths.

Objectives (a) through (e) can be achieved by implementing the following security services:

- confidentiality;
- data, system and program integrity;

- accountability, including authentication, non-repudiation and access control; and
- availability.

One type of ICT network of rapidly-growing importance is the Next Generation Network (NGN). Security requirements and objectives for NGNs are discussed in section 8.

3.4 Rationale for security standards

The requirement for a generic network security framework for international telecommunications originated from different sources including customers/subscribers, the public community/authorities, and the network operators/service providers. It is preferable that security requirements for telecommunication networks be addressed by internationally-agreed standards as this 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 and at lower cost.

Important benefits of standardized security solutions for both vendors and users of the systems include economy of scale in product development and component interoperation within telecommunication networks.

3.5 Evolution of ITU-T security standards

The ITU-T security work has evolved considerably in recent years as will be seen in later sections, where many of the individual Recommendations are discussed in more detail. Here, some key aspects of this evolution are discussed, particularly as they relate to security requirements.

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 the 1991 Rec. ITU-T X.800, *Security Architecture for Open Systems Interconnection for CCITT applications*. The previously-mentioned Rec. ITU-T E.408, *Telecommunication networks security requirements*, 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 identify or address requirements for specific networks. No new security services are considered. 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, *Overview of cybersecurity*. This Recommendation aims to build a foundation of knowledge that can help secure future networks. Various technologies that are available to counter threats 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 for securing various networks based on the discussed technologies 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.

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, networks, applications, and resources. Also, security must be comprehensive across all layers of a system. Adopting a layered approach to security, when combined with strong policy management and enforcement, provides a choice of security solutions that can be modular, flexible, and scalable.

Current cybersecurity techniques include:

– Cryptography: this powerful technology supports a number of security services including encryption of data during transmission and while in storage.

– Access controls: aim to restrict the ability of users to access, use, view or modify information on hosts, or networks.

– System integrity: aims to ensure that a system and its data are not modified or corrupted by unauthorized parties or in an unauthorized manner.

– Audit, logging and monitoring: helps system administrators to collect and review network logs during and after an attack. The data can be used to evaluate the effectiveness of the security strategy that is deployed by the network.

– Management: helps system administrators to review and to configure security settings on their hosts and networks. Management controls can be used to verify the accuracy of network and attached elements settings.

3.6 Personnel and physical security requirements

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 Rec. ITU-T X.1051, *Information security management guidelines for telecommunications organizations*. 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, general physical security requirements are identified in Rec. ITU-T X.1051 and 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 publications *Outside plant technologies for public networks* (1991) and *Application of computers and microprocessors to the construction, installation and protection of telecommunication cables* (1999). 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.

4. Security architectures

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 *open systems security architecture* (Rec. 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 *Security architecture for systems providing end-to-end communications* (Rec. 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. ITU-T X.805, which is described later in this section, complements other Recommendations of the 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 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, ITU-T X.800 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.

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 ITU-T X.800 was developed specifically as the OSI security architecture, the underlying concepts of ITU-T X.800 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 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. ITU-T X.800 reflects a strong, international consensus on these services.

The value and general applicability of ITU-T X.800 results from the fact that it represents a significant 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.

During the development of 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 were developed to provide comprehensive and consistent descriptions of each of the security services defined in 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.

The frameworks address both data elements and sequences of operations (excluding protocol elements) that are used to provide specific security services. These services may apply to the communicating entities of systems as well as to data exchanged between, and managed by them.

A *security framework overview* (Rec. 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. 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). The *authentication framework* (Rec. 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. The *access control framework* (Rec. 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 from denying later that they performed an action. Non-repudiation is concerned with establishing evidence that can later be used to counter false claims. 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. The *non-repudiation framework* (Rec. ITU-T X.813) extends the concepts of non-repudiation security services described in ITU-T X.800 and provides a framework for the development of these services. It also identifies possible mechanisms to support these services and 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. The *confidentiality framework* (Rec. ITU-T X.814) addresses the confidentiality of information in retrieval, transfer and management 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 fact. The *integrity framework* (Rec. 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, Rec. ITU-T X.805, *Security architecture for systems providing end-to-end communications*, 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 ITU-T X.805 architecture

The 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.

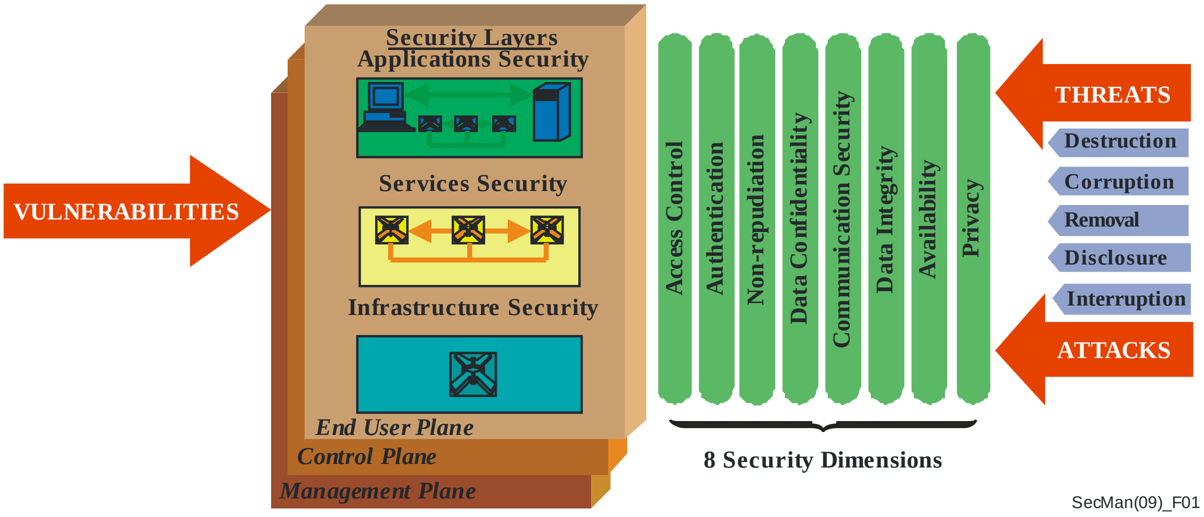


Figure 1 – Security architectural elements in Rec. ITU-T X.805

In 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 ITU-T X.800 (*Access Control*, *Authentication, Data Confidentiality*, *Data Integrity* and *Non-repudiation*) match the functionalities of the corresponding *security dimensions* of ITU-T X.805 (as depicted in Figure 1). In addition, ITU-T X.805 introduces three dimensions (*Communication Security, Availability* and *Privacy*) that are not in ITU-T X.800. 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.

The eight security dimensions of ITU-T X.805 are:

- the *Access Control* dimension, which protects against unauthorized use of network resources and ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications;
- the *Authentication* dimension, which confirms the identities of communicating entities, ensures the validity of the claimed identities of the entities participating in the communication (e.g., person, device, service or application), and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication;
- the *Non-repudiation* dimension, which provides a means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent or commitment; proof of data origin; proof of ownership; and proof of resource use). It also ensures the availability of evidence that can be presented to a third party and used to prove that an event or action has taken place;
- the *Data Confidentiality* dimension, which protects data from unauthorized disclosure and ensures that the data content cannot be understood by unauthorized entities;
- 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 *Data Integrity* dimension, which ensures that data is protected against unauthorized modification, deletion, creation, and replication and provides an alert in the event of activities that could compromise data integrity;
- 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
- 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.

As shown in Figure 1, in addition to the security dimensions, ITU-T X.805 defines three security layers and three planes. 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 are to be defined to meet the needs of each layer. The three layers are:

- *the Infrastructure* layer, which consists of the network transmission facilities as well as individual network elements. Examples of components that belong to this layer are individual routers, switches and servers and 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 signalling 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 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. The X.805 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.

Although 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 Rec. 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 infrastructure security layer consists of the network transmission facilities as well as individual network elements protected by the security dimensions. The infrastructure layer represents the fundamental building blocks of networks, their services and applications. Examples of components that belong to the infrastructure layer include routers, switches and servers, as well as the communication links between them.

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, *Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths*, 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 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: 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*; and ITU-T G.1081, *Performance monitoring points for IPTV*.

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 a supplement to this series of Recommendations (X Supplement 3, ITU-T X.800-X.849 series – *Supplement on guidelines for implementing system and network security*). 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

Peer-to-peer (P2P) is an instantiation of network architectures where all peers have equivalent authority and responsibility, in contrast to the client/server model. In the case of P2P communications, a peer can be both the server and the client. When data or messages are exchanged in a P2P network, a peer communicates with other peers directly. 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.

With the rapid advancement of telecommunication networks and computing technology, much more information and many more computing resources can be made available at distributed nodes rather than from a limited number of centralized servers.

P2P networks are typically used for connecting nodes via ad hoc connections. Such networks are useful for many purposes. Sharing data files containing audio, video, text or anything in digital format is very common. Real-time communications data, such as telephony traffic, also exploits P2P technology.

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.

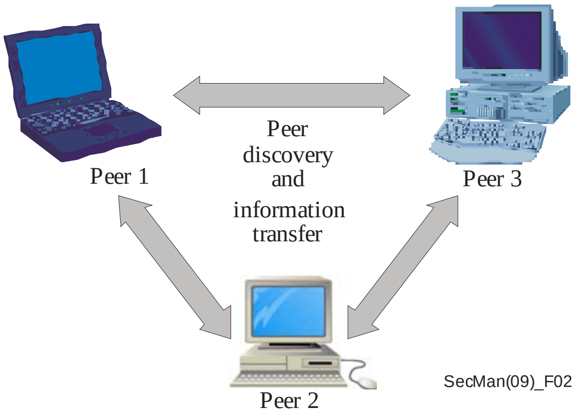


Figure 2 – P2P service architecture

Figure 3 shows the physical and logical P2P network 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 also 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 required). 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.

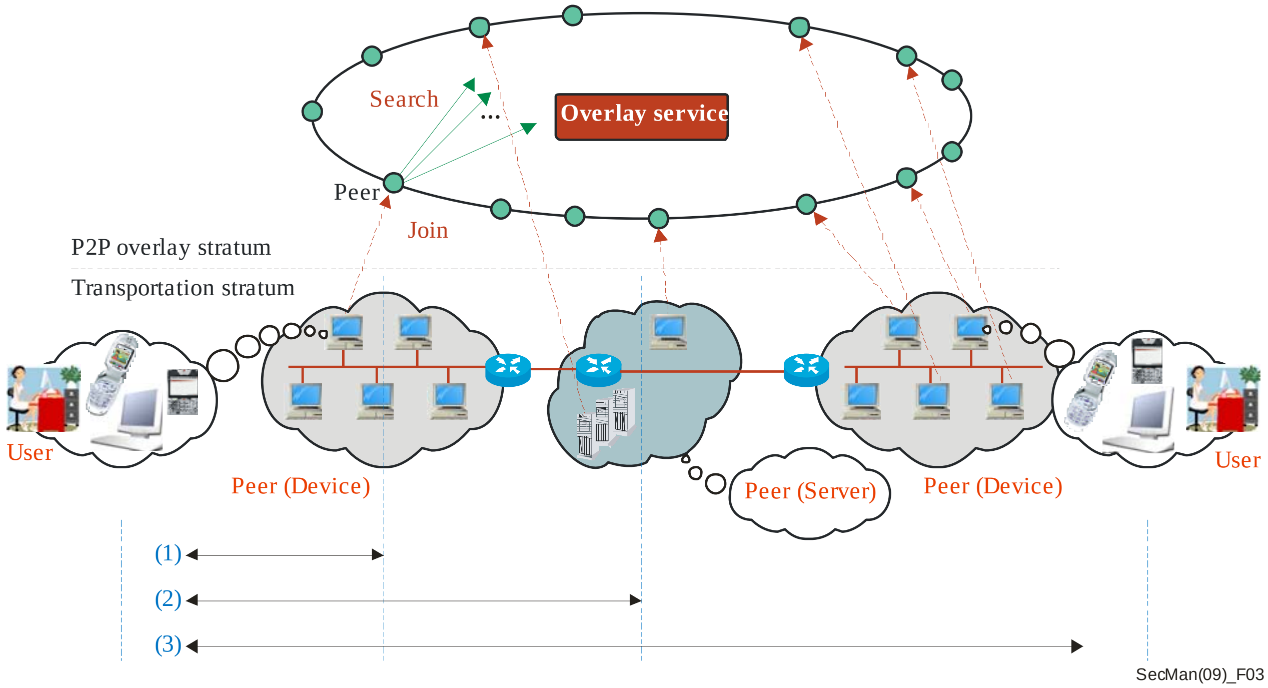


Figure 3 – Architectural reference model for the P2P network

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, *Framework for secure peer-to-peer communications*.

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

Functions 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	

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, *Security architecture for message security in mobile web services*. 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.

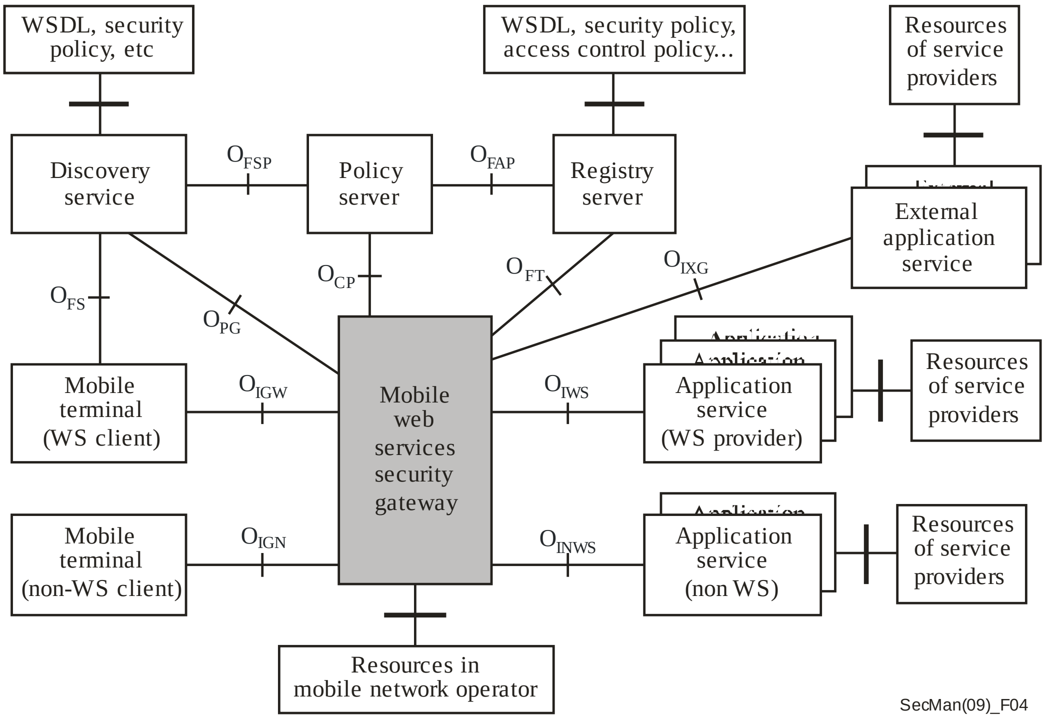

WSDL, security policy, etc
WSDL, security policy, access control policy...
Resources of service providers
Discovery service
O_{FSP}
Policy server
O_{FAP}
Registry server
External application service
O_{CP}
O_{FT}
O_{IXG}
O_{FS}
O_{PG}
Mobile terminal (WS client)
O_{IGW}
Mobile web services security gateway
O_{IWS}
Application service (WS provider)
Resources of service providers
Mobile terminal (non-WS client)
O_{IGN}
O_{INWS}
Application service (non WS)
Resources of service providers
Resources in mobile network operator
SecMan(09)_F04

Figure 4 – Security architecture for mobile Web Services

The 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
- 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.

4.6 Other network security architectures and models

Additional aspects of network security architectures are covered later in the text. In particular, please see clauses 7.2 Network management architecture; 8.1 Next Generation Network (NGN) security; 8.4.1 IPCablecom Architecture; 8.5.1 The IPCablecom2 architecture; and 9.2 IPTV.

5. Aspects of security management

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 7.

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.

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 assure its information security by implementing a structured security management process.

Effective management of information security is achieved by implementing a suitable set of controls. These controls, which apply to the telecommunications facilities, services and applications, need to be established, implemented, 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.

Telecommunication organizations whose facilities are used by subscribers to process information that may include personal data, confidential data and sensitive business data, need to ensure an appropriate level of protection to prevent compromise of the information, i.e., they need to establish an effective information security management system (ISMS).

The most widely-recognized ISMS specification is that defined in the ISO/IEC 27000 series of ISMS 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 Rec. ITU-T X.1051 | ISO/IEC 27011, *Information security management guidelines for telecommunications organizations,* based on ISO/IEC 27002, the ISMS Code of Practice.

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 ensure the confidentiality, integrity and availability of telecommunications facilities and services. Specific guidance for the telecommunication sector is included on the following topics:

- organization of information security;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control;

- information systems acquisition;
- development and maintenance;
- incident management; and
- business continuity management.

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

- information related to telecommunication organizations must 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
- all access to telecommunication information, facilities and the medium used for the provision of communication services must be authorized and should be provided only when necessary. As an extension of the availability provisions, telecommunications organizations should give priority to essential communications in case of emergency, and comply with regulatory requirements.

Information security management in telecommunication organizations is required regardless of the medium or mode of transmission. If information security management is not implemented properly, there will be increased risk associated with use of the system.

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 a telecommunication organization are accessed and utilized by not only its own employees and contractors, but also various users outside of 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 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 was introduced briefly in section 3 in the discussion on Recommendation ITU-T X.1205, *Overview of cybersecurity*. More detailed risk management guidelines are contained in Recommendation ITU-T X.1055, *Risk management and risk profile guidelines for telecommunication organizations*, which identifies processes and techniques to reduce information security risk. These processes and techniques can be used to assess telecommunications security requirements and risks, and to help to select, implement and update appropriate controls to maintain the required security level.

Many specific methodologies have been developed to address risk management. 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 5.

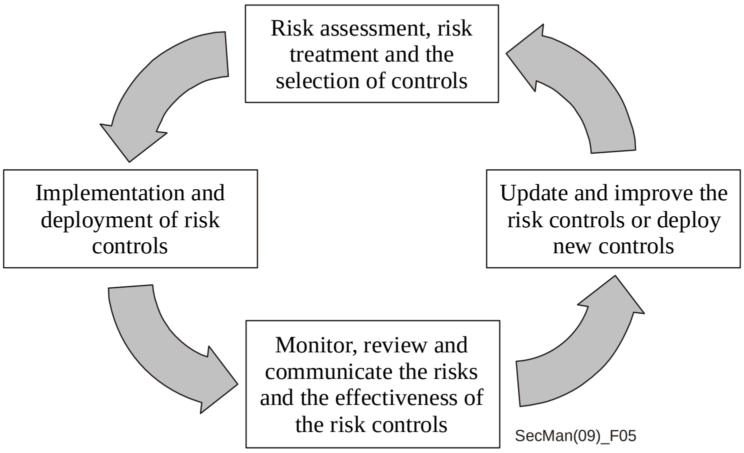

Risk assessment, risk treatment and the selection of controls
Implementation and deployment of risk controls
Update and improve the risk controls or deploy new controls
Monitor, review and communicate the risks and the effectiveness of the risk controls
SecMan(09)_F05

Figure 5 – 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 of 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.

5.3 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. A properly trained and mandated unit or group 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 general structure for incident handling (i.e., physical, administrative or organizational, and logical incidents) it is possible to obtain a general picture of the structure and flow of an incident. Recommendation ITU-T E.409, *Incident organization and security incident handling: Guidelines for telecommunication organizations*, provides an overview and framework that gives 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.

A consistent terminology is essential when reporting or handling an incident. The use of different terminology can lead to misunderstanding, 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. In addition, the definition of what is considered to be an incident can vary among professions, organizations and people. ITU-T E.409 attempts to standardize incident detection and reporting terminology and also to classify incidents according to their severity, as illustrated in Figure 6.

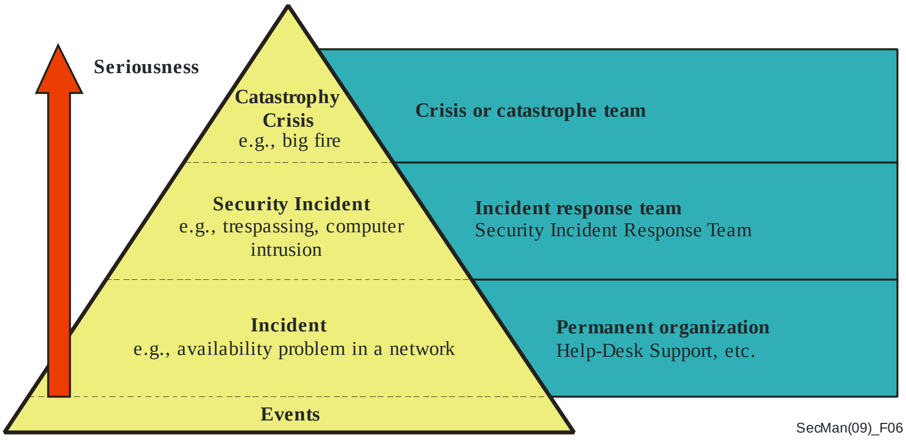


Figure 6 – ITU-T E.409 pyramid of events and incidents

Recommendation ITU-T E.409 also defines an incident handling structure (as illustrated in Figure 7) and sets out procedures for detecting, classifying, assessing, handling and following up incidents.

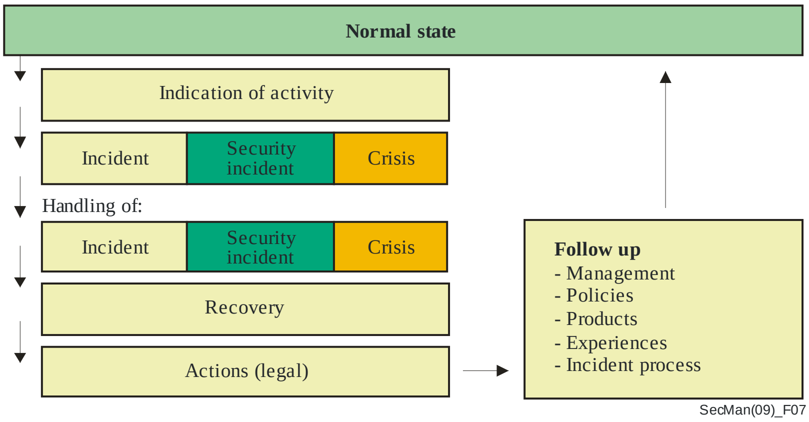


Figure 7 – ITU-T E.409 incident handling structure

The recently-approved Rec. ITU-T X.1056, *Security incident management guidelines for telecommunications organizations*, builds on the guidance provided in Rec. 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 are described in Rec. ITU-T X.1056 along with the relationship to the security management. These are illustrated in Figure 8 and Figure 9.

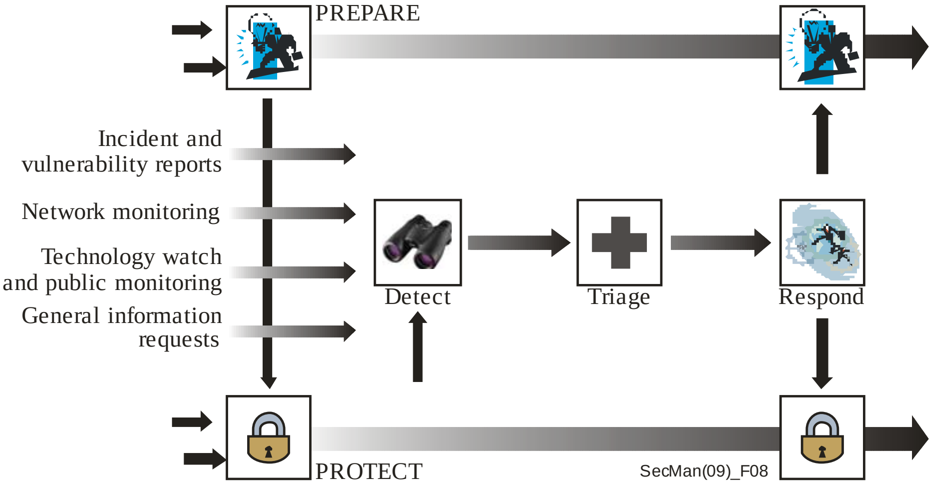

PREPARE
Incident and vulnerability reports
Network monitoring
Technology watch and public monitoring
General information requests
Detect
Triage
Respond
PROTECT
SecMan(09)_F08

Figure 8 – Five high-level incident management processes

(Source: Executive Overview of SEI MOSAIC: Technical Report CMU/SEI-2004-TR-015 – Defining Incident Management Processes for CSIRTs: A Work in Progress)

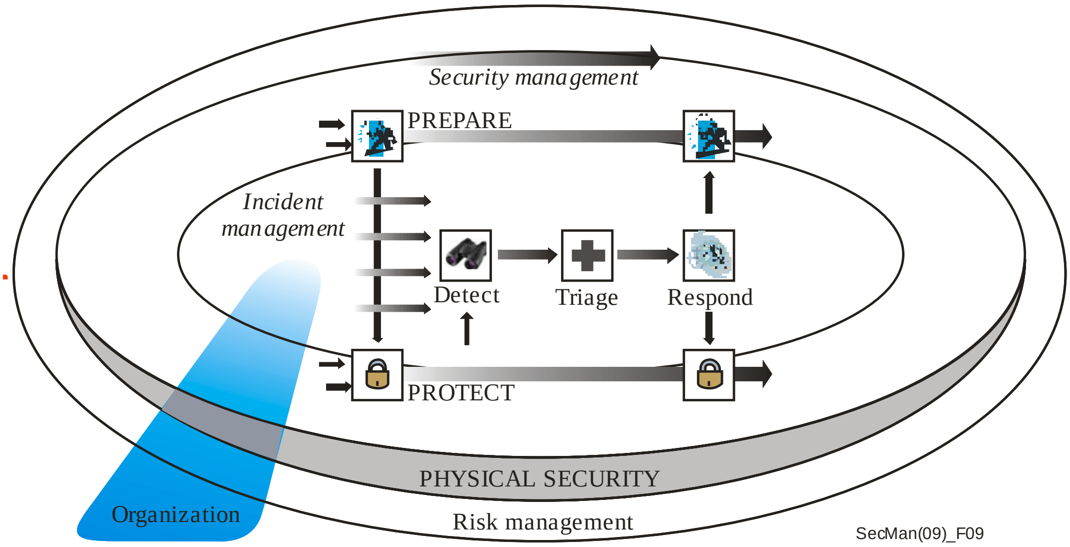


Figure 9 – Comparison of incident management and security management

(Source: Executive Overview of SEI MOSAIC: Technical Report CMU/SEI-2004-TR-015 – Defining Incident Management Processes for CSIRTs: A Work in Progress)

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

6. The Directory, authentication and identity management

6 The Directory, authentication and identity management

In general, the term directory is used to indicate an organized collection of information or files that can be queried to obtain specific information. Within the ITU-T and, more generally, within the context of security and telecommunications standardization, the term *the Directory* refers to a repository of information based on the ITU-T X.500 series of Recommendations which were developed jointly with ISO/IEC. The Directory, which is introduced in Recommendation ITU-T X.500, *The Directory: Overview of concepts, models and services*, and elaborated in Recommendations ITU-T X.501, *The Directory: Models*, ITU-T X.509, *The Directory: Public-key and attribute certificate frameworks*, and ITU-T X.519, *The Directoy: Protocol specifications*, provides directory services to facilitate communication and information exchange between entities, people, terminals, distribution lists, etc. In addition to conventional directory services such as naming, name-to-address mapping and allowing a binding between objects and their location, the Directory plays an important role in supporting security services by defining and holding authentication credentials in the form of security certificates. In particular, the ITU-T X.500 series of Recommendations cover two security aspects:

- the protection of directory information as defined primarily within ITU-T X.501 and ITU-T X.509; and
- the basic principles for public-key infrastructure (PKI) and privilege management infrastructure (PMI) as defined within ITU-T X.509.

This section begins with a discussion of the importance of the security of the Directory itself and the need to protect Directory information. The role of the Directory in supporting strong authentication, public-key infrastructures, identity management and telebiometrics is then reviewed.

6.1 Protection of Directory information

6.1.1 Directory protection objectives

Data protection, which is a major consideration in identity management, is constantly in focus in the Directory work. 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. Entity information may be sensitive and should be revealed only to those having a right and a *need-to-know*.

There are three aspects of data protection:

- authentication of the user seeking access to 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.

Almost from the beginning, data protection features have been an important part of ITU-T X.500. ITU-T X.500 is the only directory specification having these important features.

6.1.2 Authentication of Directory users

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

a) name only;

b) name plus unprotected password (i.e., the name and a password that is transmitted in clear text);

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 also allows detection of attempted replay.

Different levels of data protection are required for different types of accessing users. The authentication level of a user also affects the access rights of that user.

6.1.3 Directory access control

Access control is used to permit or deny operations on pieces of directory information. ITU-T X.500 is very flexible on how directory information and users can be subdivided for access control purposes. A piece of information to be 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.

6.1.4 Privacy protection

The ITU-T X.500 data privacy protection is unique and very powerful. Data privacy protection is mainly an issue when a user searches the directory by supplying general search criteria that could result in the return of a substantial amount of information. (Such searches are sometimes called data trawling.)

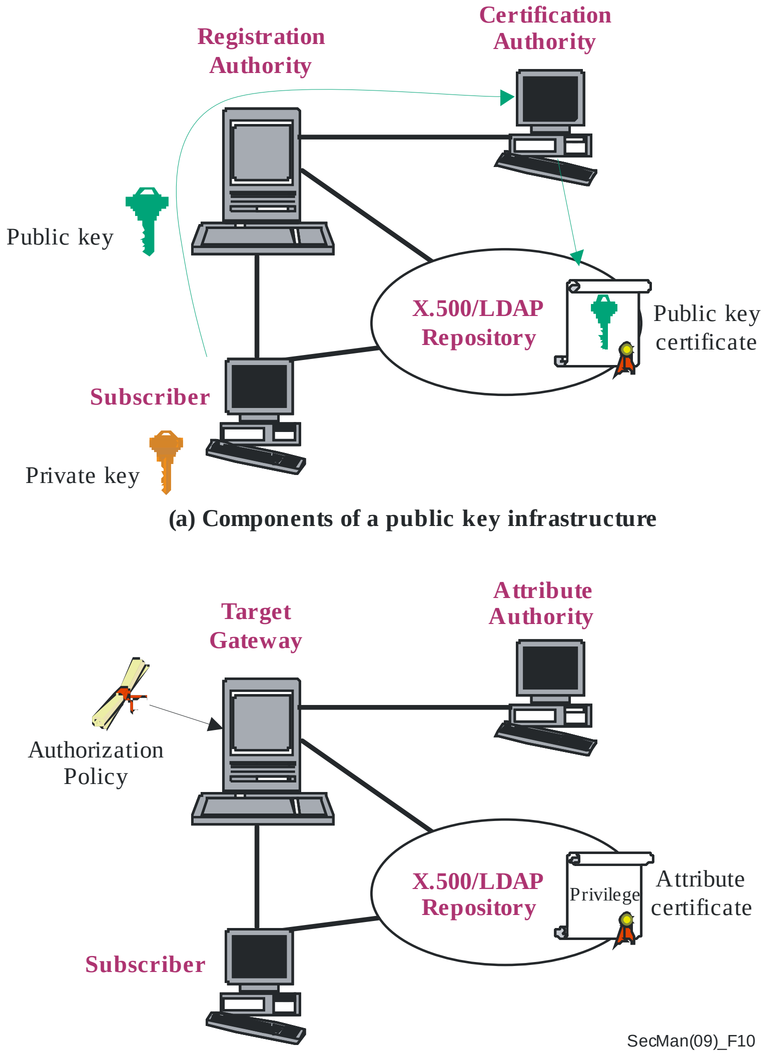
ITU-T X.500 has a table-driven service administration concept which, in addition to administration of general services, also provides data privacy protection capabilities. The administrator creates one or more tables for each combination of service type and group of users. For data retrieval to succeed, there must be a table that exactly matches the type of service and the type of user group. However, this is not enough. The table is protected by access control, i.e., 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 the recently-approved Recommendation ITU-T X.1171, *Threats and requirements for protection of personally-identifiable information in applications using tag-based identification*, which is discussed in more detail in section 9.5 on Tag-based Services, and the guideline on protection for personally-identifiable information in RFID application that is now in development by SG 17 as part of the IDM work (see section 6.4).

6.2 Strong authentication: public-key security mechanisms

A public-key infrastructure (PKI) facilitates the management of public keys to support authentication, encryption, integrity and non-repudiation services. The fundamental technology of PKI is public-key cryptography, which is described below. Recommendation ITU-T X.509, *The Directory: Public key and attribute certificate frameworks* is a PKI standard for strong authentication based on public-key certificates and certification authorities. In addition to defining an authentication framework for PKI, ITU-T X.509 also provides for a privilege management infrastructure (PMI), which is used to ascertain rights and privileges of users in the context of strong authorization, based on attribute certificates and attribute authorities. The components of PKI and PMI are illustrated in Figure 10.



(a) Components of a public key infrastructure

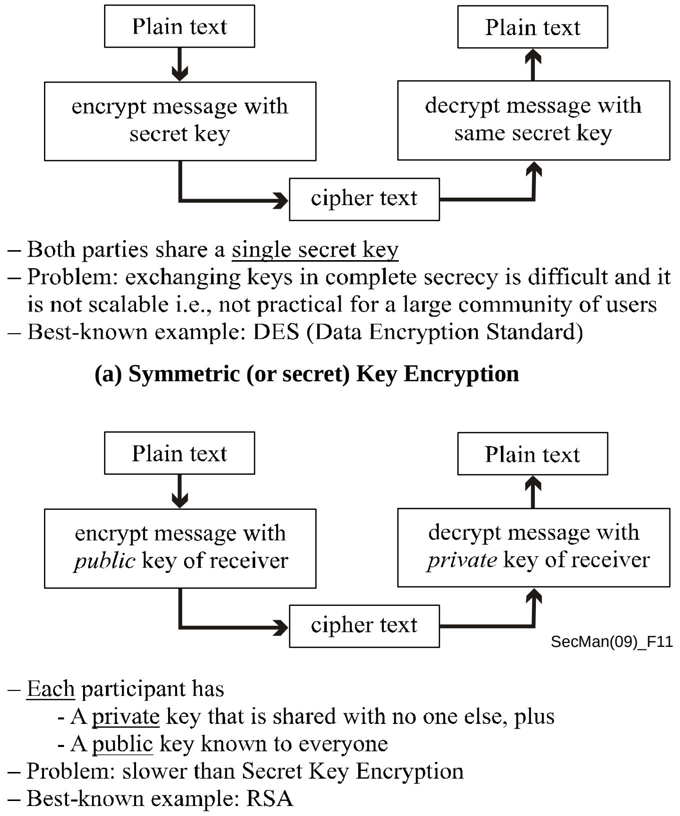
(b) Components of a privilege management infrastructure

Figure 10 – Components of PKI and PMI

6.2.1 Secret key and public key cryptography

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 11 (a). In a symmetric cryptosystem communicating individuals share a unique secret key. The key must be distributed to the individuals via secure means, because knowledge of the enciphering key implies knowledge of the deciphering key and vice versa.

An *asymmetric* (or *public key*) cryptography system involves a pair of keys – a public key and a private key – as illustrated in Figure 11 (b). Public keys can be widely distributed but the private key must always be kept secret. The private key is usually held on a smart card or on a token. The public key is generated from the private key and, although these keys are mathematically related, there is no feasible way to reverse the process to derive the private key from the public key. To send confidential data to someone securely using public-key encryption, the sender encrypts the data with the recipient's public key. The recipient decrypts it with their corresponding private key. Public-key encryption can also be used to apply a digital signature to data to provide confirmation that a document or message originated with the person who claims to be the sender (or originator). The digital signature is actually a digest of the data produced using the signer's private key and appended to the document or message. The recipient uses the signer's public key to confirm the validity of the digital signature. (NOTE – Some public-key systems use two distinct public/private key pairs, one for encryption/decryption, the other for digital signature/verification.)


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(09)_F11

– 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: DES (Data 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 11 – Illustration of secret key and public-key encryption processes

With symmetric encryption, each pair of users must have different keys and these must be distributed and held securely. With asymmetric encryption, on the other hand, the public encryption keys can be published in the Directory and everyone can use the same (public) encryption key to send data to a particular user 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. In practice asymmetric encryption is typically used to distribute symmetric encryption keys securely. The symmetric keys are then used to encrypt the body of the message using a more computationally-efficient symmetric algorithm. When a digital signature is required, a digest (or hash) of the message is produced using a secure one-way hash function (such as SHA-1 or MD5). The hash is then encrypted (using the private key of the sender) and appended to the message. The recipient can confirm the validity of the digital signature by decrypting the digital signature with the sender's public key to obtain the hash generated by the sender and then creating its own hash of the received message. The two hashes must be the same for the signature to be valid.

Regardless of whether symmetric or asymmetric encryption is used, it is not possible to route messages to their recipients if the entire message (including the headers) is encrypted, since the intermediate nodes will not be able to determine the recipient's address. Therefore, message headers must generally be unencrypted.

Secure operation of a public-key system is highly dependent on the validity of the public keys. Public keys are normally published in the form of digital certificates that are held within an ITU-T X.500 Directory. A certificate contains not only the public encryption key and, where applicable, the signature verification key for an individual, but also additional information including the validity of the certificate. Certificates that have been revoked for any reason are also normally listed in the Directory in a certificate revocation list (CRL). Before public keys are used, their validity is normally checked against the CRL.

6.2.2 Public-key certificates

A public-key certificate (sometimes called "digital certificate") is one way of validating the owner of an asymmetric key pair. A public-key certificate strongly binds a public key to its owner, and it is digitally signed by a trusted authority attesting to this binding. This trusted authority is known as a Certification Authority (CA). The internationally-recognized, standardized format for public-key certificates is defined in ITU-T X.509. An ITU-T X.509 public-key certificate comprises a public key, an identifier of the asymmetric algorithm with which the key is to be used, the name of the key pair owner, the name of the CA attesting to this ownership, the serial number and validity period of the certificate, the ITU-T X.509 version number to which the certificate conforms, and an optional set of extension fields that hold information about the certification policy of the CA. The whole certificate is digitally signed using the private key of the CA. An ITU-T X.509 certificate can be widely published, for example on a web site, in an LDAP Directory, or in a vCard[1] attached to e-mail messages. The CA's signature ensures that the certificate contents cannot be modified without detection.

To confirm the validity of a certificate, a person needs to have access to the valid public key of the issuing CA in order to verify the CA's signature on the certificate. As a CA may have its public key certified by another (superior) CA, validating public keys may involve a chain of certificates and CAs. Eventually this chain must end somewhere, which is typically the certificate of the CA that is the "root of trust". Root CA public keys are distributed as self-signed certificates (in which the root CA is attesting that this is its own public key). The signature allows a user to confirm that the key and CA name have not been tampered with since the certificate was created. However the name of the CA embedded in a self-signed certificate cannot automatically be assumed to be correct, since the CA inserted the name in the certificate itself. Thus, a critical component of a public-key infrastructure is the secure distribution of root CA public keys in a manner that can provide assurance that the public key really does belong to the root CA named in the self-signed certificate. Without this assurance, one cannot be sure that someone is not masquerading as the root CA.

6.2.3 Public-key infrastructures

The main purpose of a PKI is to issue and manage public-key certificates, including the certificates of the root CA. Key management includes the creation of key pairs, the creation of public-key certificates, the revocation of public-key certificates (for example, if a user's private key has been compromised), the storage and archival of keys and certificates, and their destruction once they have come to the end of their life. Each CA will operate according to a set of policies. ITU-T X.509 provides mechanisms for distributing some of this policy information in the extension fields of the ITU-T X.509 certificates issued by the CA. The policy rules and procedures followed by a CA are usually defined in a certificate policy (CP) and a certification practice statement (CPS), which are documents published by the CA. These documents help to ensure a common basis for evaluating the trust that can be placed in the certificates issued by CAs, both

[1] A vCard is a standard-format electronic business card that is often exchanged by e-mail.

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 certificates.

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

6.2.4 Privilege management infrastructure

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 4 illustrates the similarities between the two infrastructures.

Table 4 – 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 5.

Table 5 – Structure of a 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 (see section 6.5) 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 ITU-T X.509: the privilege asserter; the privilege verifier; the object method; the privilege policy; and environmental variables (see Figure 12). The privilege verifier can control access to the object method by the privilege asserter, in accordance with the privilege policy.

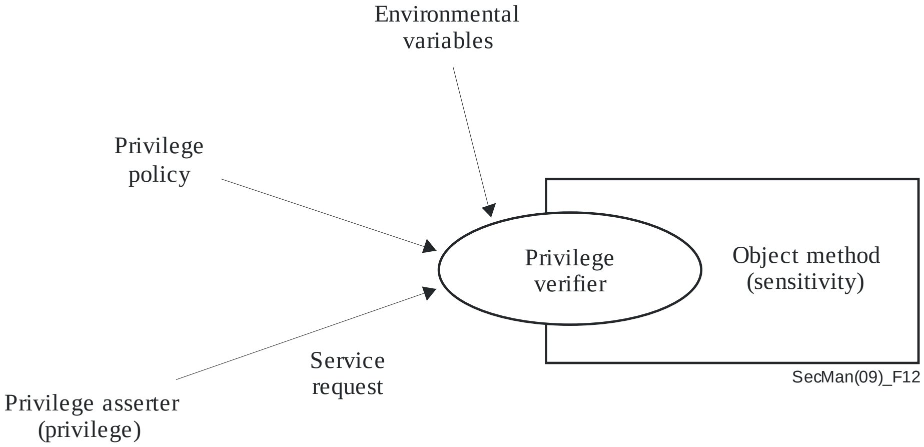


Figure 12 – X.509 PMI control model

Where delegation of privilege is necessary for an implementation, four components of the delegation model for PMI are considered in ITU-T X.509: the privilege verifier; the source of authority; other attribute authorities; and the privilege asserter (see Figure 13).

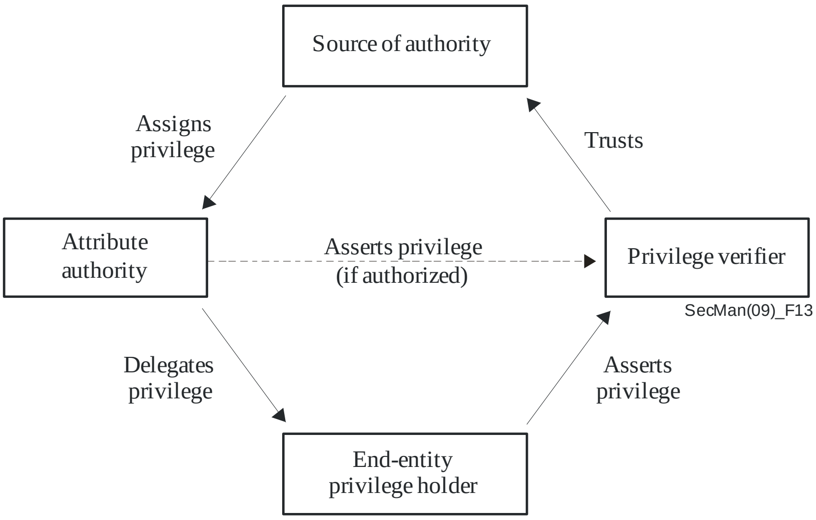


Figure 13 – X.509 PMI delegation model

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 a role. When accessing a resource, the user has his or her role checked against the policy to enable any subsequent action.

6.3 Authentication guidelines

A number of guidelines have been developed that deal with specific aspects of authentication. These are summarized below.

6.3.1 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 Rec. ITU-T X.1151, *Guideline on secure password-based authentication protocol with key exchange*. This protocol is very simple. It is easy to implement and use and it requires no other infrastructure (such as PKI). It is expected to be of growing importance to many applications in the near 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 14).

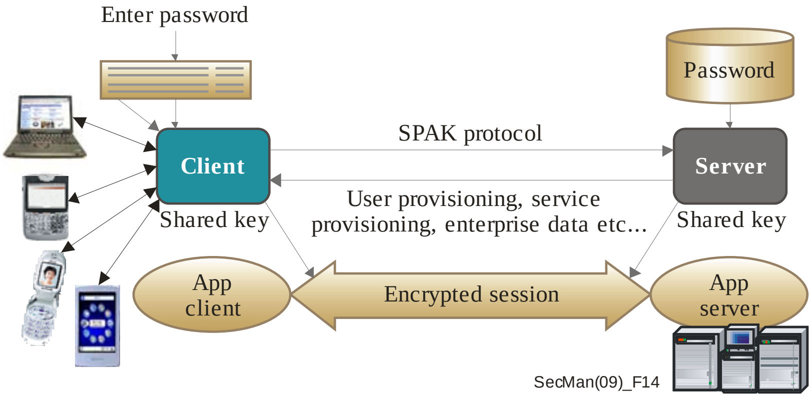


Figure 14 – Typical operation for SPAK protocol

6.3.2 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 15. 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 of an end-user 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 15). 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 as a result of the EAP protocol. In the key distribution phase, the authentication server transports the master secret to an authenticator to allow authentication to derive various cryptographic keys for a subsequent session between a supplicant and an authenticator. To prevent the use of the same secret key over and over, 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.

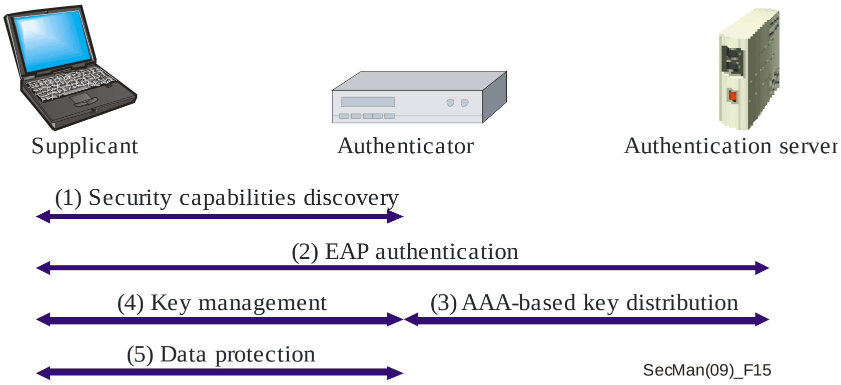


Figure 15 – Four operational phases for the authentication and key management of the lower layer

6.4 Identity management

6.4.1 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 the 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 and can provide 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 capability 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).

The ITU-T X.1250 series supplement Overview of identity management in the context of cybersecurity provides a brief introduction to the topic of identity management.

6.4.2 ITU-T identity management work

Although there is still on-going discussion on some of the basic concepts and underlying vocabulary, work is progressing in a number of areas in SG 17 (the Lead SG on IdM) as well as SG 2 (operational aspects of service provision and telecommunication management) and SG 13 (future networks including mobile and NGN).

SG 2 is responsible for studies relating to ensuring the consistency of the format and structure of IdM identifiers and for specifying interfaces to management systems to support the communication of identity information within or between organizational domains.

SG 13 is responsible for NGN-specific identity management 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. SG 13 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*, has already been approved. This standard describes a structured approach for designing, defining, and implementing IdM solutions and facilitating interoperability in heterogeneous environments.

SG 17 is responsible for studies relating to the development of a generic identity management model that is independent of network technologies and supports the secure exchange 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. In September 2009 two Recommendations were approved: Rec. ITU-T X.1250, *Baseline capabilities for enhanced global identity management and interoperability*, and Rec. ITU-T X.1251, *A framework for user control of digital identity*. In addition, a baseline set of IdM-related definitions is in preparation to help ensure uniform and consistent terminology in ITU-T IdM standards.

A Joint Coordination Activity for Identity Management (JCA-IdM) has been established to coordinate the ITU-T IdM work. An IdM Global Standards Initiative (IdM-GSI) has also been established to harmonize the different world-wide approaches to IdM and to collaborate with other bodies working on this topic. The IdM Lead Study Group page provides extensive information on IdM activities, approved and developing IdM recommendations and other information related to the IdM work.

6.5 Telebiometrics

Telebiometrics focuses on personal identification and authentication using biometric devices in telecommunication environments. In particular, it focuses on how identification and authentication of users may be improved by the use of safe and secure telebiometric methods. The ITU-T work on this topic is done in close cooperation with other standards development organizations and covers topics that include: interaction between a human being and the environment; biometric digital keys; biometric extensions for X.509 certificates; and biometric authentication in an open network.

6.5.1 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 (false accept rate) determined by the threshold parameter differs between different biometric products. Therefore, the service provider cannot claim to maintain a uniform accuracy level; and
- the accuracy of biometric verification may decline with the aging of end-users, because biometrics uses characteristics of the human body.

General biometric authentication protocols and profiles for telecommunication systems in an open network are specified in Recommendation ITU-T X.1084, *General biometric authentication protocol and system model profiles for telecommunications systems*.

Figure 16 illustrates the authentication of an end user via a non-face-to-face open network.

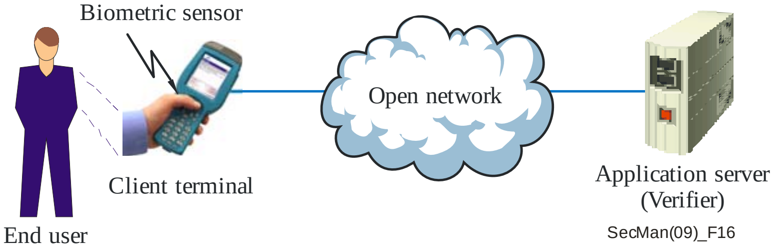


Figure 16 – Telebiometric authentication of an end user

6.5.2 Telebiometric digital key generation and protection

A framework for biometric digital key generation has been defined in Rec. ITU-T X.1088, *A framework for biometric digital key generation and protection*. 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 17); and
- biometric-key binding/restoring, in which the key is stored in a database and can be extracted by biometric authentication (Figure 17)

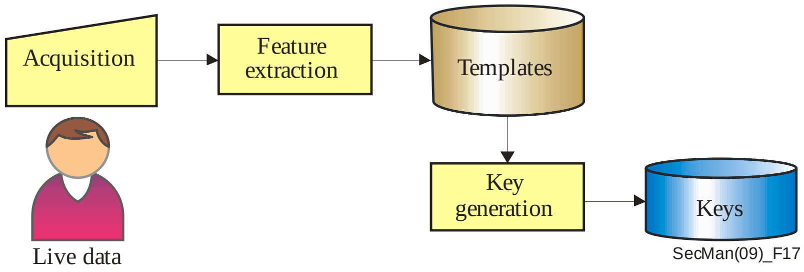


Figure 17 – Biometric-key generation

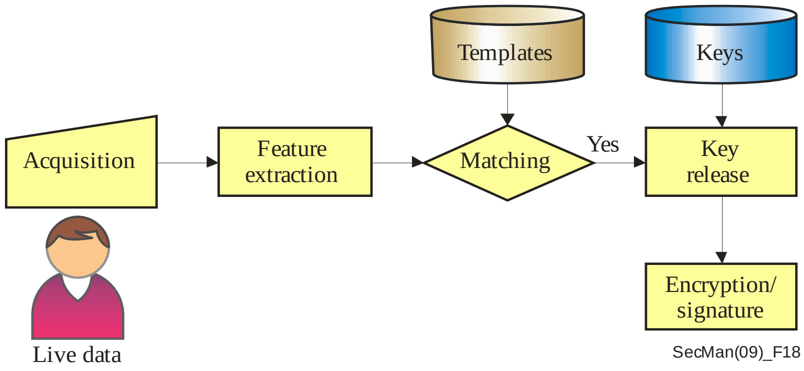


Figure 17 – Biometric-key binding/restoring

6.5.3 Security and safety aspects of telebiometrics

A framework for the security and safety aspects of telebiometrics has been defined in the telebiometric multimodal model (Rec. ITU-T X.1081, *A framework for the specification of security and safety aspects of telebiometrics*), which defines the interactions between a human being and the environment and also the quantities and units used to measure these interactions. The telebiometric multimodal model is not limited to consideration of purely physical interactions, but also recognizes behavioural interactions which are currently not quantified by standard units.

6.5.4 Telebiometrics related to human physiology

Security and safety aspects of telebiometrics are also addressed in Recommendation ITU-T X.1082, *Telebiometrics related to human physiology*, 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.

6.5.5 Other developments in telebiometrics 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 Rec. ITU-T X.1089, *Telebiometrics authentication infrastructure.*

Recommendation ITU-T X.1083, *BioAPI interworking protocol* specifies the syntax (using ASN.1), semantics, and encodings of messages that enable a BioAPI-conforming application to request biometric operations in BioAPI-conforming biometric service providers (BSPs) across node or process boundaries, and to be notified of events originating in those remote BSPs.

7. Securing the network infrastructure

7 Securing the network infrastructure

The data used to monitor and control the telecommunications network management traffic 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, *Principles for a telecommunications management network*. 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 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.

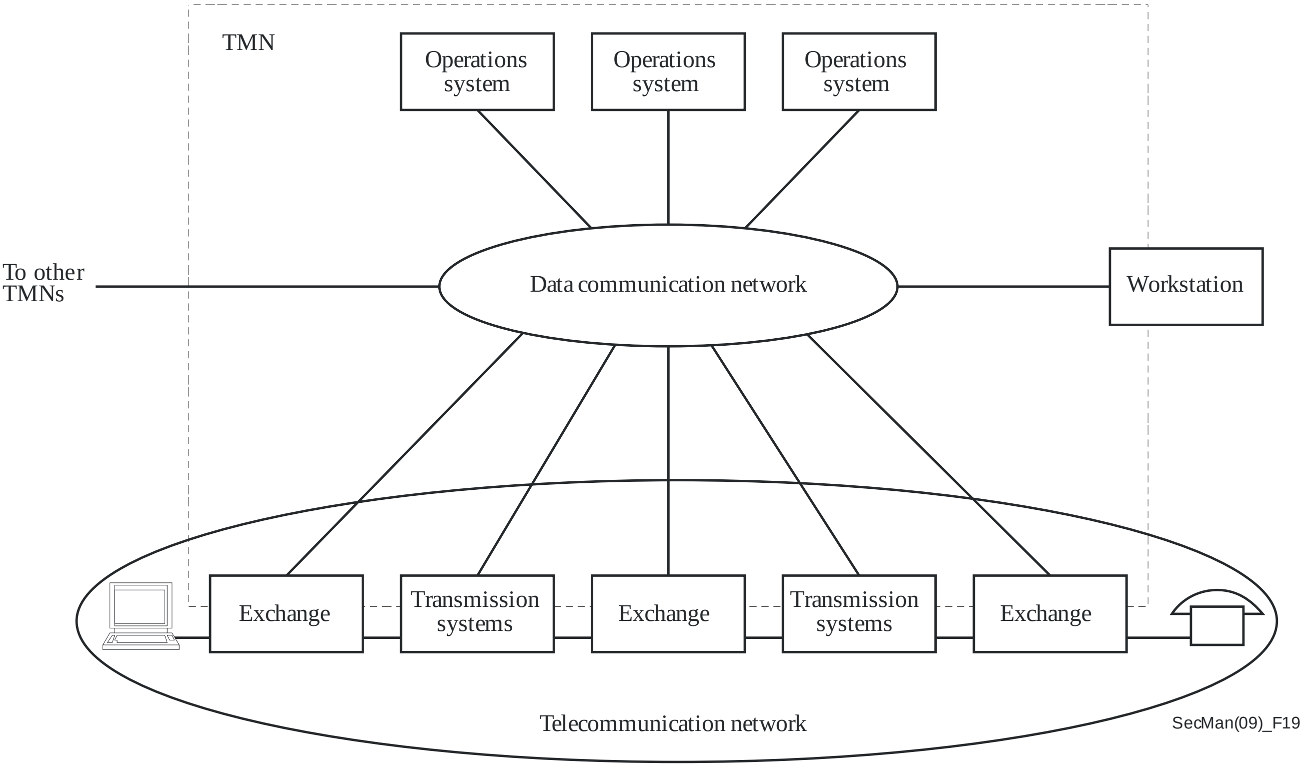
Other network management applications include those related to environments where different service providers need to interact to offer end-to-end services. Examples include communications facilities provided to regulatory or government institutions in support of disaster recovery, and situations where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

7.1 The telecommunications management network

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, and many types of malicious activities become possible.

7.2 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 18. The management network architecture defines interfaces that determine the exchanges required to perform the operations, administration, maintenance and provisioning functions.



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

Figure 18 – 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 Rec. ITU-T M.3010. Because not all requirements need to be supported by all organizations, Rec. ITU-T M.3016.4 provides a proforma for creating profiles based on the security requirements, services and mechanisms. This may be used to 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). 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 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.

7.3 Securing the infrastructure elements of a network

End-to-end connectivity may be considered in terms of access network(s) and core network(s). 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 Rec. 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 19 shows the various objects 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.

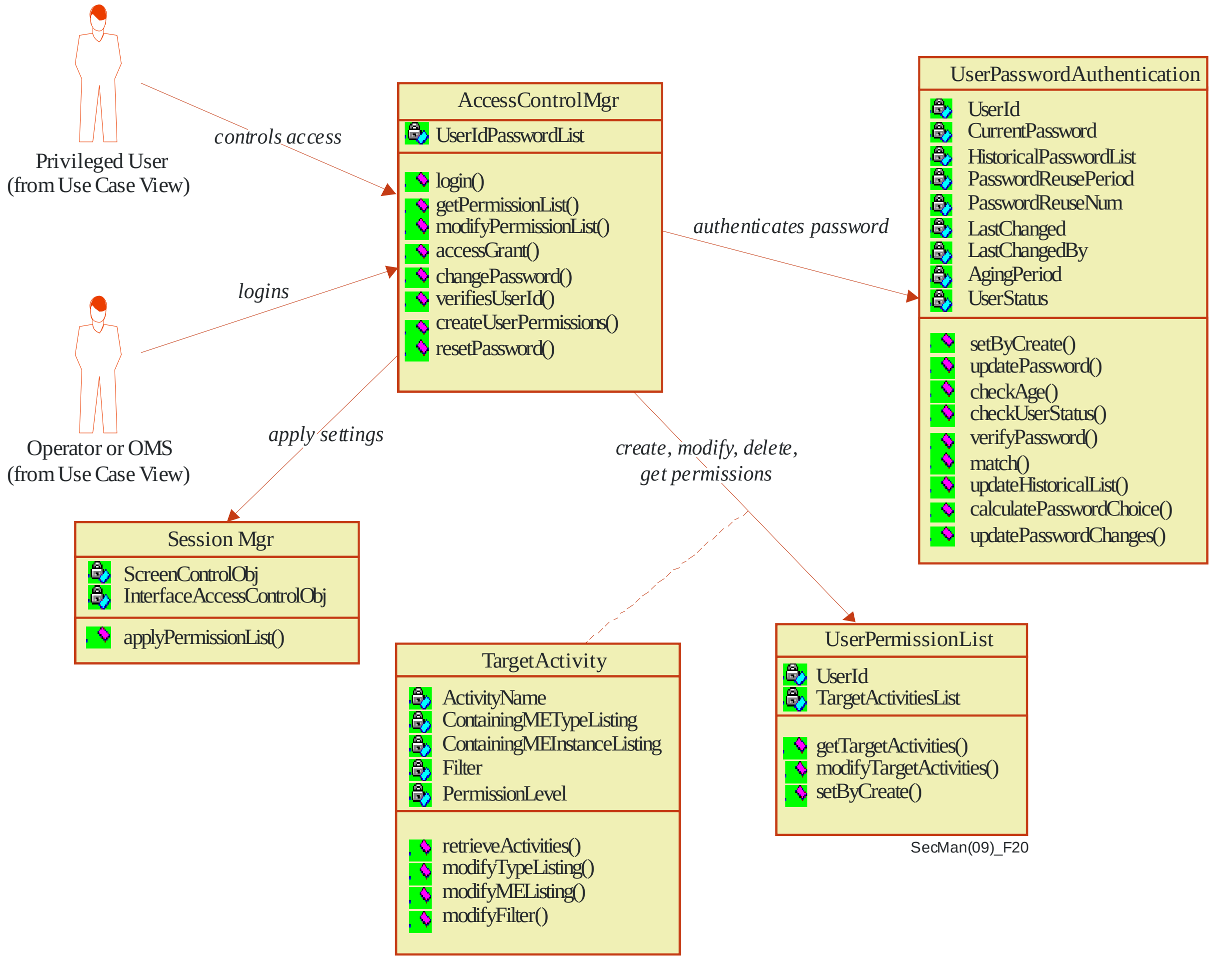


Figure 19 – Administering user privileges in ITU-T Q.834.3

7.4 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, *Connection management of pre-provisioned service link connections to form a leased circuit service*, 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 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, *TMN management services for IMT-2000 security management,* 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 in the home location collects appropriate information about a subscriber who is registered on the visited network. Scenarios a) and b) in Figure 20 show initiation of the monitoring management 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.

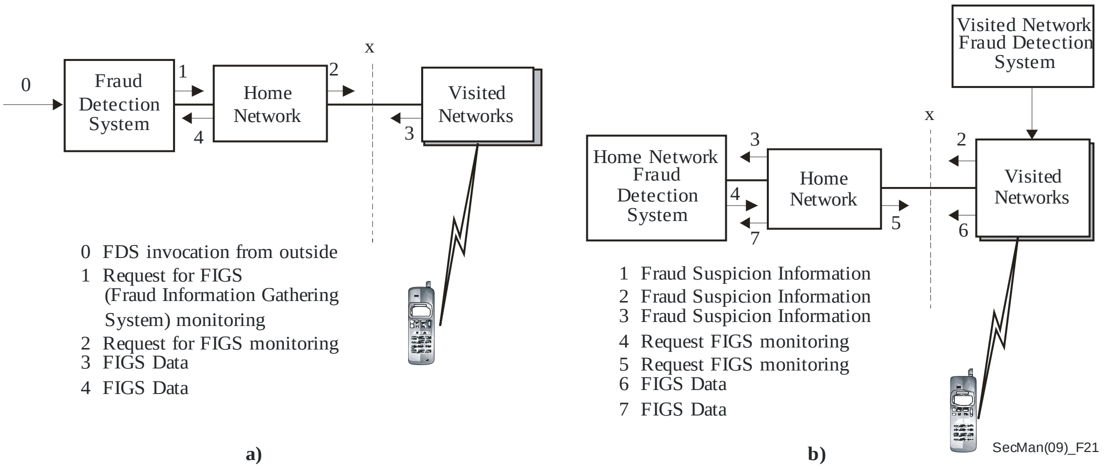

0
Fraud Detection System
1
4
Home Network
2
x
Visited Networks
3
0 FDS invocation from outside
1 Request for FIGS (Fraud Information Gathering System) monitoring
2 Request for FIGS monitoring
3 FIGS Data
4 FIGS Data
a)
Visited Network Fraud Detection System
Home Network Fraud Detection System
3
4
7
Home Network
5
x
2
Visited Networks
6
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(09)_F21

Figure 20 – Fraud Management for Wireless Services

7.5 Securing network-based 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, and 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 21 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.

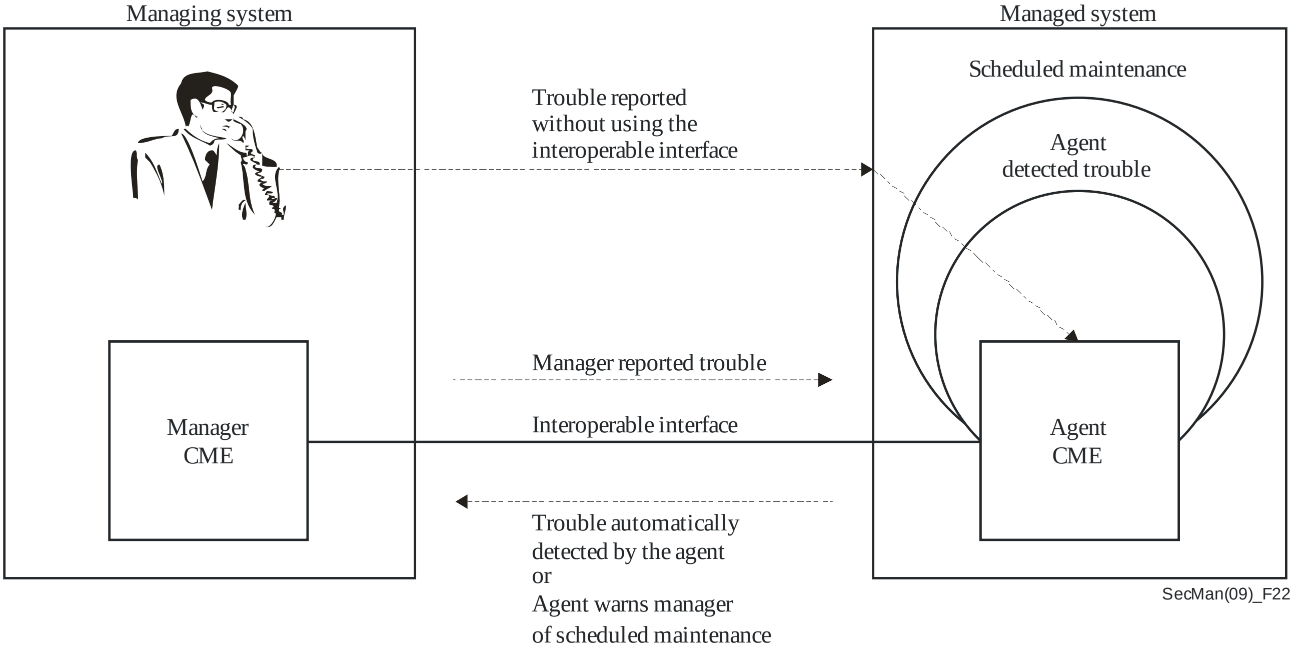


Figure 21 – Trouble management report creation

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

7.6 Common security management services

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

7.6.1 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 6.

Table 6 – Security alarm causes

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 tamper 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

These alarm causes are explained further in Rec. ITU-T X.736, *Security alarm reporting function*.

7.6.2 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 Rec. ITU-T X.740.

7.6.3 Access control for managed entities

A very detailed definition for the model associated with assigning access control to various managed entities is described in Rec. ITU-T X.741, *Objects and attributes for access control*. 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.

7.6.4 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 Rec. ITU-T X.780, *TMN Guidelines for defining CORBA managed objects*; Rec. ITU-T X.780.1, *TMN guidelines for defining coarse-grained CORBA managed object interfaces*; Rec. ITU-T X.780.2, *TMN guidelines for defining service-oriented CORBA managed objects and façade objects*; and Rec. ITU-T X.781, *Requirements and guidelines for Implementation Conformance Statements proformas associated with CORBA-based systems*. 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.

8. Some specific approaches to network security

8 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. Next, security provisions for home networks and cable television are examined. Lastly, the challenges of security for ubiquitous sensor networks are presented.

8.1 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 broadband, 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, *General overview of NGN*.

8.1.1 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.

The NGN security studies must address and develop network architectures that:

- provide for maximum network and end-user resource protection;
- allow for highly-distributed intelligence end-to-end;
- allow for co-existence of multiple networking technologies;
- provide for end-to-end security mechanisms;
- provide for security solutions that apply over multiple administrative domains;
- provide for secure identity management, which involves, but is not limited to:
  - reliable authentication of the NGN entities (e.g. users, user devices, network providers, service providers, identity providers, etc.);
  - prevention of the unauthorized access to identity data in NGN;
  - secure exchange of identity information among federated entities in NGN;
  - support for keeping records of the use of identity information in NGN;
  - support for the user privacy and anonymity in NGN; and
  - capability of supporting the NGN users to help them manage their identity information securely (e.g., modifying user profiles, changing passwords, enabling location-based services, viewing billing records, etc.);

- provide for security solutions for IPTV that are cost-effective and have acceptable impact on the performance, quality of service, usability, and scalability. The types of protection that IPTV security should provide include, but are not limited to:
  - content protection;
  - service protection;
  - network protection;
  - terminal protection; and
  - subscriber protection.

Recommendation ITU-T Y.2701, *Security requirements for NGN release 1*, which is based on the principles of 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 22.

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.

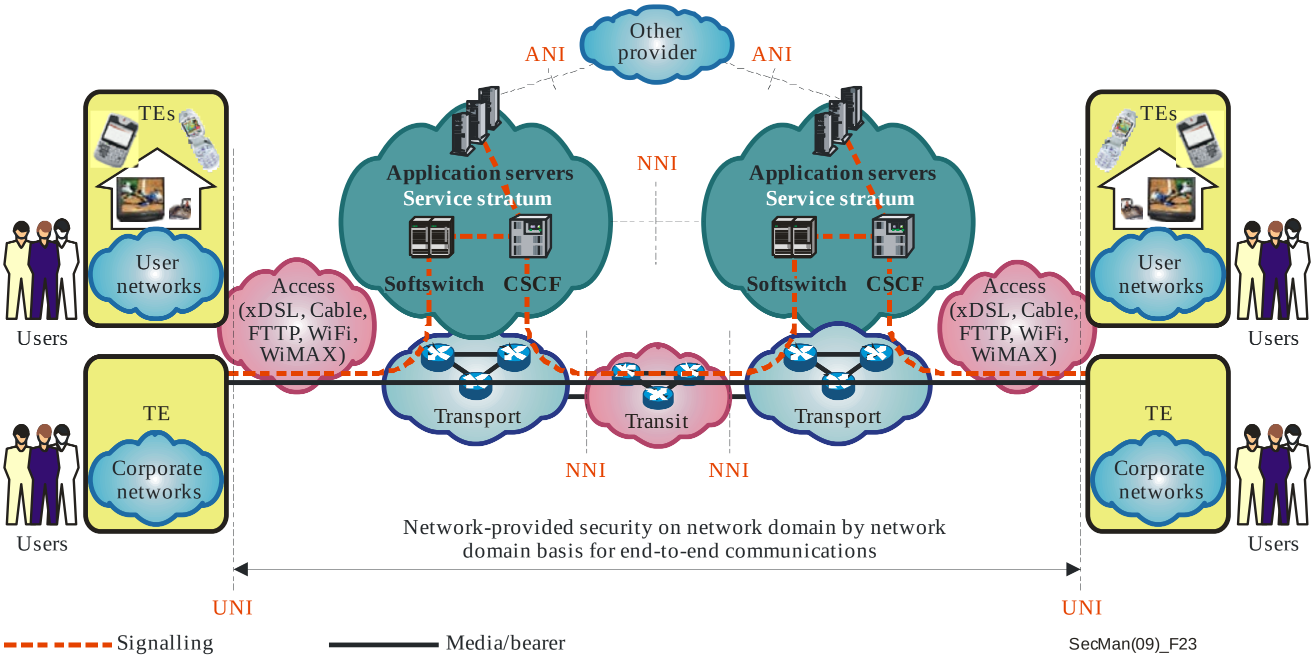


Figure 22 – Security of communications across multiple networks

8.2 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. In other words, 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.

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 will threaten 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. With the deployment of mobile IP services and applications, security measures become much more important to the user, the operator and the service provider.

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.

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 will exploit 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, including 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, *Framework for IMT-2000 networks*, ITU-T Q.1702, *Long-term vision of network aspects for systems beyond IMT-2000* and ITU-T Q.1703, *Service and network capabilities framework of network aspects for systems beyond IMT-2000*.

In addition, the 3G specifications contained in the ITU-T Q.1741 (3GPP) series of Recommendations and in the ITU-T Q.1742 (3GPP2) series 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.

8.2.1 Secure mobile end-to-end data communications

Mobile terminals with data communications capability (e.g., IMT-2000 mobile phones, laptop PCs, and PDAs with a radio-card) are widely available and various application services (such as e-commerce) use terminals connected to the mobile network. For business applications as well as for protection of the end user, effective security is essential.

Mobile networks are particularly vulnerable due to the nature of the wireless network and the inherent vulnerabilities of wireless communication technologies. 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.

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

Recommendation ITU-T X.1121, *Framework of security technologies for mobile end-to-end data communications* 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 23 and Figure 24. The ASP provides the service 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 25 depicts the threats in the mobile end-to-end data communication network. Figure 26 shows the places where security features are required for each entity and the relationship between entities.

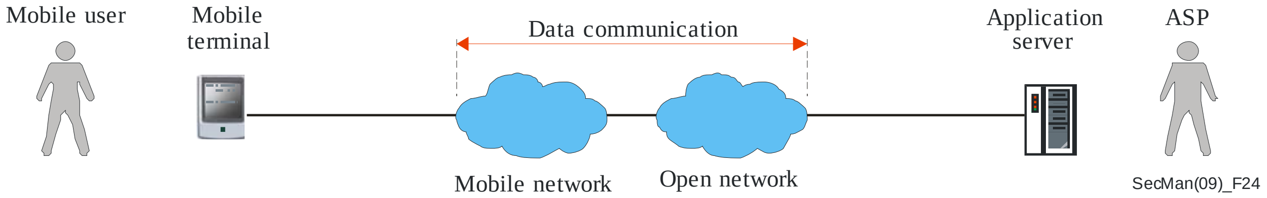


Figure 23 – General model of end-to-end data communication between a user and an ASP

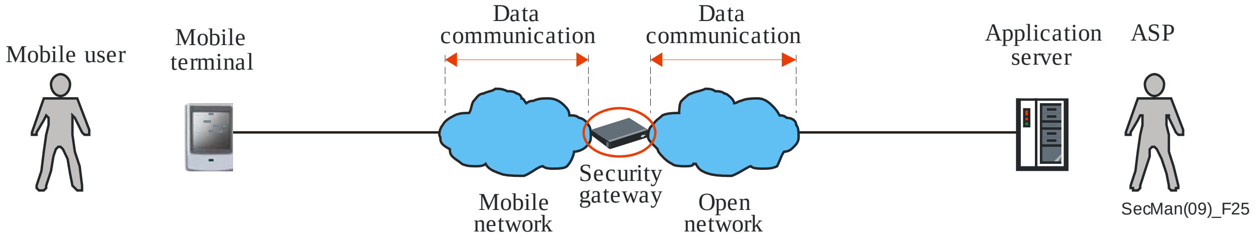


Figure 24 – Gateway model of mobile end-to-end data communication between a mobile user and an ASP

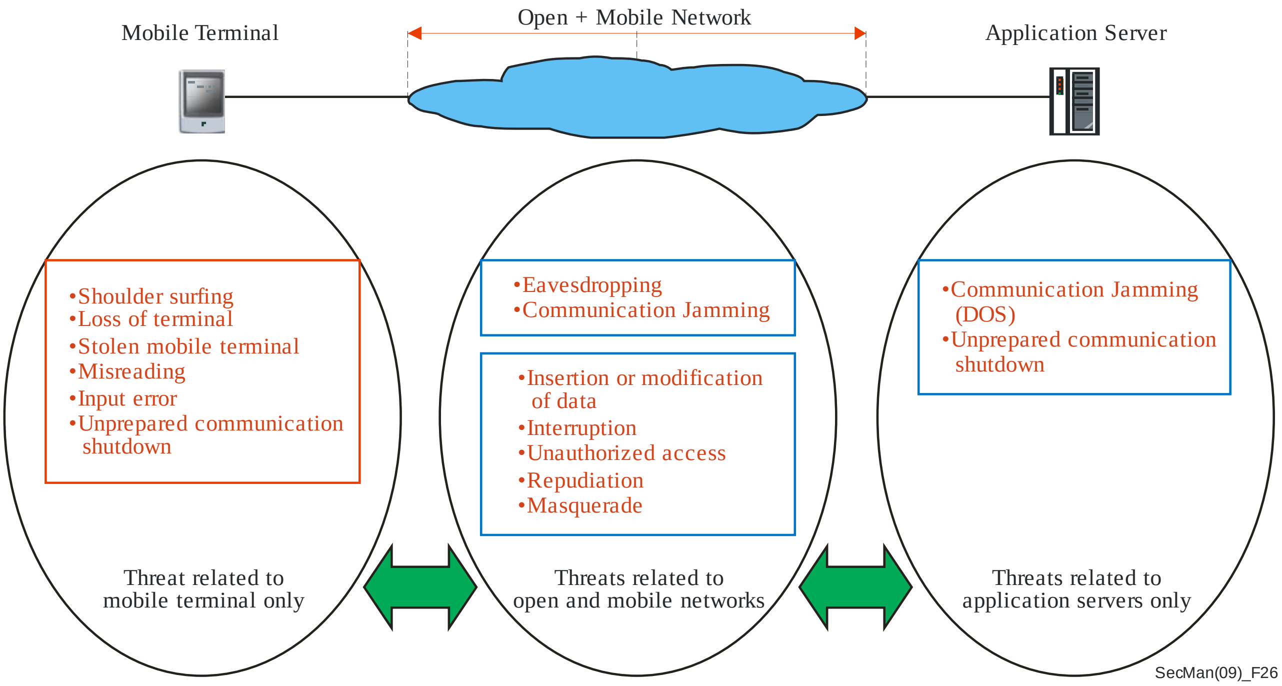

Mobile Terminal
Open + Mobile Network
Application Server
•Shoulder surfing
•Loss of terminal
•Stolen mobile terminal
•Misreading
•Input error
•Unprepared communication shutdown
•Eavesdropping
•Communication Jamming
•Insertion or modification of data
•Interruption
•Unauthorized access
•Repudiation
•Masquerade
•Communication Jamming (DOS)
•Unprepared communication shutdown
Threat related to mobile terminal only
Threats related to open and mobile networks
Threats related to application servers only
SecMan(09)_F26

Figure 25 – Threats in the mobile end-to-end communications

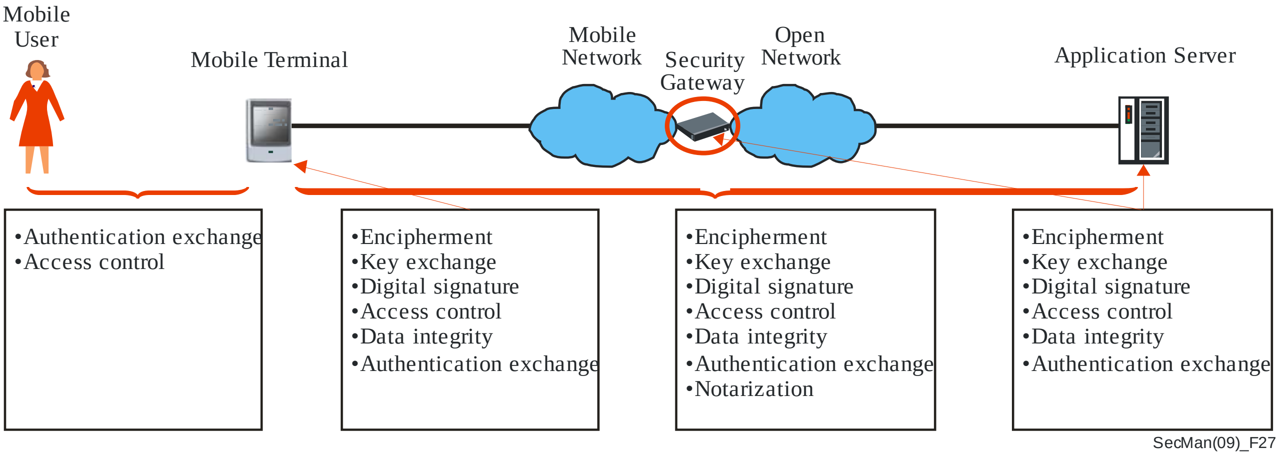


Figure 26 – Security function required for each entity and relation between entities

8.2.1.2 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 Rec. ITU-T X.1122, *Guideline for implementing secure mobile systems based on PKI*, which provides both a general PKI model and a gateway PKI model.

In the general model (shown in Figure 27) the mobile user's CA issues the user's certificate and manages the repository and certificate revocation list (CRL). The mobile user's validation authority provides an online certificate validation service to the mobile user. The ASP's CA 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.

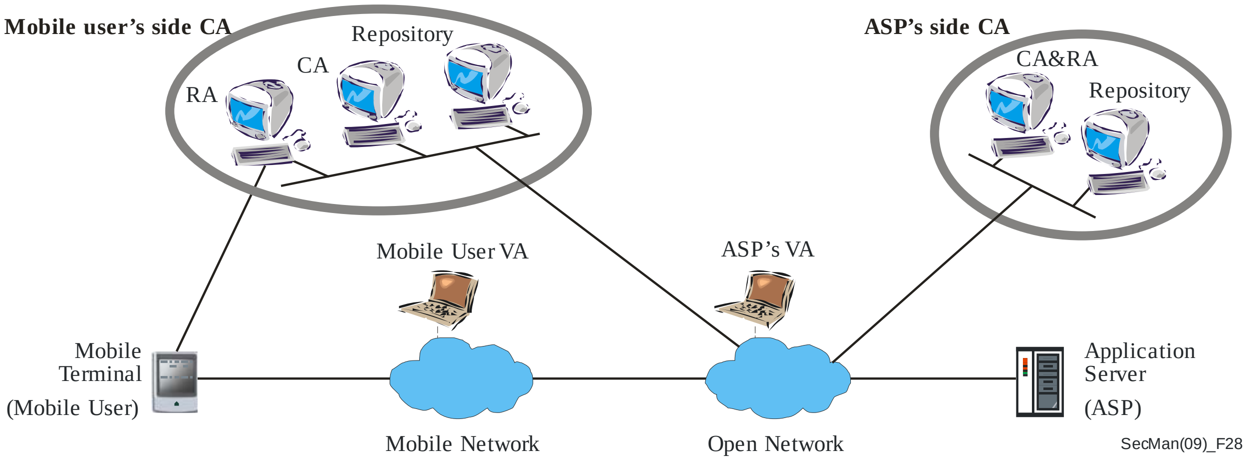


Figure 27 – General PKI model for mobile end-to-end data communications

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 at the mobile-terminal factory; 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 28 illustrates the procedure for a mobile terminal to acquire a certificate, where the cryptographic key pair is generated in the mobile terminal.

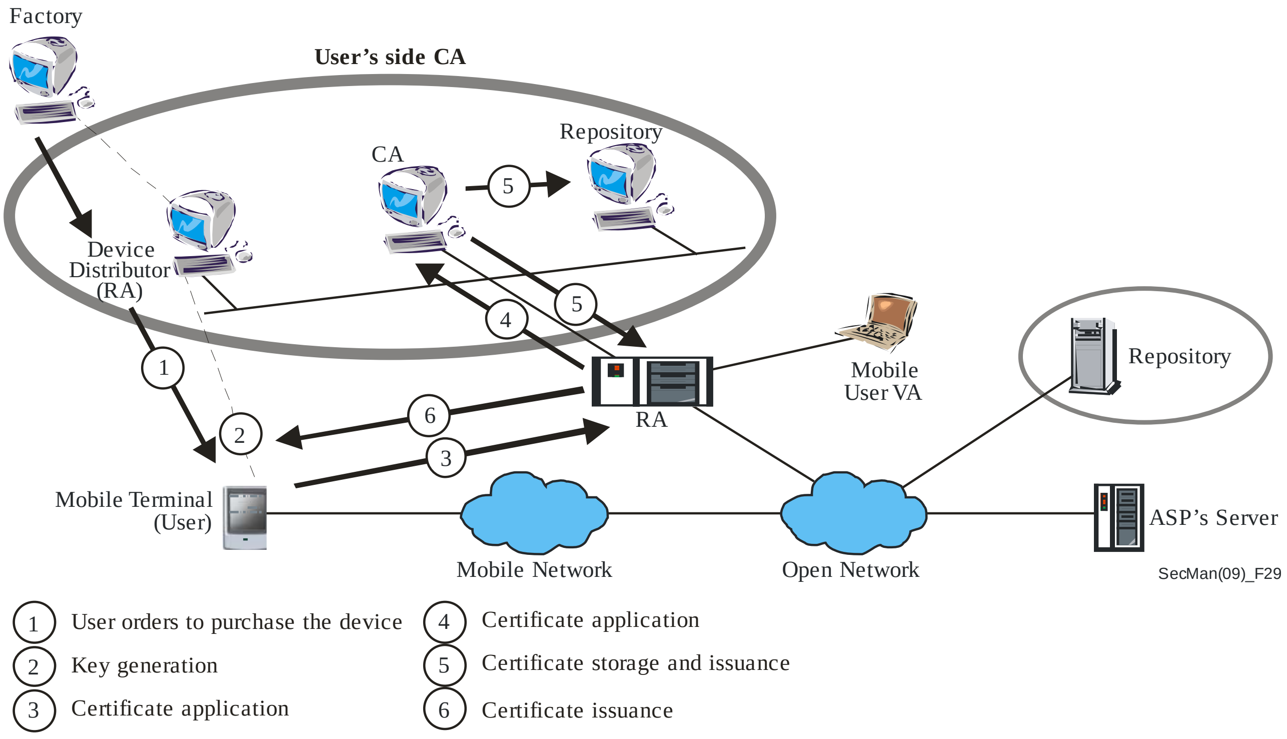


Figure 28 – Certificate issuance procedure for mobile terminal

The mobile terminal has a limited computational power and memory size. As a result, online certificate validation is preferable to off-line certificate validation based on a CRL. Figure 29 depicts the on-line certificate validation procedure for a mobile terminal.

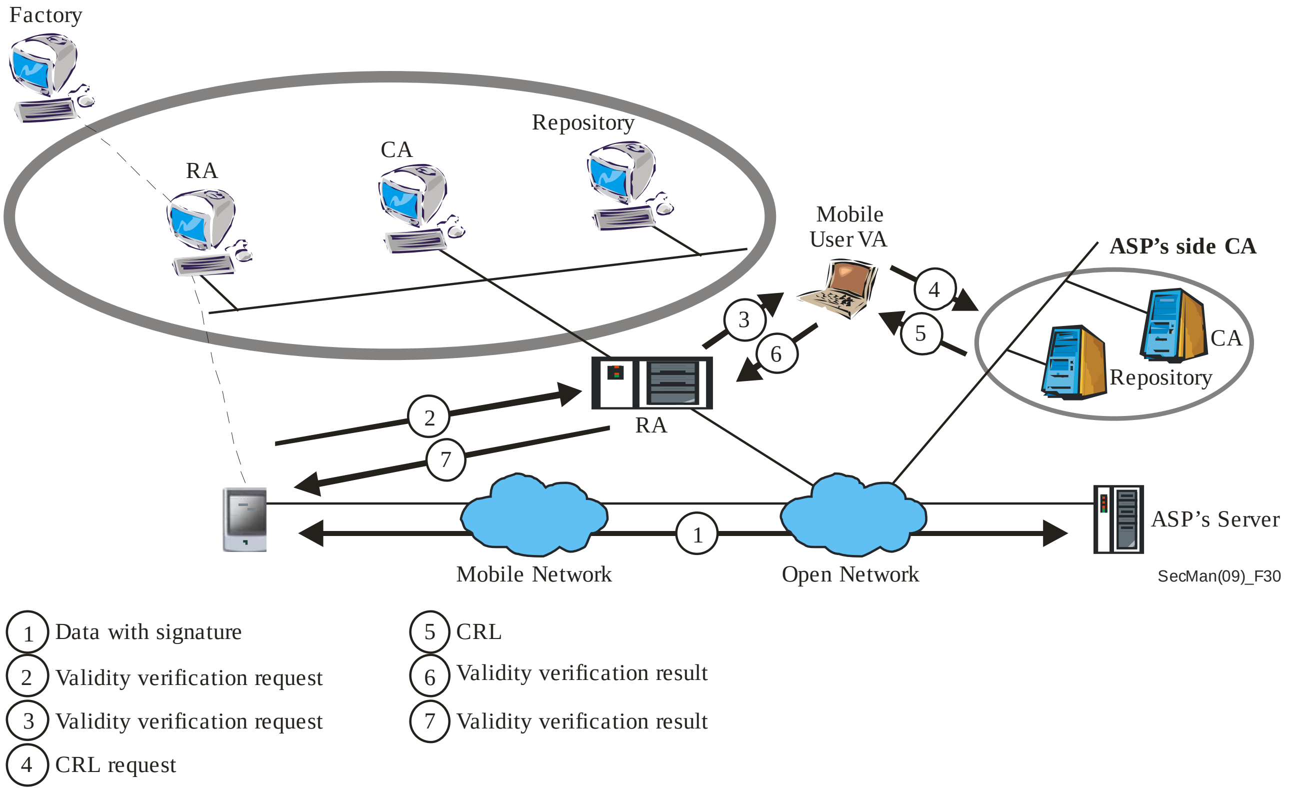


Figure 29 – Certificate validation for mobile end-to-end data communications

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.

8.2.1.3 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 together 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.

8.3 Security for home networks

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

8.3.1 Security framework for the home network

Recommendation ITU-T X.1111, *Framework of security technologies for home network*, builds upon the threat model of Rec. 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;
- remote terminals may be carried around by remote users; and
- the various types of home network device require different levels of security.

The general home network model for security, which is shown in Figure 30, 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 are bridges that connect type C devices (which have no communication interface) to the network, i.e., 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.

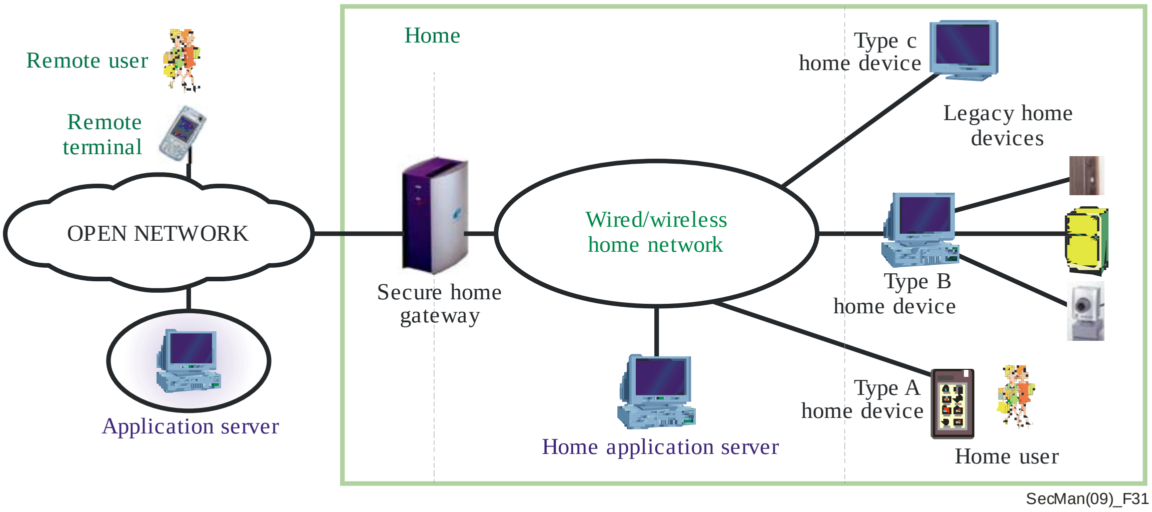


Figure 30 – General home network model for security

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.

8.3.2 Device certification 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 31.

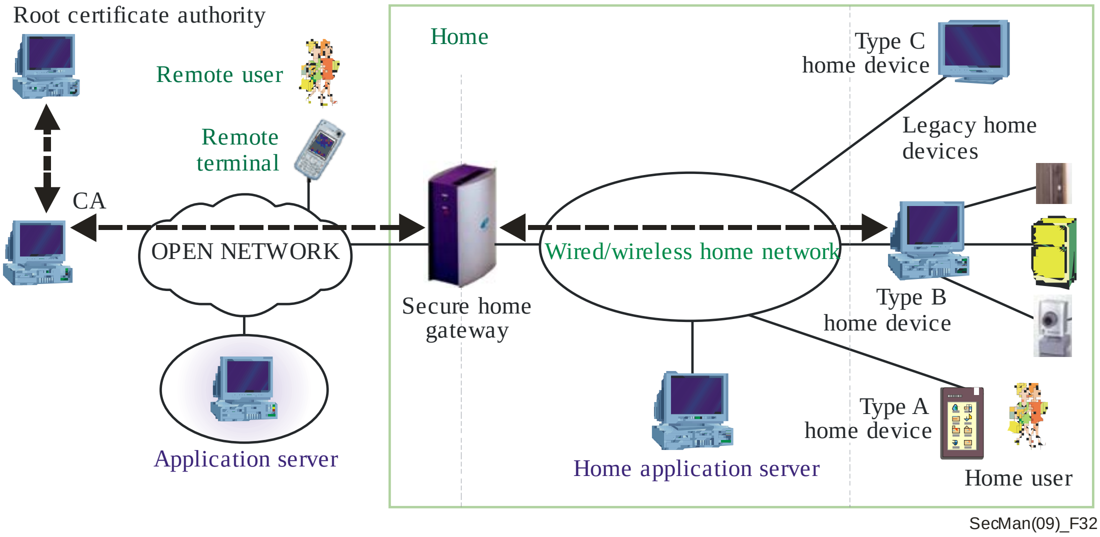


Figure 31 – Device authentication model for the secure home network

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

Figure 32 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.

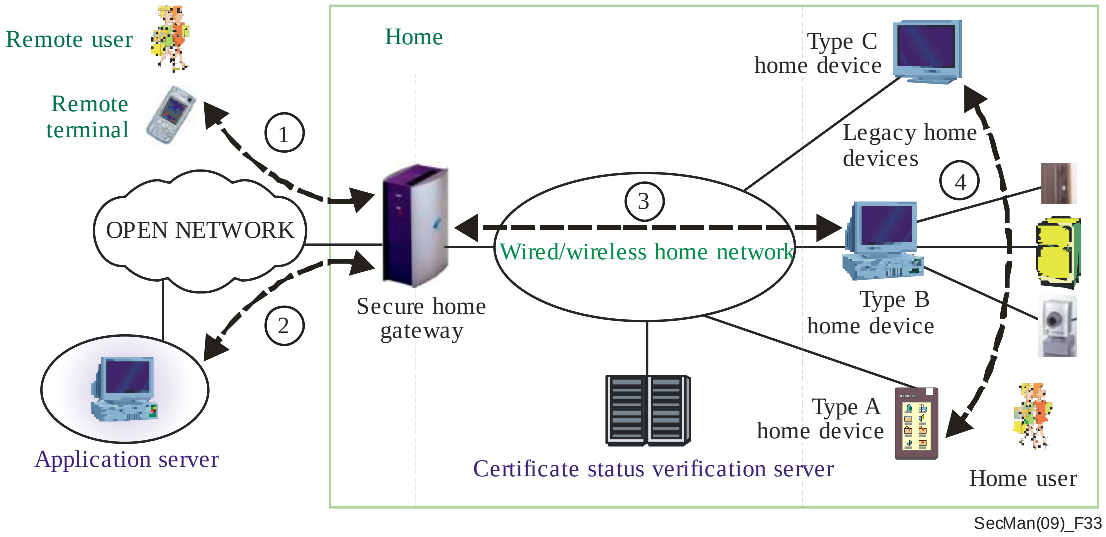


Figure 32 – Device authentication use case based on general home network model for security

For external Internet service from the home device to the 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.

8.3.3 Human user authentication for home network services

Some environments demand authentication of the human user rather than a process or a device. In these instances, the authentication system requires human users to prove their uniqueness. Such uniqueness is generally based on characteristics such as something known, something possessed, or some immutable characteristic of the user.

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 33 shows authentication service flows based on the general model of home network security defined in 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.

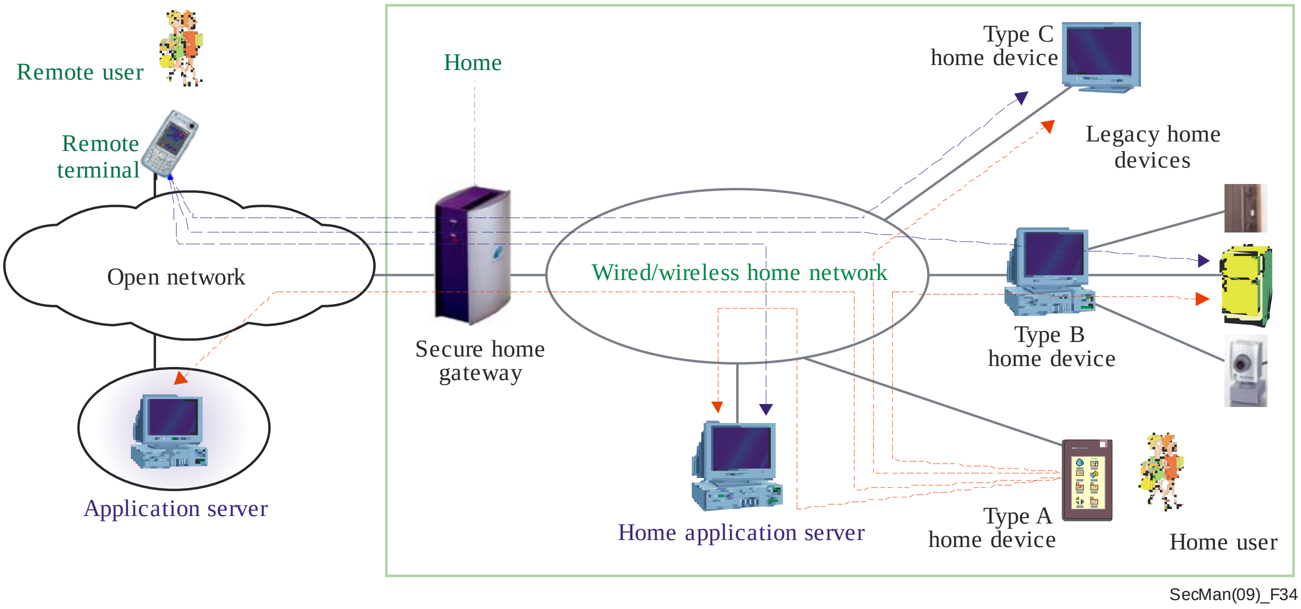


Figure 33 – Authentication service flows for the home network

8.4 IPCablecom

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.

8.4.1 IPCablecom Architecture

The IPCablecom architecture is defined in Recommendation ITU-T J.160. IPCablecom components are illustrated in Figure 34. 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.

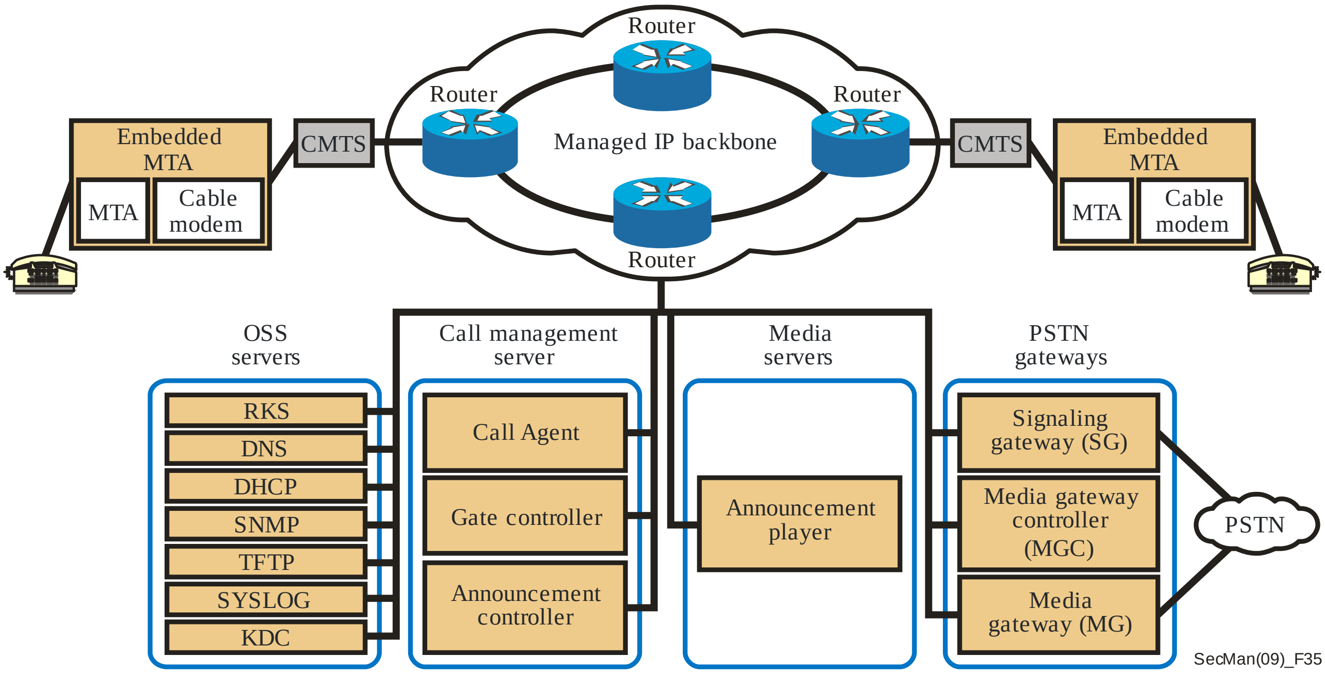


Figure 34 – IPCablecom component reference model

8.4.2 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, *IPCablecom security specification*. 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.

8.4.3 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, the underlying security mechanisms (such as IPsec) that provide the protocol interface with the security services it requires. In terms of the X.805 architecture, the overview of the security services for IPCablecom addresses all the nine cells resulting from the three planes and layers in Figure 1.

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.

8.5 IPCablecom2

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

8.5.1 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 production of technical specifications for GSM and third generation (3G) mobile system networks, and development of a SIP-based IP-communications architecture for mobile networks. The resulting architecture, the *IP multimedia subsystem*, forms the basis of the IPCablecom2 architecture defined in Rec. ITU-T J.360.

8.5.2 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
- leverage and extend the IMS security 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. Trust domains can be demarcated by physical or logical boundaries. Communication across trust domains must always be protected with authentication and authorization. In addition, the interfaces connecting network elements within a domain, the interfaces between domains, and the interfaces between UEs and the service provider must be secured against a variety of threats.

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.

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 media network traffic at its interfaces); and attacks using zombies (i.e., many compromised endpoint systems).

Signalling channel threats

In a multimedia environment, signalling messages include data pertaining to identity, services, routing and other sensitive and critical data. Multimedia components such as proxies exist in the access domain, exposing them to a greater number of 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.

8.5.3 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.

8.5.3.1 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.

8.5.3.2 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.

8.6 Security for ubiquitous sensor networks

A sensor is simply a device that generates an electrical signal that represents a measureable physical property. A ubiquitous sensor network (USN) is 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. Figure 35 illustrates potential USN applications.

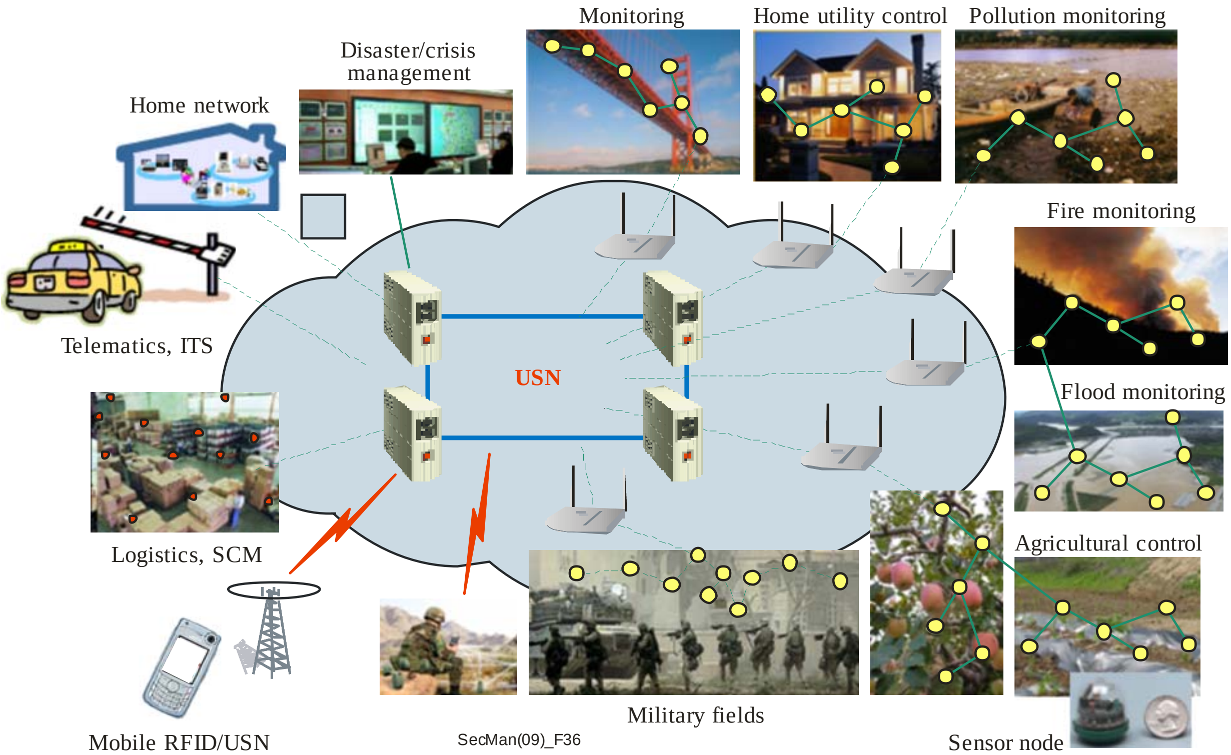


Figure 35 – Potential USN applications

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.

In addition to standard networking threats (such as those discussed in section 3) there are threats specific to USNs. These include:

- **sensor node compromise**, due to individual sensors being attacked or compromised or through an attacker introducing illicit sensors;

- **eavesdropping**, by monitoring transmissions between nodes;
- **compromise or exposure of sensed data**;
- **denial of service attacks** against the sensors or the communications; and
- **malicious use or misuse of network sensors**, e.g., using sensors for illegal purposes.

In addition, USNs are subject to a number of threats related to routing between the sensor nodes.

The characteristics of a sensor network greatly complicate the process of secure network design. For example, due to the limited computational power and memory of the sensor nodes and limited power and bandwidth, it is not feasible to use public-key cryptography or to store unique keys with the nodes. In addition, the sensors may be located in hostile environments and their exact location may not be known after deployment. Lastly, the sensor network is highly reliant on its base station, which is not only a potential single point of failure but a tempting target for would-be attackers.

USN middleware provides a common application platform to support various functions on behalf of USN applications and services and to control the sensor networks. The large amount of data collected by the sensor network is stored, managed and analysed by USN middleware which must also deliver data securely to the appropriate applications. Middleware security measures must address security of data in storage and during transmission as well as availability of the middleware.

Although no USN Recommendations have yet been finalized, work is well underway to address both the security needs of the USN itself as well as well as those of USN middleware.

9. Application security

9 Application security

With 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 inherent vulnerabilities. In addition, evolving threats frequently expose and exploit previously-unknown vulnerabilities.

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.

9.1 Voice over IP (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 may also include other forms of media, including video and data. VoIP also includes associated supplementary services such as conferencing (bridging), call forwarding, call waiting, multi-line, call diversion, park and pick-up, consultation, and "follow-me", among many other intelligent network services. Voice-over-Internet is a particular case of VoIP deployment, in which the voice traffic is carried over the public Internet backbone.

Recommendation ITU-T H.323, *Packet-based multimedia communications systems*, 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). These networks dominate today's corporate desktops and include packet-switched TCP/IP and Internet Packet Exchange (IPX) over Ethernet, Fast Ethernet and Token Ring network technologies. By complying with ITU-T H.323, multimedia products and applications from multiple vendors can interoperate, allowing users to communicate without concern for compatibility. 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, entertainment, and professional applications. Security specifications for the ITU-T H.323 series of Recommendations are contained in Recommendations ITU-T H.Imp235, *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.235.x, a series of nine security frameworks and standards, and ITU-T H.530, *Symmetric security procedures for H.323 mobility in ITU-T H.510*. Mobility for ITU-T H.323 multimedia systems and services is addressed in Rec. ITU-T H.510.

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

Rec. ITU-T H.323 defines four major components for a network-based communications system: terminals, gateways, gatekeepers, and multipoint control units. Additionally, border or peer elements are also possible. These elements are illustrated in Figure 36.

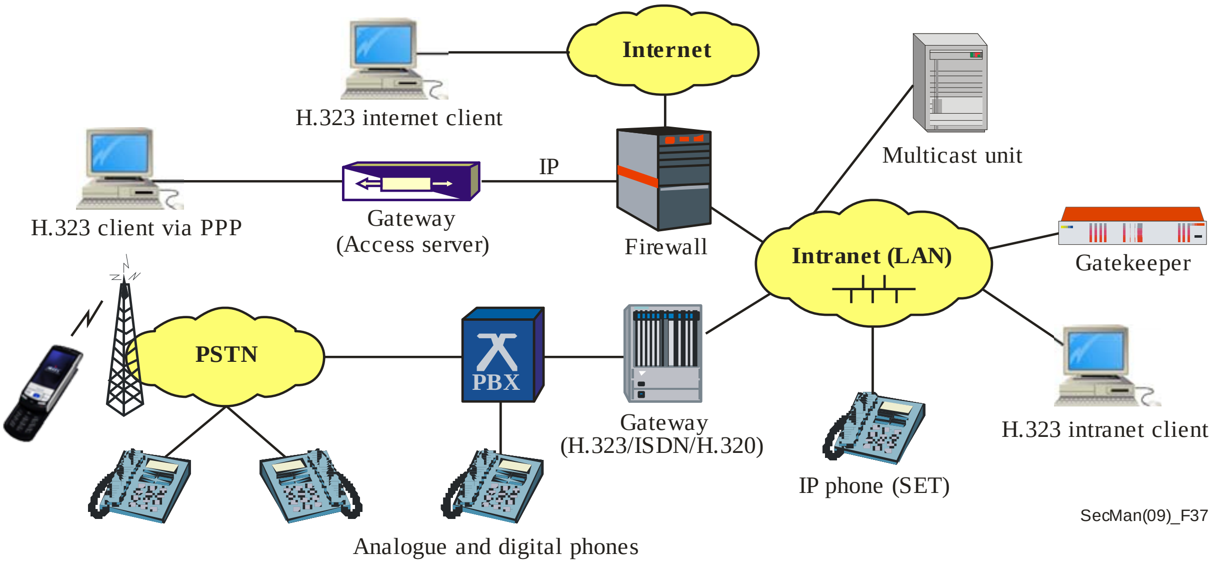


Figure 36 – H.323 system: components and deployment scenarios

Examples of where ITU-T H.323 is used include wholesale transit by operators, especially for VoIP backbones and calling card services. In corporate communications, ITU-T H.323 is used for IP-PBX, IP-centrex, voice VPN, integrated voice and data systems, Wi-Fi phones, implementation of call centres, and mobility services. For professional communications, it is widely used for voice (or audio) and videoconferencing, for voice/data/video collaboration, and distance learning. In a residential environment, uses include broadband audiovisual access, PC-to-phone, phone-to-PC, and PC-to-PC calling; it could also be used for delivery of custom news and information.

9.1.1 Security issues in multimedia and VoIP

As all the elements of an 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 37.

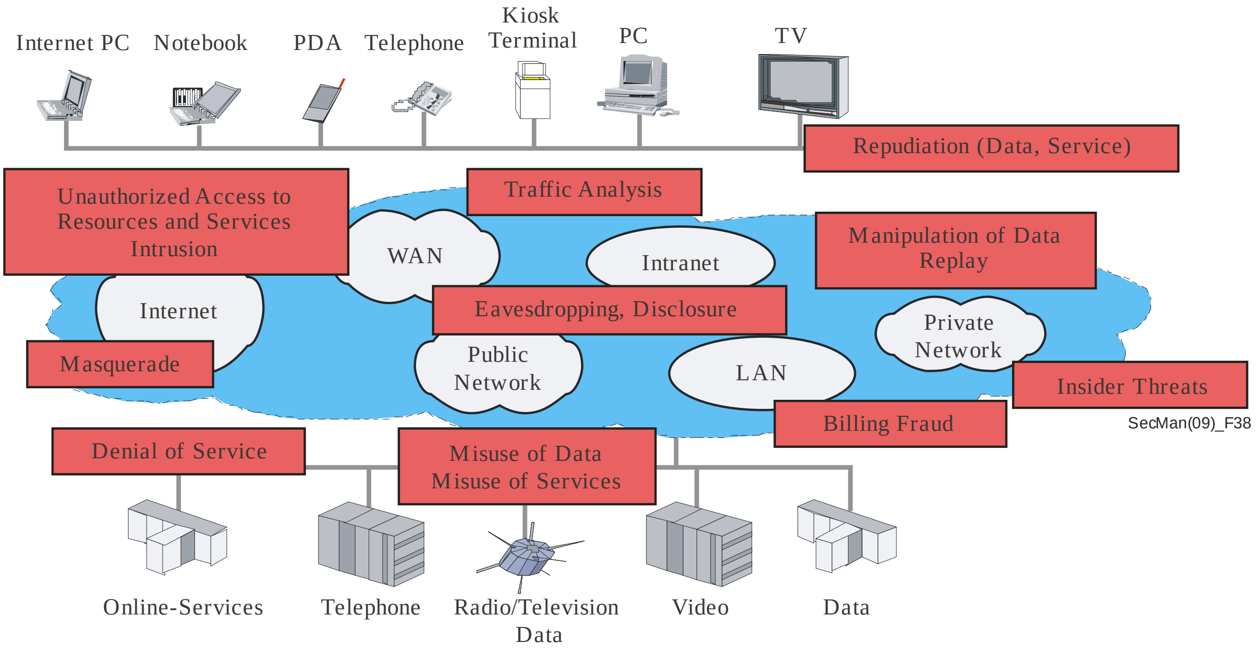


Figure 37 – Security threats in multimedia communications

The main security issues in 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 (gatekeepers, multicast units, gateways), users need to know if they are talking with the proper server and/or with the correct service provider. This applies to both fixed and mobile users.
- 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 (QoS, bandwidth, codec, etc.). 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 confidentiality: This is realized through encryption of the voice packets and protects against eavesdropping. In general, the media packets (e.g., video) of multimedia applications are encrypted

as well as voice data. Advanced protection of media packets also includes authentication/integrity protection of the payloads.

- Key management: This includes not only all tasks that are necessary for securely distributing keying material to users and servers, but also tasks like updating expired keys and replacing lost keys. Key management 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.
- 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 ITU-T H.323 security. Security issues that are considered outside the scope of ITU-T H.323 include security policy, network management security, security provisioning, implementation security, operational security and security incident handling.

9.1.2 An overview of H.235.x subseries Recommendations

The H.235.x series of Recommendations comprise eleven standards plus one implementor's guide that together 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.

ITU-T H.235 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.

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

Figure 38 shows the scope of ITU-T H.235, which encompasses provisions for setting up calls (ITU-T H.225.0 and ITU-T H.245 blocks) and bidirectional communication (encryption of RTP payloads containing compressed audio and/or video). The functionalities include mechanisms for authentication, integrity, privacy, and non-repudiation. 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, but is commonly implemented using the IP security (IPSec) and transport layer security (TLS) protocols. Where required by end system policy, IPSec or TLS can be used to provide authentication and, optionally, confidentiality at the IP layer transparent to whatever (application) protocol runs above.

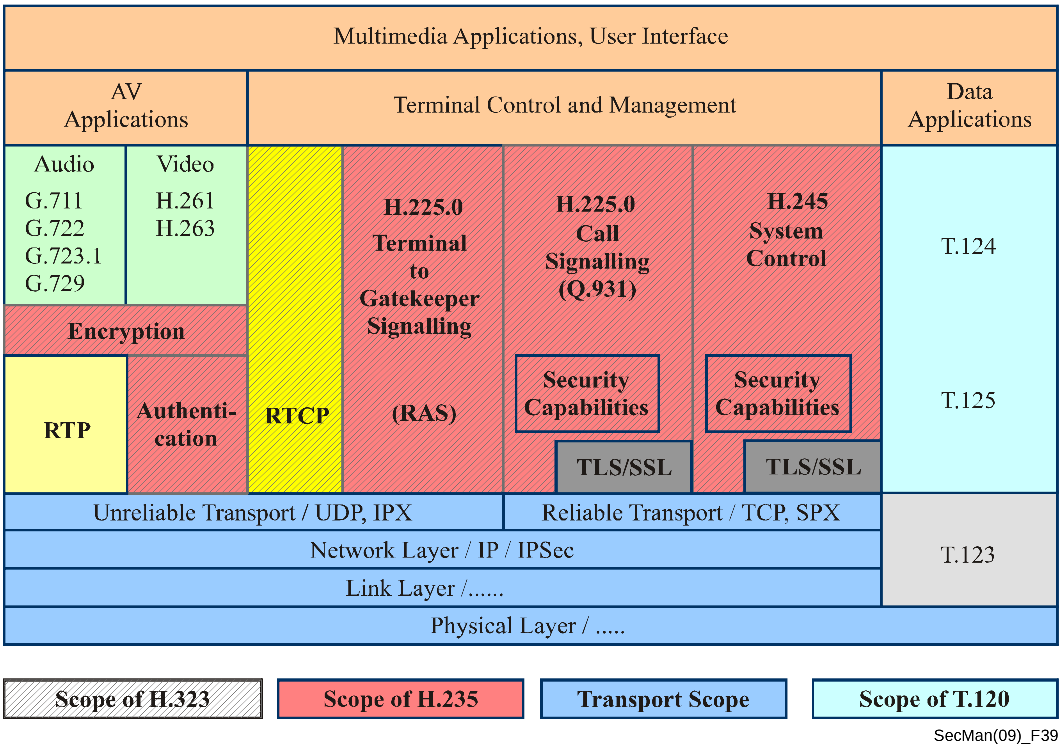


Figure 38 – Security in ITU-T H.323 as provided by ITU-T H.235

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 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. ITU-T H.235.3 is called the hybrid security profile as this Recommendation combines symmetric security procedures from ITU-T H.235.1 and PKI-based certificates and signatures from ITU-T H.235.2 thereby achieving optimized performance and shorter call-set time. ITU-T H.235.4 loosens the strict dependency on a gatekeeper-routed, server-centric architecture and 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, 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. Rec. ITU-T H.235.6, *Voice encryption profile with native H.235/H.245 key management*, collects all the procedures that are necessary to achieve encryption of the RTP media stream including the surrounding key management that is entirely expressed within ITU-T H.245 signalling fields.

Secure user and terminal mobility in distributed ITU-T H.323 environments is covered in Rec. ITU-T H.530, *Symmetric security procedures for ITU-T H.323 mobility in ITU-T H.510*, 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 signaling data between a mobile terminal and visited domain.

Rec. ITU-T H.235.0 provides the overall security framework for H-series multimedia systems. 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 ITU-T H.323, SIP, ITU-T H.320 and generic messaging services into a directory service, so that modern identity management practices can be applied to multimedia communications.

9.1.3 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 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 ITU-T H.323 traffic from external devices to pass through to reach internal ITU-T H.323 devices, communication is simply not possible. This poses a problem for any user of 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. 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 three of the ITU-T H.460 series of Recommendations that allow ITU-T H.323 communications to seamlessly traverse one or more NAT/FW devices. Those Recommendations are: ITU-T H.460.17, *Using H.225.0 call signalling connection as transport for H.323 RAS messages*; ITU-T H.460.18, *Traversal of H.323 signalling across network address translators and firewalls*; and ITU-T H.460.19, *Traversal of H.323 media across network address translators and firewalls.*

Figure 39 depicts how a special "proxy" device might be used to aid NAT/FW "unaware" devices to properly traverse the NAT/FW boundary.

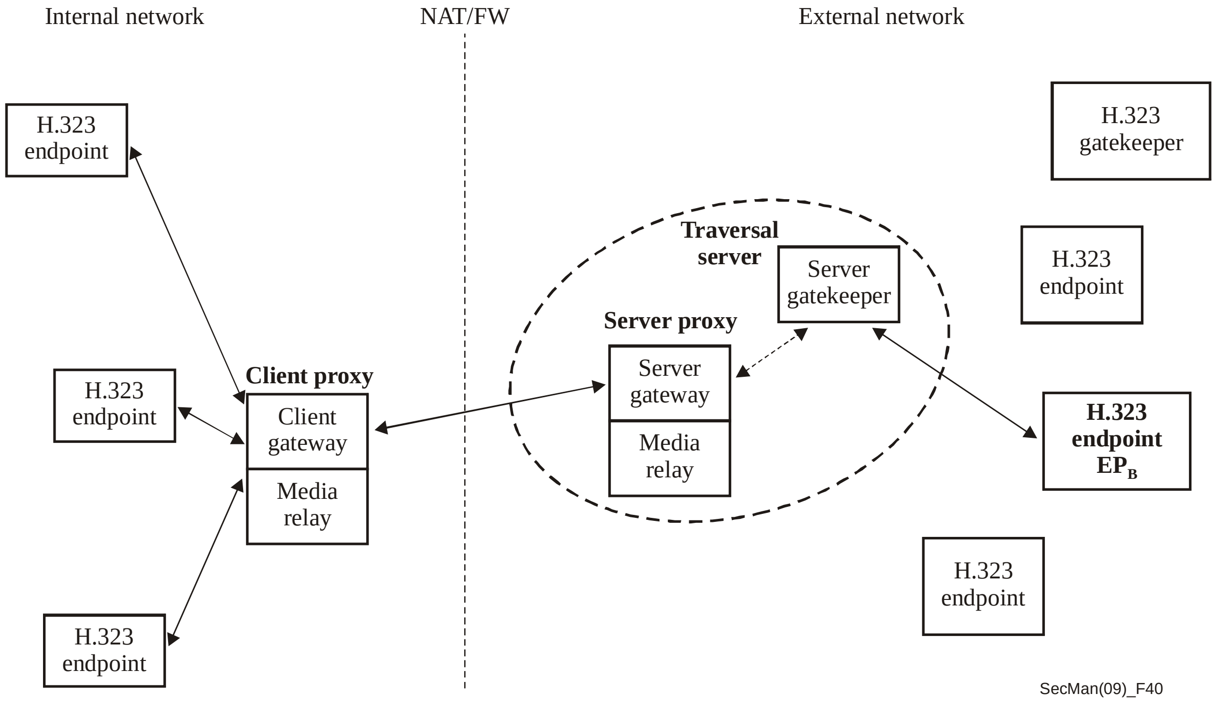


Figure 39 – NAT/FW traversal in H.460.18 architecture

The above topology may be used, for example, where an enterprise wishes to control the route along which ITU-T H.323 call signalling and media flows through the network. However, ITU-T H.460.17 and ITU-T H.460.18 also allow endpoints to traverse NAT/FW boundaries without the aid of any special internal "proxy" devices. Figure 40 depicts one such topology:

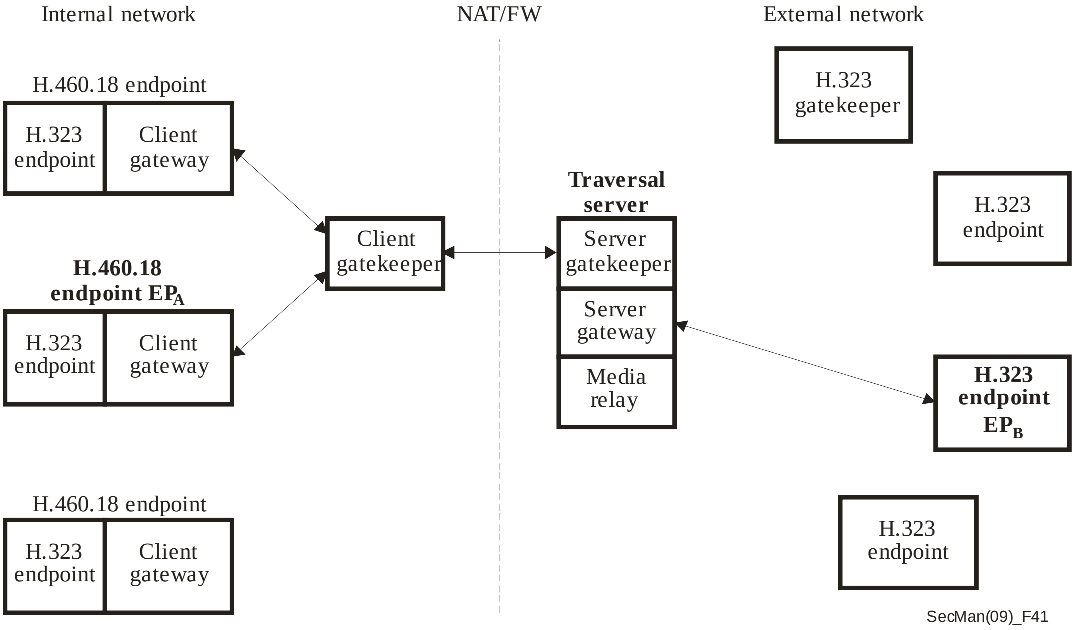


Figure 40 – Gatekeeper communication architecture

In Figure 40, 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 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 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.

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 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.

9.2 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 only acquire a service and the content which they are entitled to receive. It also includes protecting the service against unauthorized access.

A number of IPTV-specific security Recommendations are in preparation and one, Rec. ITU-T X.1191, *Functional requirements and architecture for IPTV security aspects*, has been approved. The general security architecture for IPTV defined in this Recommendation is shown in Figure 41. 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.

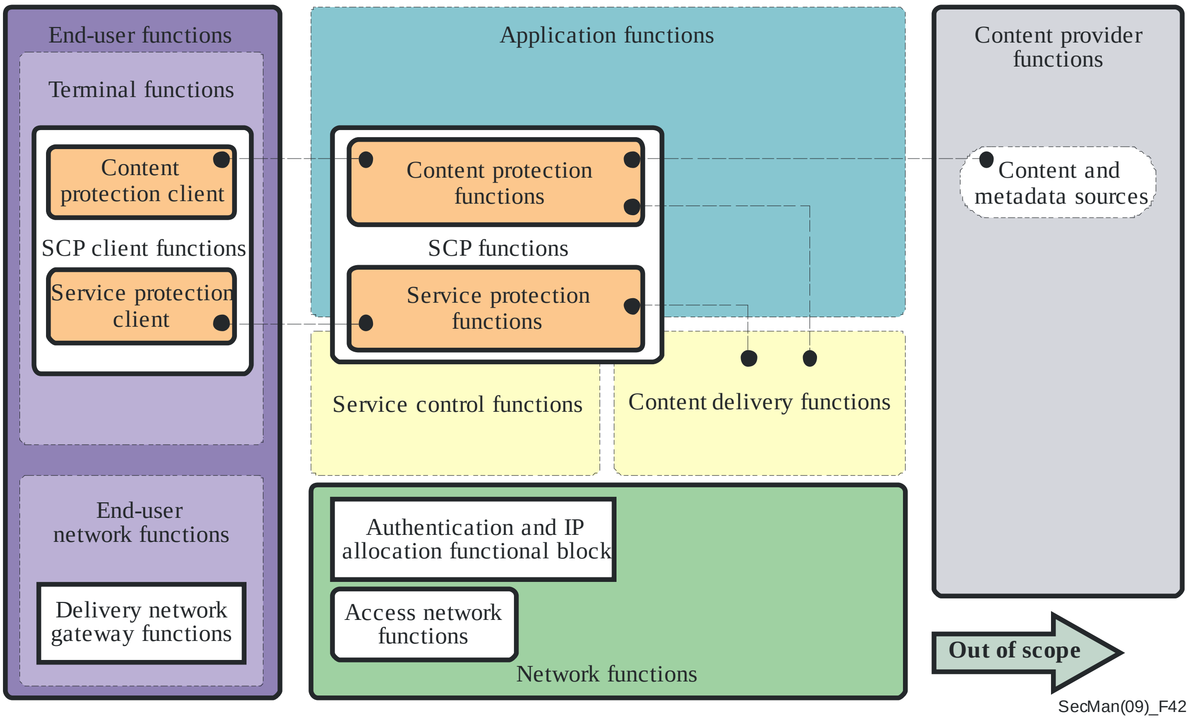

End-user functions
Terminal functions
Content protection client
SCP client functions
Service protection client
End-user network functions
Delivery network gateway functions
Application functions
Content protection functions
SCP functions
Service protection functions
Service control functions
Content delivery functions
Authentication and IP allocation functional block
Access network functions
Network functions
Content provider functions
Content and metadata sources
Out of scope
SecMan(09)_F42

Figure 41 – General security architecture for IPTV

9.2.1 Mechanisms for protecting IPTV content

Security mechanisms that can be used to protect content include:

- content encryption;
- watermarking (i.e., 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;
- 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).

9.2.2 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).

9.2.3 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 ITU-T X.1191.

9.3 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 (Rec. ITU-T T.4) and then for ISDN (Rec. ITU-T T.563). More recently, extensions were specified for fax transmission in real time over IP networks (including the Internet) (Rec. ITU-T T.38) and via store-and-forward systems (Rec. 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 Rec. ITU-T T.36, *Security capabilities for use with Group 3 facsimile terminals*, 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.

9.4 Web services

Web technologies including service-oriented architectures (SOA) are being widely applied as they enable developers to develop and deploy new services efficiently and cost-effectively, and to integrate content from a variety of sources to form composite services easily and rapidly. There are many security aspects of web services. Mechanisms for authentication and single sign-on (SSO) are important and, since web services are being applied to mobile networks, it is also important to consider the security mechanisms needed for 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 the information systems department, by human resources, by the legal department and by the finance department. The policy may be enforced via the extranet, mail, WAN and remote-access systems – platforms that inherently implement a permissive security policy. The current practice is to manage the configuration of each point of enforcement independently in order to implement the security policy as accurately as possible. Consequently, it is an expensive and unreliable proposition to modify the security policy. It is also difficult (perhaps even impossible) to obtain a consolidated view of the safeguards in effect throughout the enterprise to enforce the policy. At the same time, there is increasing pressure on corporate and government executives from consumers, shareholders and regulators to demonstrate "best practice" in the protection of the information assets of the enterprise and its customers.

For these reasons, a common language is needed for expressing security policy. If implemented throughout an enterprise, a common policy language allows the enterprise to manage the enforcement of all the 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.

9.4.1 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.

SAML assertions are usually made about a *subject*. 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*.

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.

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 is defined to support single sign-on (SSO) of browsers and other client devices. Figure 42 illustrates the basic template for achieving SSO.

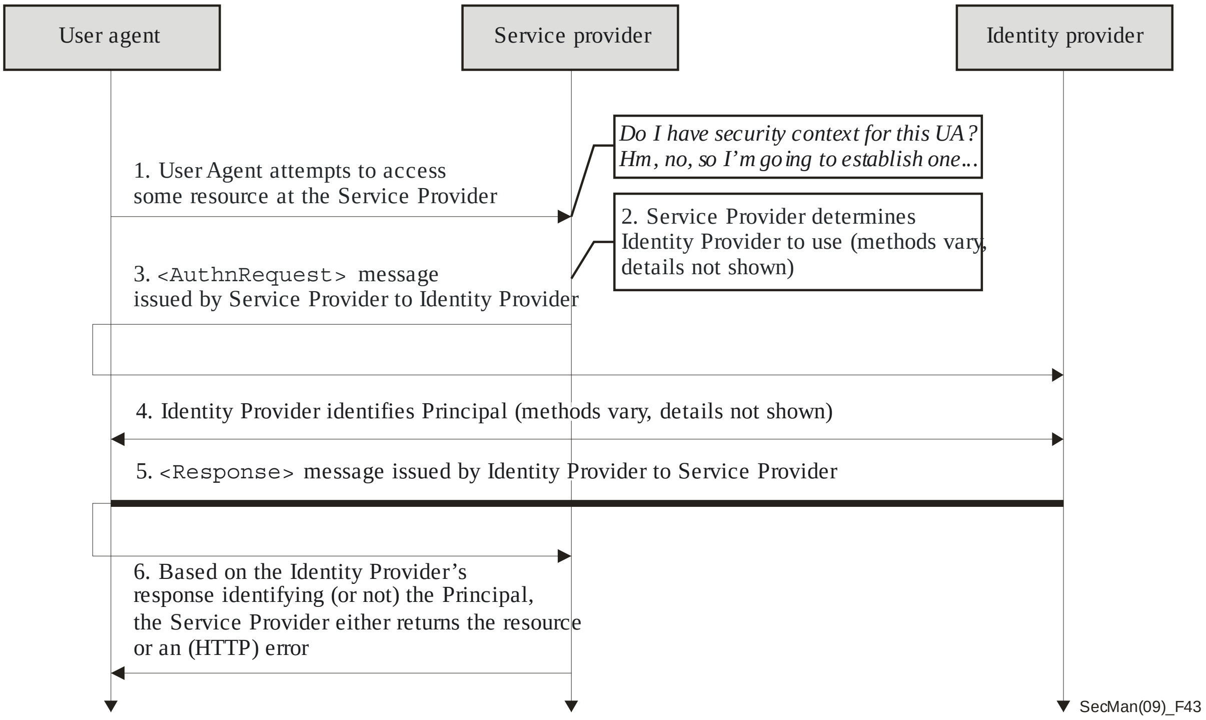

User agent
Service provider
Identity provider
Do I have security context for this UA? Hm, no, so I'm going to establish one...
1. User Agent attempts to access some resource at the Service Provider
2. Service Provider determines Identity Provider to use (methods vary, details not shown)
3. <AuthnRequest> 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(09)_F43

Figure 42 – Basic template for achieving SSO

9.4.2 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 a requested resource access should be allowed and enforcing that decision. Recommendation ITU-T X.1142 defines core XACML including syntax of the language, models, context with policy language model, syntax and processing rules. To improve on the security of exchanging XACML-based policies, ITU-T X.1142 also specifies 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.

9.5 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, *Threats and requirements for protection of personally identifiable information in applications using tag-based identification*, 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 defines the basic structure of 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 the information content delivery service, the customer retrieves the information by using the reader device he/she owns. In this type of service, most application service providers may assume that the customer has a mobile terminal equipped with a reader device. Figure 43 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 the directory service and then performs content retrieval.

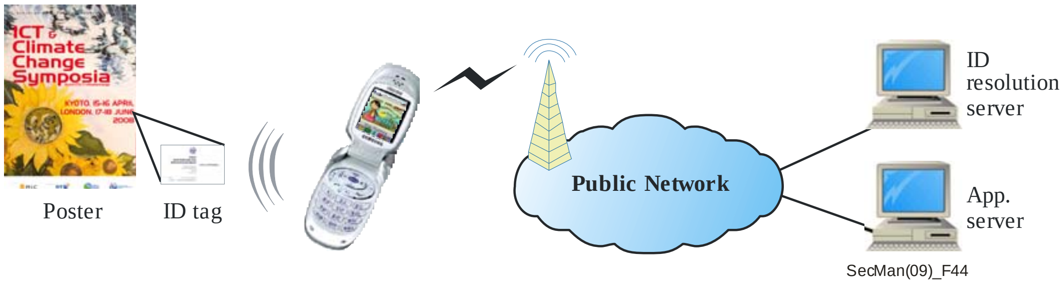


Figure 43 – Basic model of a B2C application using tag-based identification

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 are of the fixed terminal type and/or mobile terminal type. The customer may not need his/her own reader device.

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 upon purchasing the tagged product after browsing the product information contents from his/her mobile terminal. In another example, a healthcare-related service triggered 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, the attacker can 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.
- 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 may 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 to 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.
- *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 44 illustrates the general PPS service flow of the application using tag-based identification.

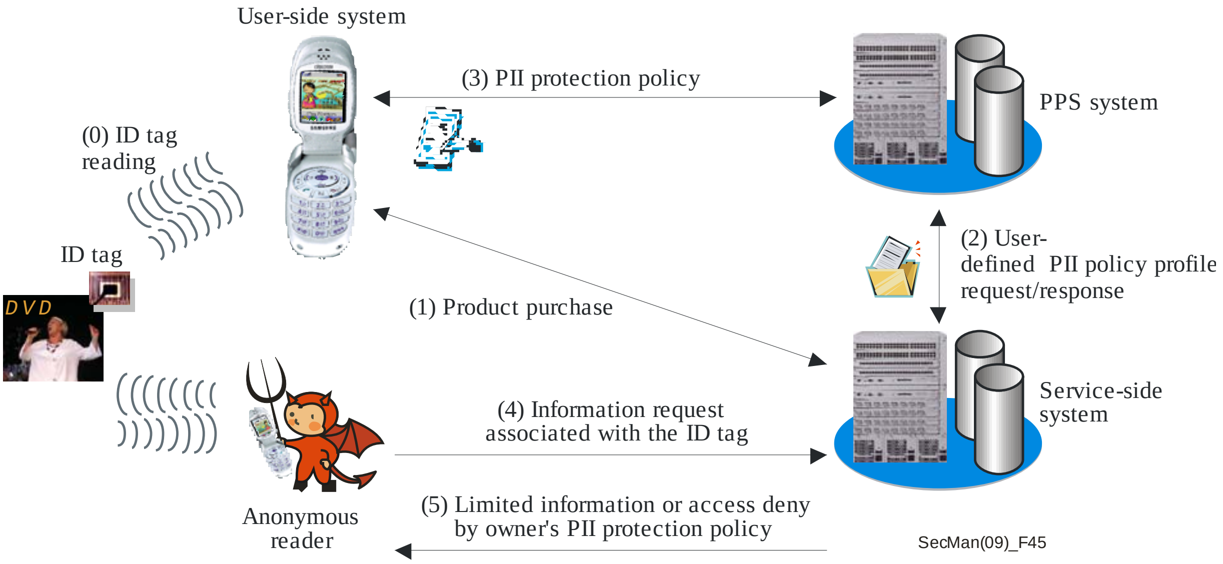


Figure 44 – General PII protection service (PPS) service flow

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 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.

10. Countering common network threats

10 Countering common network threats

Threats to computer systems and to the networks that link them 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.

10.1 Countering spam

Spam (i.e., unsolicited, unwanted e-mail) is widely recognized as a major problem for network users and network and service providers. Spam interferes with legitimate operations, consumes bandwidth and processing cycles and, in extreme cases, can result in denial of service attacks by flooding networks. Both legal and technical measures are being used to counter spam with varying degrees of effectiveness. 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, including spam filtering; international cooperation; and education of users and Internet service providers.

The ITU-T work on countering spam focuses primarily on the technical aspects of the problem so, in this section, we focus on technical means for countering spam and the development and application of anti-spam technologies.

10.1.1 Technical strategies on countering spam

Recommendation ITU-T X.1231, *Technical strategies on countering spam*, 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 45. 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.

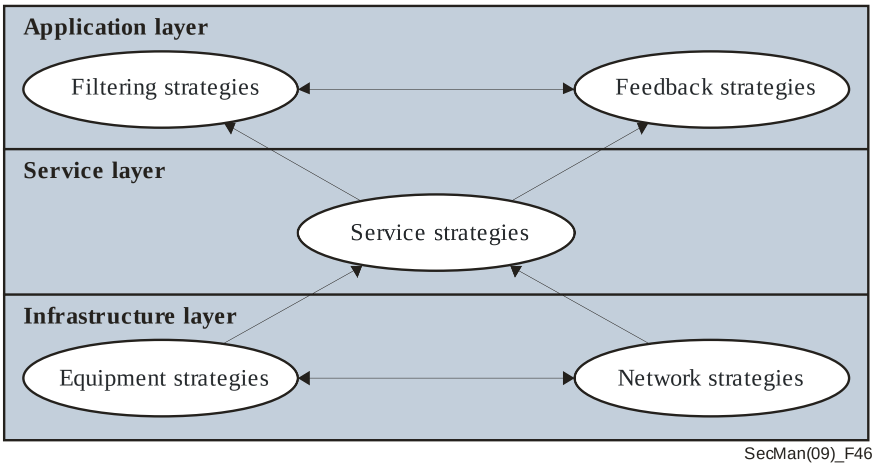


Figure 45 – General model for countering spam

10.1.2 Email spam

The most widely recognized form of spam is email 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 email 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. ITU-T X.1240, *Technologies involved in countering email spam*, is directed towards users who want to develop technical solutions for countering email spam. It specifies basic concepts, characteristics, effects, and the technical issues associated with countering email spam. It also identifies current technical solutions and related activities from standards development organizations and other groups that are working on countering email spam.

Recommendation ITU-T X.1241, *Technical framework for countering e-mail spam*, 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 email spam between different email 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, the *ITU-T X.1240 series – Supplement on countering spam and associated threats* reviews international fora where spam is being addressed and includes a case study.

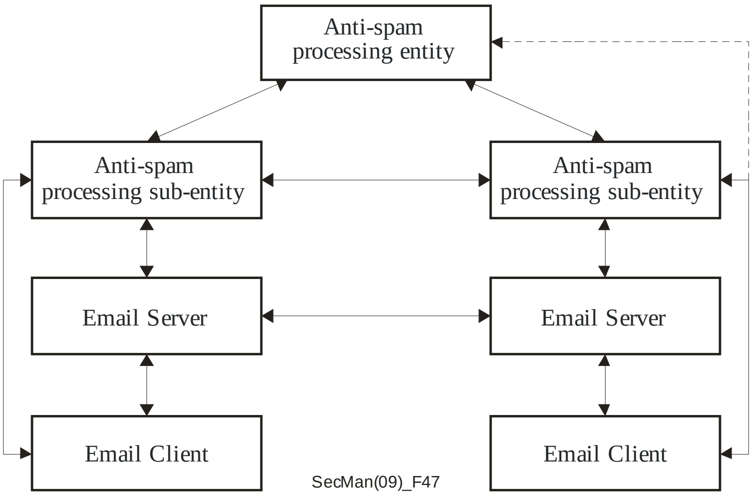

Anti-spam processing entity
Anti-spam processing sub-entity
Anti-spam processing sub-entity
Email Server
Email Server
Email Client
Email Client
SecMan(09)_F47

Figure 46 – General structure of e-mail anti-spam processing domain

Figure 46 illustrates the processes of the ITU-T X.1241 framework. The anti-spam processing entity is located in an independent system while the anti-spam processing 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.

10.1.3 IP multimedia spam

Recommendation ITU-T X.1244, *Overall aspects of countering spam in IP-based multimedia applications*, 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 email spam can also be used in countering IP multimedia application spam. 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 7 shows the classification used in ITU-T X.1244.

Table 7 – Classification of IP multimedia application spam

	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

10.1.4 Short message service (SMS) spam

Recommendation ITU-T X.1242, *Short message service (SMS) spam filtering system based on user-specified rules*, 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 ITU-T X.1242.

10.2 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 (i.e., software that performs unauthorized activities) also pose significant risk. Unless organizations and individuals implement a range of proactive measures (including 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.

Recommendation ITU-T X.1207, *Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software,* 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.

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.

10.3 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, *A vendor-neutral framework for automatic notification of security related information and dissemination of updates*, discusses the difficulties associated with maintaining up-to-date software and provides a vendor-neutral way of addressing the problems. Once an asset is registered, updates on vulnerability information and patches or updates can be automatically made available to users or directly to applications. 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.

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 ITU-T X.1206 together with the format of the information that should be used in and between components implementing this framework.

11. The future of ICT security standardization

11 The future of ICT security standardization

For more than 30 years, the ITU-T has been engaged in the development of ICT standards. This work 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.

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 detail 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.

Looking towards the future, telecommunications networks and computer networks will continue to converge. Next Generation Networks and web-based services will continue to grow rapidly and will become increasingly important, but threats will continue to evolve and it will remain an on-going challenge to design and develop 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.

The 191 Member States and over 551 Sector Members 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 at the 2008 World Telecommunication Standardization Assembly. Wherever possible, to minimize duplication of effort and focus on resources, ITU-T will collaborate with other standards development organizations to achieve harmonized solutions as efficiently and expeditiously as possible.

12. Sources of additional information

12 Sources of additional information

This manual presents a broad overview of the ITU-T security work together. Much more detailed information, including many of the standards, is freely available via the ITU-T web site.

12.1 Overview of SG 17 work

As a first step, the SG 17 home page provides links to information about the SG 17 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.

12.2 The Security Compendium

The Compendium contains information on ITU Recommendations, related information and ITU security activities. It consists of five parts, each of which is downloadable:

- a catalogue of the approved Recommendations related to telecommunication security, which includes those designed for security purposes and those which describe or use of functions of security interest and need;
- a list of ITU-T approved security definitions extracted from approved ITU-T Recommendations;
- a summary of ITU-T Study Groups with security-related activities;
- a summary of Recommendations within ITU-T Study Groups under review for security considerations;
- a summary of other ITU security activities.

12.3 The Security Standards Roadmap

The 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 information about the ITU-T security work, the Roadmap includes information on the security standards work of ISO/IEC, ATIS, ENISA, ETSI, IEEE, IETF, OASIS, 3GPP, and 3GPP2.

Like the Compendium, the Roadmap is in five parts and most 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;
- Part 3, *Security standards under development*;
- Part 4, *Future needs and proposed new security standards*; and
- Part 5: *Security best practices*.

12.4 Implementation guidelines for security

Supplement 3 to the ITU-T X.800-X.849 series of Recommendations, *Supplement on guidelines for implementing system and network security*, 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.

12.5 Additional information on the Directory, authentication and identity management

For more information on ITU-T X.500-series Recommendations, the authorized source of information is the ITU-T X.500-series of Recommendations itself. Additional tutorial information and an Implementor's Guide may be found at www.x500standard.com. The following links contain additional information:

http://www.x500standard.com/index.php?n=X509.X509ProtectingDirectory has information about user authentication;

http://www.x500standard.com/index.php?n=X500.AccessControl gives more information on access control; and

http://www.x500standard.com/index.php?n=X500.DataPrivacyProtection provides a more extensive description of the X.500 data privacy features.

Annex A – Security definitions

Annex A
Security definitions

The following table contains definitions for terms used in the manual. All definitions are contained in current ITU-T Recommendations. A more complete list of security definitions is contained in the compendium of ITU-T approved security definitions extracted from ITU-T Recommendations 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.	X.800 J.170
access control list	A list of entities, together with their access rights, which are authorized to have access to a resource.	X.800
access control policy	The set of rules that define the conditions under which an access may take place.	X.812
accidental threats	Threats that exist with no premeditated intent. Examples of realized accidental threats include system malfunctions, operational blunders and software bugs.	X.800
accountability	The property that ensures that the actions of an entity may be traced uniquely to the entity.	X.800
algorithm	A mathematical process which can be used for the scrambling and descrambling of a data stream.	J.93
attack	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.	H.235
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).	X.400
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.	X.509 X.842
attribute certificate	A data structure, digitally signed by an Attribute Authority, that binds some attribute values with identification information about its holder.	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.	X.811

Term	Definition	Reference
	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 Rec. 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.	X.811 X.800 X.217 J.170 J.93
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.	X.800 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 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).	M.3016.2
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.	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.	X.800 H.235 J.170
availability	The property of being accessible and useable upon demand by an authorized entity.	X.800
capability	A token used as an identifier for a resource such that possession of the token confers access rights for the resource.	X.800
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.	H.235

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.	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.	X.509 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.	X.509 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.	X.800
cleartext	Intelligible data, the semantic content of which is available.	X.800
confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.	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.	M.3016.2
credentials	Data that is transferred to establish the claimed identity of an entity.	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. 3. The science of recovering the plaintext of a message without access to the key (to the electronic key in electronic cryptographic systems).	X.800 J.170 J.93
cryptographic algorithm	Mathematical function that computes a result from one or several input values.	H.235
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.	X.509 Q.815

Term	Definition	Reference
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.	X.800
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.	X.509
data integrity	The property that data has not been altered or destroyed in an unauthorized manner.	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.	X.800 X.811
decipherment	The reversal of a corresponding reversible encipherment.	X.800
decryption	See decipherment.	X.800
delegation	Conveyance of privilege from one entity that holds such privilege, to another entity.	X.509
denial of service	The prevention of authorized access to resources or the delaying of time-critical operations.	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.	X.800 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 X.500.	X.843
eavesdropping	A breach of confidentiality by monitoring communication.	M.3016.0
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.	X.800 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)	J.170 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.	X.800

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.	X.842 X.902
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.	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.	X.813
forgery	An entity fabricates information and claims that such information was received from another entity or sent to another entity.	M.3016.0
hash function	A (mathematical) function that maps values from a (possibly very) large set of values into a smaller range of values.	X.810
indirect attack	An attack on a system which is not based on the deficiencies of a particular security mechanism (e.g. attacks which bypass the mechanism, or attacks which depend on the system using the mechanism incorrectly).	X.814
integrity	The property that data has not been altered in an unauthorized manner. (See also data integrity)	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.	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".	X.800
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.	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.	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.	X.800 J.170
key exchange	The swapping of public keys between entities to be used to encrypt communication between the entities.	J.170

Term	Definition	Reference
key management	The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.	X.800
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.	X.1151
masquerade	The pretence by an entity to be a different entity.	X.800
mutual authentication	The assurance of the identities of both principals.	X.811
non-repudiation	1. The ability to prevent a sender from denying later that he or she sent a message or performed an action. 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.	J.170 H.235 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.	X.800
passive threat	The threat of unauthorized disclosure of information without changing the state of the system.	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.	X.800 H.530
physical security	The measures used to provide physical protection of resources against deliberate and accidental threats.	X.800
principal	An entity whose identity can be authenticated.	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.	X.800 H.235
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.	X.509 X.810 J.170
privilege	An attribute or property assigned to an entity by an authority.	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.	X.509

Term	Definition	Reference
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.	X.509 X.810 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.	X.509 H.235 J.170
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.	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.	X.509
relying party	A user or agent that relies on the data in a certificate in making decisions.	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).	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.	X.800 M.3016.0 X.402
revocation list certificate	A security certificate that identifies a list of security certificates that have been revoked.	X.810
secret key	A key that is used with a symmetric cryptographic algorithm. Possession of a secret key is restricted (usually to two entities).	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.	X.800

Term	Definition	Reference
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.	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.	X.800
security audit trail	Data collected and potentially used to facilitate a security audit.	X.800
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.	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.	X.841 X.411
security information (SI)	Information needed to implement security services.	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.	M.3016.0
security model	A framework for describing the security services that counter potential threats to the MTS and the security elements that support those services.	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.	X.509 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.	X.800
security threat (threat)	A potential violation of security	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.	X.810
sensitivity	Characteristic of a resource that implies its value or importance.	X.509
shared secret	Refers to the security key for the cryptographic algorithms; it may be derived from a password.	H.530
signature	See digital signature.	X.800
simple authentication	Authentication by means of simple password arrangements.	X.509
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.	X.509
spam	Unsolicited and unwanted e-mail	H.235
spoofing	Impersonating a legitimate resource or user	X.509

Term	Definition	Reference
strong authentication	Authentication by means of cryptographically derived credentials.	X.811
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.	
threat	A potential violation of security.	X.800
token	See security token	
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.	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.	X.810
trusted functionality	Functionality perceived to be correct with respect to some criteria, e.g., as established by a security policy.	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).	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.	M.3016.0
user authentication	Establishing proof of the identity of the human user or application process.	M.3016.0
verifier	An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.	X.811
vulnerability	Any weakness that could be exploited to violate a system or the information it contains.	X.800
ITU-T X.509 certificate	A public-key certificate specification developed as part of the ITU-T X.500 standards directory.	J.170

Annex B – Acronyms and abbreviations used in this manual

Annex B
Acronyms and abbreviations used in this manual

Acronym	Meaning
ACI	Access Control Information
AES	Advanced Encryption Standard Algorithm
ASN.1	Abstract Syntax Notation One
ASP	Application Service Provider
ATIS	Alliance for Telecommunications Industry Solutions
A/V	Audiovisual
BioAPI	Biometric Application Program/programming Interface
BPON	Broadband Passive Optical Network
B2C	Business-to-Customer
CA	Certification Authority. A trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates.
CDMA	Code Division Multiple Access
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DNS	Domain Name Server/System/Service
DSL	Digital Subscriber Loop
EAP	Extensible Authentication Protocol
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
FMC	Fixed Mobile Convergence
FW	Firewall
GK	Gatekeeper
GPRS	General Packet Radio System
GSM	Global System for Mobile communications
GW	Gateway
HFX	Hawthorne Facsimile Cipher

Acronym	Meaning
HKM	Hawthorne Key Management algorithm
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
ID	Identifier
IdM	Identity Management
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
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
IP	Internet Protocol
IPSec	Internet Protocol Security
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)
MIS	Management Information System
MTA	Message Transfer Agent (In messaging) Media Terminal adapter (In cable technology)
MWSSG	Mobile Web Services Security Gateway
NAT	Network Address Translation
NGN	Next Generation Network
OASIS	Organization for the Advancement of Structured Information Standards
OMG	Object Management Group
OSI	Open Systems Interconnection
P2P	Peer-to-peer
PC	Personal Computer

Acronym	Meaning
PDA	Personal Data Assistant
PIN	Personal Identification Number
PII	Personally Identifiable Information
PKI	Public-key Infrastructure
PKINIT	Public-key Cryptography Initial Authentication
PMI	Privilege Management Infrastructure
PSS	PII Protection Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RBAC	Role-Based Access Control
RFID	Radio Frequency Identification
RSA	Rivest, Shamir and Adleman (public-key algorithm)
RTP	Real time protocol
SAML	Security Assertion Markup Language
SG	Study Group
SHA1	Secure Hash Algorithm 1
SIP	Session Initiation Protocol. An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SoA	Source of Authority
SOA	Service Oriented Architecture
SPAK	Secure Password-based Authentication protocol with Key exchange
SSL	Secure Socket Layer
SSO	Single Sign-On
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TMN	Telecommunication Management Network
UE	User Equipment
UICC	Universal Integrated Circuit Card
USN	Ubiquitous Sensor Network
VoIP	Voice over IP
VPN	Virtual Private Network

Acronym	Meaning
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity (trademark of the Wi-Fi Alliance for certified products based on the IEEE 802.11 standards)
WTSA	World Telecommunication Standardization Assembly
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language
3G	3rd Generation
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2

Annex C – Summary of security-related ITU-T Study Groups

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 SG 17, which has security as its primary focus, has been designated the Lead Study Group on security. Table 8 summarizes the Study Groups' roles with security-related responsibilities and lists their respective Lead Study Group responsibilities.

Table 8 – Study Groups with security-related responsibilities

Study Group	Title	Responsibilities/Security role
SG 2	Operational aspects of service provision and telecommunications management	Lead Study Group for service definition, numbering and routing Lead Study Group on telecommunications for disaster relief/early warning Lead Study Group on telecommunication management
SG 5	Environment and climate change	Lead Study Group on electromagnetic compatibility and electromagnetic effects Lead Study Group on ICTs and climate change
SG 9	Television and sound transmission and integrated broadband cable networks	Lead Study Group on integrated broadband cable and television networks
SG 11	Signalling requirements, protocols and test specifications	Lead Study Group on signalling and protocols Lead Study Group on intelligent networks Lead Study Group on test specifications
SG 12	Performance, QoS and QoE	Lead Study Group on quality of service and quality of experience
SG 13	Future networks including mobile and NGN	Lead Study Group for future networks and NGN Lead Study Group on mobility management and fixed-mobile convergence
SG 15	Optical transport networks and access network infrastructures	Lead Study Group on access network transport Lead Study Group on optical technology Lead Study Group on optical transport networks
SG 16	Multimedia coding, systems and applications	Lead Study Group on multimedia coding, systems and applications Lead Study Group on ubiquitous applications ("e-everything", such as e-health) Lead Study Group on telecommunication/ICT accessibility for persons with disabilities
SG 17	Security	Lead Study Group on telecommunication security Lead Study Group on identity management Lead Study Group on languages and description techniques

Annex D – Security Recommendations referenced in this manual

Annex D
Security Recommendations 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: www.itu.int/rec/T-REC/en. ITU-T security-related Recommendations are available via Part 2 (Database) of the Security Standards Roadmap (www.itu.int/ITU-T/studygroups/com17/ict/index.html).

Recommendation	Title	Equivalent text
E.408	Telecommunication networks security requirements	
E.409	Incident organization and security incident handling: Guidelines for telecommunication organizations	
G.827	Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths	
G.1000	Communications Quality of Service: A framework and definitions	
G.1030	Estimating end-to-end performance in IP networks for data applications	
G.1050	Network model for evaluating multimedia transmission performance over Internet Protocol	
G.1081	Performance monitoring points for IPTV	
H.235.0	H.323 security: Framework for security in H series H.323 and other H.245-based) multimedia systems	
H.235.1	H.323 security: Baseline security profile	
H.235.2	H.323 security: Signature security profile	
H.235.3	H.323 security: Hybrid security profile	
H.235.4	H.323 security: Direct and selective routed call security	
H.235.5	H.323 security: Framework for secure authentication in RAS using weak shared secrets	
H.235.6	Voice encryption profile with native H.235/H.245 key management	
H.Imp235	Implementors Guide for H.235 V3: "Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals"	
H.323	Packet-based multimedia communications systems	
H.350	Directory services architecture for multimedia conferencing	
H.460.17	Using H.225.0 call signalling connection as transport for H.323 RAS messages,	
H.460.18	Traversal of H.323 signalling across network address translators and firewalls	
H.460.19	Traversal of H.323 media across network address translators and firewalls	
H.510	Mobility for H.323 multimedia systems and services	

Recommendation	Title	Equivalent text
H.530	Symmetric security procedures for H.323 mobility in H.510	
J.160	Architectural framework for the delivery of time-critical services over cable television networks using cable modems	
J.170	IPCablecom security specification	
J.360	IPCablecom2 Architecture Framework - Main document	
M.3010	Principles for a telecommunications management network	
M.3016.0	Security for the management plane: Overview	
M.3016.1	Security for the management plane: Security requirements	
M.3016.2	Security for the management plane: Security services	
M.3016.3	Security for the management plane: Security mechanism	
M.3016.4	Security for the management plane: Profile proforma	
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	
M.3210.1	TMN management services for IMT-2000 security management	
Q.816	CORBA-based TMN services	
Q.834.3	A UML description for management interface requirements for Broadband Passive Optical Networks	
Q.834.4	A CORBA interface specification for Broadband Passive Optical Networks based on UML interface requirements	
Q.1701	Framework for IMT-2000 networks	
Q.1702	Long-term vision of network aspects for systems beyond IMT-2000	
Q.1703	Service and network capabilities framework of network aspects for systems beyond IMT-2000	
Q.1741.1	IMT-2000 references to release 1999 of GSM evolved UMTS core network with UTRAN access network	3GPP
Q.1742.1	IMT-2000 references to ANSI-41 evolved core network with cdma2000 access network	3GPP2
T.4	Standardization of Group 3 facsimile terminals for document transmission	
T.36	Security capabilities for use with Group 3 facsimile terminals	
T.37	Procedures for the transfer of facsimile data via store-and-forward on the Internet	
T.38	Procedures for real-time Group 3 facsimile communication over IP networks	
T.563	Terminal characteristics for Group 4 facsimile apparatus	
X.500	The Directory: Overview of concepts, models and services	ISO/IEC 9594-1
X.501	The Directory: Models	ISO/IEC 9594-2
X.509	The Directory: Public-key and attribute certificate frameworks	ISO/IEC 9594-8
X.511	The Directory: Abstract service definition	ISO/IEC 9594-3
X.518	The Directory: Procedures for distributed operation	ISO/IEC 9594-4
X.519	The Directory: Protocol specifications	ISO/IEC 9594-5
X.520	The Directory: Selected attribute types	ISO/IEC 9594-6
X.521	The Directory: Selected object classes	ISO/IEC 9594-7
X.525	The Directory: Replication	ISO/IEC 9594-9

Recommendation	Title	Equivalent text
X.530	The Directory: Use of systems management for administration of the Directory	ISO/IEC 9594-10
X.711	Common management information protocol: Specification	ISO/IEC 9596-1
X.736	Systems Management: Security alarm reporting function	ISO/IEC 10164-7
X.740	Systems Management: Security audit trail function	ISO/IEC 10164-8
X.741	Systems Management: Objects and attributes for access control	ISO/IEC 10164-9
X.780	TMN Guidelines for defining CORBA Managed Objects	
X.780.1	TMN guidelines for defining coarse-grained CORBA managed object interfaces	
X.780.2	TMN guidelines for defining service-oriented CORBA managed objects and façade objects	
X.781	Requirements and guidelines for Implementation Conformance Statements proformas associated with CORBA-based systems	
X.790	Trouble management function for ITU-T applications	
X.800	Security architecture for Open Systems Interconnection for CCITT applications	ISO/IEC 7498-2
X.802	Lower layers security model	ISO/IEC TR 13594
X.803	Upper layers security model	ISO/IEC 10745
X.805	Security architecture for systems providing end-to-end communications	ISO/IEC 18028-2
X.810	Security frameworks for open systems: Overview	ISO/IEC 10181-1
X.811	Security frameworks for open systems: Authentication framework	ISO/IEC 10181-2
X.812	Security frameworks for open systems: Access control framework	ISO/IEC 10181-3
X.813	Security frameworks for open systems: Non-repudiation framework	ISO/IEC 10181-4
X.814	Security frameworks for open systems: Confidentiality framework	ISO/IEC 10181-5
X.815	Security frameworks for open systems: Integrity framework	ISO/IEC 10181-6
X.816	Security Frameworks for open systems: Security audit and alarms framework	ISO/IEC 10181-7
X.830	Generic upper layers security: Overview, models and Notation	ISO/IEC 11586-1
X.831	Generic upper layers security: Security Exchange Service Element (SESE) service definition	ISO/IEC 11586-2
X.832	Generic upper layers security: Security Exchange Service Element (SESE) protocol specification	ISO/IEC 11586-3
X.833	Generic upper layers security: Protecting transfer syntax specification	ISO/IEC 11586-4
X.834	Generic upper layers security: Security Exchange Service Element (SESE) Protocol Implementation Conformance Statement (PICS) proforma	ISO/IEC 11586-5
X.835	Generic upper layers security: Protecting transfer syntax Protocol Implementation Conformance Statement (PICS) proforma	ISO/IEC 11586-6
X.841	Security techniques – Security Information Objects for access control	ISO/IEC 15816
X.842	Security techniques – Guidelines for the use and management of trusted third party services	ISO/IEC TR 14516
X.843	Security techniques – Specification of TTP services to support the application of digital signatures	ISO/IEC 15945
X.Sup3 to X.800-X.849	Supplement on guidelines for implementing system and network security	

Recommendation	Title	Equivalent text
X.1031	Roles of end users and telecommunications networks within security architecture	
X.1034	Guidelines on extensible authentication protocol based authentication and key management in a data communication network	
X.1035	Password-authenticated key exchange (PAK) protocol	
X.1036	Framework for creation, storage, distribution and enforcement of policies for network security	
X.1051	Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	ISO/IEC 27011
X.1055	Risk management and risk profile guidelines for telecommunication organizations	
X.1056	Security incident management guidelines for telecommunications organizations	
X.1081	A framework for the specification of security and safety aspects of telebiometrics	
X.1082	Telebiometrics related to human physiology	ISO/IEC 80000-14
X.1083	Biometrics – BioAPI interworking protocol	ISO/IEC 24708
X.1084	Telebiometrics system mechanism - Part 1: General biometric authentication protocol and system model profiles for telecommunications systems	
X.1086	Telebiometrics protection procedures - Part 1: A guideline to technical and managerial countermeasures for biometric data security	
X.1088	Telebiometrics digital key framework (TDK) – A framework for biometric digital key generation and protection	
X.1089	Telebiometrics Authentication Infrastructure (TAI)	
X.1111	Framework for security technologies for home network	
X.1112	Device certificate profile for the home network	
X.1113	Guideline on user authentication mechanisms for home network services	
X.1114	Authorization framework for home network	
X.1121	Framework of security technologies for mobile end-to-end data communications	
X.1122	Guideline for implementing secure mobile systems based on PKI	
X.1123	Differentiated security service for secure mobile end-to-end data communication	
X.1124	Authentication architecture for mobile end-to-end communication	
X.1125	Correlative reacting system in mobile data communication	
X.1141	Security Assertion Markup Language (SAML 2.0)	OASIS SAML 2.0
X.1142	eXtensible Access Control Markup Language (XACML 2.0)	OASIS XACML 2.0
X.1143	Security architecture for message security in mobile web services	
X.1151	Guideline on secure password-based authentication protocol with key exchange	
X.1152	Secure end-to-end data communication techniques using trusted third party services	
X.1161	Framework for secure peer-to-peer communications	

Recommendation	Title	Equivalent text
X.1162	Security architecture and operations for peer-to-peer networks	
X.1171	Threats and requirements for protection of personally-identifiable information in applications using tag-based identification	
X.1191	Functional requirements and architecture for IPTV security aspects	
X.1205	Overview of cybersecurity	
X.1206	A vendor-neutral framework for automatic notification of security related information and dissemination of updates	
X.1207	Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software	
X.1231	Technical strategies on countering spam	
X.1240	Technologies involved in countering email spam	
X.1241	Technical framework for countering e-mail spam	
X.1242	Short message service (SMS) spam filtering system based on user-specified rules	
X.1244	Overall aspects of countering spam in IP-based multimedia applications	
X.1250	Baseline capabilities for enhanced global identity management and interoperability	
X.1251	A framework for user control of digital identity	
X.1303	Common alerting protocol (CAP 1.1)	OASIS CAP v1.1
X.Sup6	ITU-T X.1240 series - Supplement on countering spam and associated threats	
X.Sup7	ITU-T X.1250 series - Supplement on overview of identity management in the context of cybersecurity	
Y.2001	General overview of NGN	
Y.2701	Security Requirements for NGN release 1	
Y.2720	NGN identity management framework	
	Other Publications	
	Outside plant Technologies for public networks	
	Application of Computers and Microprocessors to the Construction, Installation and Protection of Telecommunication Cables	

Printed in Switzerland
Geneva, 2009