International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(09/2020)

XSTR-SUSS

Successful use of security standards

Summary

This Technical Report on successful use of security standards presents examples of how ITU-T Recommendations are used today in the market place to help protect networks, people, data and critical infrastructure. It is intended to help users, especially those from developing countries, to gain a better understanding of the value of using security-related ITU-T Recommendations in a variety of contexts (e.g., business, commerce, government, industry).

NOTE

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

© ITU 2021

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Technical Report ITU-T TR-SUSS

Successful use of security standards

1 Scope

This Technical Report present examples of how ITU-T Recommendations are used today in the market place to help protect networks, people, data and critical infrastructure. The report focuses on how approved security-related ITU-T Recommendations can be successfully deployed. Examples, of individual Recommendations (such as Recommendation ITU-T X.805) and families of Recommendations (such as CYBEX) are considered.

In selecting the specific standards for inclusion in this Technical Report, ITU-T Recommendations implemented in telecommunication networks and for the provision of services will be considered, as well as those provided for foundational understanding and high-level guidance for secure operation.

The target audience is users, especially those from developing countries.

This Technical Report also serves as a promotional tool of successful ITU-T achievements.

2 Abbreviations and acronyms

AA	Attribute Authority
ABAC	Attribute Based Access Control
ASN.1	Abstract Syntax Notation 1
B2B	Business to Business
BER	Basic Encoding Rules
B2C	Business to Customer
CA	Certification Authority
CAP	Common Alerting Protocol
CER	Canonical Encoding Rules
CIRTs	Computer Incident Response Teams
CRL	Certificate Revocation List
CYBEX	Cybersecurity Information Exchange
DLT	Distributed Ledger Technologies
DID	Decentralized Identifier
DNS	Domain Name System
FIDO	Fast Identity Online
FTAM	File Transfer Access and Management
RFC	Request For Comments
G2C	Government to Citizen
HTTP	Hyper Text Transmission Protocol
ICT	Information and Communication Technology
IETF	Interent Engineering Task Force

IoT	Internet of Things
IoS	iPhone Operating System
IPAWS	Integrated Public Alert and Warning Systems
IPTV	Internet Protocol Television
ITS	Intelligent Transportation System
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
MoU	Memorandum of Understanding
NGN	Next Generation Network
OASIS	Organization for the Advancement of Structured Information Standards
Pwd	Password
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
RBAC	Role-Based Access Control
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SSI	Self-Sovereign Identity
SOA	Source Of Authority
SNMP	Simple Network Management Protocol
SSO	Single Sign On
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
TARA	Threat Assessment and Remediation Analysis
TPM	Trusted Platform Module
KYC	Know Your Customer
W3C	World Wide Web Constorium
WAIS	Wide Area Information Server
WebAuthN	Web Authentication
WMO	World Meteorological Organization
XML	Extensible Markup Language
XSD	XML Schema Definition
U2F	Universal Second factor Protocol
UAF	Universal Authentication Protocol
UN	United Nations
4G	4th Generation Network
5G	5th Generation Network

3 Introduction

Standards play a pivotal role in improving cyber security across different organizations, networks, communities and cross-security domains. Standardizing processes and procedures is essential to achieving effective cooperation across security domains. The use of internationally agreed upon standards as a basis for network security promotes commonality of approaches and provides a cost effective means for deploying secure solutions as opposed to developing one-off solutions for each organization.

The use of common standardized security profiles facilitates interoperability and the reuse of solutions and products. Such profiles can help developing countries to incorporate security faster, more consistently and at lower cost. The use of common and interoperable security standards makes it easier for organizations to enhance network resilience.

Security standards play an important role in improving approaches to cyber security threat analysis, mitigation and sharing. In particular, standards can help improve an organization's internal processes through the use of proven security methodologies. Security standards can provide means for adopters to assess new products or services. Security standards can be used as an impetus for testing and adopting of new technologies or business models.

To be able to mitigate cybersecurity threats at a global level, the task of standardizing processes and procedures is essential for enabling successful cooperation in a cross-border or cross-community environment. In the event of a cybersecurity threat, the use of common standards would help ensure that various entities can interact with each other according to well-understood set of best practice procedures.

Standardized network security solutions benefit both suppliers and service providers through economies of scale in product development and component interoperability. ITU-T standards act as repositories for the industry best security practices.

3.1 Evolution of ITU-T security standards

Organizations need to devise a comprehensive plan for addressing their security needs. Organizations are encouraged to view security as a process or way of thinking on how to protect systems, networks, applications, and resources.

Cybersecurity (see Recommendation ITU-T X.1205) aims at securing the cyber environment, which is a system of systems that may involve stakeholders belonging to public and private organizations, using diverse components and different approaches to security. As such, it is beneficial to think of cybersecurity in the following sense:

– The collection of policies and actions that are used to protect connected networks (including, computers, devices, hardware, stored information and information in transit) from unauthorized access, modification, theft, disruption, interruption or other threats.

– An ongoing evaluation and monitoring of the above policies and actions in order to ensure the continued quality of security in the face of the changing nature of threats.

Organizations need to devise a comprehensive plan for addressing their security needs. Security is not 'one size fits all' (see Recommendation ITU-T X.805). Security cannot be achieved by a collection of modules that are interconnected together. Organizations are encouraged to view security as a process or way of thinking on how to protect systems, networks, applications, and network services.

Security has to be comprehensive across all network layers. Adopting a layered approach to security that, when combined with strong policy management and enforcement, provides security professionals with a choice of security solutions that could be modular, flexible, and scalable.

Security is difficult to test, predict and implement. Security is not a 'one size fits all' situation. The security needs and the recommended security strategy of each organization are unique and different.

For example, an enterprise, a telecommunication provider, a network operator, or service providers each can have a unique set of business needs and may have evolved their networking environment to meet these needs. ITU-T Recommendations can help organizations to properly evaluate their security needs and adopt best of breed solutions for solving those problems.

ITU-T, and in particular its Study Group 17, is responsible for building confidence and security in the use of information and communication technologies (ICTs). This includes studies relating to cybersecurity, security management, countering spam and identity management. It also includes security architecture and framework, protection of personally identifiable information, and security of applications and services for the Internet of things (IoT), smart grid, smartphone, Internet protocol television (IPTV), web services, social network, cloud computing, mobile financial system, and tele-biometrics.

The ITU-T security work continues to evolve in response to requirements raised by ITU-T members as reflected in trends in industry and security communities. ITU-T provides a venue to help its members standardize best of class security Recommendations that can be used to address many security risks and challenges.

In general, ICT security requirements are defined in terms of perceived threats to networks and systems, the inherent vulnerabilities in networks and system, and the steps that should be taken to counter these threats to reduce exposure to their vulnerabilities. Protection requirements extend to the network and its components. Each organization should prioritize its security profile based on well-articulated and understood risk appetite. Understanding risk including disaster recovery plans should be an integral component of any security policy. Fundamental concepts of security, including threats, vulnerabilities and security countermeasures, are defined in many ITU-T individual or families of Recommendations.

3.2 Who does the ITU-T security Recommendations affect

ITU-T develops security Recommendations that affect many aspects of telecommunication networks. The telecommunication sector of information security has its own needs and special security requirements. ITU-T develops standards that focus on telecommunications networks since telecom environment risk affects real-time critical infrastructure and may differ significantly from other verticals.

Standards are essential for the success in securing complex and geographically distributed security implementations. It is important to have a standardized and widely accepted approach on security to ensure interoperability among systems, services and networks.

ITU-T Recommendations enable adopters to achieve a proven and documented level of security that facilitate governance of security systems and in many cases ensure compliance with regulations.

In many cases, ITU-T Recommendations can provide vendors with an advantage in meeting customer requirements and objectives. This is important where in specific cases the customers are required to pass certification criteria and accreditation. In other cases, customers will need to meet accreditation criteria that are needed to conduct business with the public sector. There are many requirements on meeting certain authentication assurance levels when dealing with health and personal data. For example, Recommendation ITU-T X.1254 helps companies to comply with regulations requiring strong authentication assurance.

ITU-T Recommendations affect adoption, and national deployments. In many cases, it is important to note that ITU-T Recommendations can be used as benchmarks and for technology maturity comparisons. Furthermore, standards ensure interoperability among systems, which is good for the business since it prevents vendor lock-in.

All ITU-T security Recommendations are freely available and are thereby accessible to a variety of users. Many ITU-T security Recommendations are available in six United Nations (UN) languages; especially all those having regulatory or policy implications. Such multi linguistic standards are of interest to developing countries in regions where English may not be the primary language.

3.3 Business benefits

There are many business benefits for using and adopting ITU-T security Recommendations. One benefit is for international corporations, where costs can be saved through the adoption of ITU-T standards. Security service providers can also benefit from adopting ITU-T security best practices and profiles. Having telecom based security as an integral component of enterprises, in public and private sector implementations protects citizens and enhances the range of offerings that citizens can trust and get accustomed to enjoying and appreciating.

International security standards as developed by ITU-T can enhance the range of service offerings to citizens and consumers. Recommendations as developed by ITU-T provide a set of security requirements that act as a baseline that enterprises can use to determine needed trust among participants when exchanging sensitive information. ITU-T Recommendations can be used to verify how and if organizations can meet claimed level of security.

3.4 Success factors

Standards play an important role in implementing effective solutions for providing confidence and security in the use of ICT across different geographical regions and communities. Standards provide the template for public and private entities to produce internal standardized processes and procedures that are essential for achieving interoperable and secure collaboration across borders and security domains.

ITU-T standards are designed to be used by organizations to meet a variety of security objectives in an interoperable fashion. The success of ITU-T standards is based on the observation that the development of standards is necessary for security and is best done with the participation of public and private sectors in the process. This working principle is important since the cooperation of various stakeholders is essential for the development of successful standards.

The online world does not observe national borders or legal boundaries. It does not share a uniform perception or definition of security and privacy. Today's Internet is built using a relatively common set of Internet security protocols and technologies. This observation is a key concept in the development of ITU-T security standards. ITU-T realizes both public and private sector information security practices in the developments of its standards. Therefore, by identifying and responding to evolving risks and the ability to develop technology with solutions that are based on current foundational technologies, ITU-T standards play an important role in improving solutions for information security across different geographical regions and communities.

There are many metrics for measuring the success and maturity of a standard. Examples of these criteria are provided next.

3.4.1 Readiness, abilities and effectiveness

ITU-T security Recommendations contain measures of information security, which pertain to the readiness, and ability of operators or users to counter security threats.

Creation of standards that help individual actors to work together to develop well defined procedures is an essential part of achieving successful cooperation across diversified implementations. In the absence of reliance on common standards, individual organizations could fail to develop internal standards that enable them to work and compete in an increasingly connected world. As such, standardizing both processes and communications using ITU-T standards can be very effective. For example, using cybersecurity threat and vulnerability standards

from ITU-T can enable entities belonging to different organizations to react to a major cyber incident in a collaborated fashion. They can be used to predict the next attack vector and stop it before it causes major damage.

3.4.2 Balance of interests

In responding to threats, the balance of stakeholder interests should be maintained; it is crucial to reflect a diversity of interests during the development of a standard. A variety of stakeholders (private sector/industry, governments, academia and research) should be involved and consulted in the development of standards. Finding consensus among the diverse interests during standards development helps to ensure wide applicability of the resulting standard.

ITU-T can help vendors to develop products based on standardized technologies. Corporations benefit from this approach since standards harmonization among vendors encourages security cooperation among organizations and ensures a larger pool of available subject matter in the industry.

3.4.3 Impact

Security standards and counter measures are ranked according to their potential impact and their estimated implementation costs.

ITU-T standards provide a blueprint to enable an organization to design an internal security infrastructure that is secure. For example, an organization using ITU-T Recommendations can use ITU-T standards to explain its security solutions in a manner that is easily understood by its customers. This simple practice can provide a competitive edge to the organization. The reliance on ITU-T standards in today's shrinking budgets reduces an organization's auditing and compliance costs. ITU-T profiles and best practices can provide organizational standard blueprints for setting up internal security standards.

Using ITU-T standards can help an organization to reduce costs when evaluating products from various vendors. An organization can use ITU-T Recommendations to classify vendor security products into various security categories and then compare the products in a meaningful manner using appropriate benchmarking methods. Interoperability among vendors can also be tested and evaluated.

3.4.4 Controllability

All ITU-T security Recommendations in this technical report are verifiable, published and maintained using accepted methodologies.

ITU-T maintains ICT security standard roadmaps. The ICT Security Standards Roadmap has been developed to assist in the development of security standards by bringing together information about existing standards and current standards work in key standards development organizations. In addition to aiding the process of standards development, this Roadmap provides information that helps potential users of security standards, and other standards stakeholders gain an understanding of which standards are available or under development as well as the key organizations that are working on these standards.

The Roadmap was initiated by ITU-T Study Group 17 in 2006 and subsequently gained the support of other standards development organizations as well as a number of public sector organizations with an interest in security standards.

In addition, ITU-T maintains a security manual. The manual provides an overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications. 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 security manual does not

attempt to cover all the ITU-T security work that has either been completed or is underway. Instead, it focuses on key selected topics and provides web links to additional information.

3.4.5 Variety of implementations

Successful security standards provide flexibility in the choice of implementation while keeping to a minimum the variety of options relative to the number of mandatory features.

ITU-T understands that in some cases different components of a solution might be standardized at different standards bodies. In this regard, ITU-T has established effective liaisons, memorandum of understanding (MoUs) and other means of collaboration with other bodies to help to identify and bridge the gap among standards in order to ensure interoperability.

ITU-T standards take into account the benefit of the consumer and profiles that benefit the targeted audience. For example, in some areas of information security public-key infrastructure (PKI) technology is developed at ITU-T, OASIS and IETF with many vendor related libraries that can be considered as de-facto standards. ITU-T work helps adopters to navigate among these technologies and, there are several different groups of standards that are defined. To some extent, these standards are competing with each other for adoption and it is often difficult for the end user to judge which is best for their particular requirements. Occasionally, it is necessary to mix and match standards from different families in order to achieve the goal. For instance, when implementing PKI, it is not unusual to see organizations adopt a combination of standards (for example Recommendation ITU-T X.509 (ITU) for the certificate format, PKIX (IETF) standards for core PKI and PKCS (RSA) standards for interfacing to secure devices).

3.4.6 How to measure success

A standard can be successful during its development since it met all of its design considerations, but may not be adequately deployed in the field. In this work, we consider the teachings of an ITU-T Recommendation to be successful if it meets its original goals and is respected and referenced in the industry.

3.4.6.1 Sound technical design

This factor means that the protocol follows good design principles that lead to ease of implementation and interoperability, such as those described in Recommendations ITU-T X.800 and ITU-T X.1205. The standards comply with simple, modular, and good failure proof measures. Extensibility is also a measure of success. The ability to extend a standard to be used beyond its original design goals is a desirable feature for those standards that are geared to solve mufti-purpose goals.

3.4.6.2 Threats mitigation

Hackers target widely adopted protocols. In general, the more successful a protocol becomes, the more attractive a target it will be for hackers. Regardless of the care that is taken during development, security holes will likely be discovered in the field. A standards body should be able to deal with these threats and vulnerabilities and allow the rapid release of fixes to such threats. ITU-T has a sophisticated development process to issue security fixes and bug fixes to its Recommendations.

3.4.6.3 Threat awareness

As organizations grow in size, complexity and maturity, the need for a well thought and documented security threat and awareness for the enterprise becomes essential.

The more specialized the employees become, the more the need for focused and targeted training programs will be needed within organizations.

ITU-T Recommendations help organizations to build internal programs that identify security risks.

4 Example of security Recommendations and their adoption

This clause provides examples of the successful use and adoption of many ITU-T standards in the security area. The clause is divided into several categories to better illustrate the impact within a given security area.

4.1 Public key infrastructure

Recommendation ITU-T X.509, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

Recommendation ITU-T X.509 is part of the ITU-T X.500 series of Recommendations that is also widely used outside a directory context. It provides a framework for both public-key infrastructure (PKI) and for privilege management infrastructure (PMI). An ITU-T X.500 directory may store PKI-related and PMI-related information objects to support those infrastructures and an ITU-T X.500 directory may use PKI and PMI capabilities to protect directory information. The ITU-T X.500 series includes a set of directory Recommendations that are also published as ISO/IEC specifications. In particular, the list of identical Recommendations includes:

– Recommendation ITU-T X.500 (2019) | ISO/IEC 9594-1:2020, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.

– Recommendation ITU-T X.501 (2019) | ISO/IEC 9594-2:2020, *Information technology – Open Systems Interconnection – The Directory: Models*.

– Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

– Recommendation ITU-T X.511 (2019) | ISO/IEC 9594-3:2020, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition*.

– Recommendation ITU-T X.518 (2019) | ISO/IEC 9594-4:2020, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation*.

– Recommendation ITU-T X.519 (2019) | ISO/IEC 9594-5:2020, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications*.

– Recommendation ITU-T X.521 (2019) | ISO/IEC 9594-7:2020, *Information technology – Open Systems Interconnection – The Directory: Selected object classes*.

– Recommendation ITU-T X.525 (2019) | ISO/IEC 9594-9:2020, *Information technology – Open Systems Interconnection – The Directory: Replication*.

These Recommendations constitute a family of Recommendations that specify public-key infrastructure (PKI).

4.1.1 Who does this standard affect?

This standard affects any vendor that is developing products, profiling applications or deploying security solutions that are based on public-key infrastructure (PKI) or privilege management infrastructure (PMI). The standard is particularly applicable for services such as authentication, encryption and confidentiality, digital signatures, nonrepudiation and authorization.

4.1.2 Summary of standard

The standard defines frameworks for PKI and for PMI. These frameworks include:

– Infrastructure models;

– Certificate and certificate revocation list (CRL) syntax definitions;

– Directory schema object definitions;

– Certificate path processing procedures.

The standard also specifies use of these frameworks by Directory systems in their provision of secure services to Directory users.

Eight editions of ITU-T X.509 have been published over the years, with the most recent being approved by ITU in September 2016. All editions have been developed cooperatively by ITU and ISO/IEC. The corresponding ISO/IEC standard is ISO/IEC 9594-8.

4.1.2.1 Public key infrastructure

The basic PKI model consists of public-key certificates being issued by certification authorities (CAs) to end-entities for use in security services including authentication, confidentiality, and non-repudiation. CAs may also issue certificates to other CAs creating certificate paths between a given end-entity certificate and remote verifiers. A revocation scheme and mechanism for publishing information about certificates that are no longer considered trustworthy by their issuer is also defined.

The PKI framework has evolved from the 1st edition through the 8th edition. As additional requirements emerge, the basic PKI models have remained unchanged; however, the syntaxes of both public-key certificates and CRLs have evolved. The versions, defined in the 3rd edition and maintained through the 8th edition, are public-key certificate (v3) and CRL (v2).

These syntaxes enable an unbounded set of extensions to be included in certificates and CRLs. The standard set of extensions, enables inclusion of additional information such as:

– Key and policy information;
– Subject and Issuer details;
– Certification path constraints;
– CRL numbers and certificate revocation reasons;
– CRL partitioning and delta information.

Additional extensions can be defined by other industry groups.

The necessary Directory schema definitions to store and retrieve PKI data objects in lightweight directory access protocol (LDAP) and ITU-T X.500 repositories are specified. These objects include certification authorities (CAs), certificate subjects, CRLs, certification paths and policy objects.

4.1.2.2 Privilege management infrastructure

The privilege management infrastructure (PMI) framework is more recent than its PKI counterpart. The 3rd edition of ITU-T X.509 was the first to introduce a basic syntax for attribute certificates. The 4th edition extended that structure resulting in attribute certificate (v2) and defined the framework for privilege management, along the same basic models as for PKI. The 6th edition has further extended the framework by allowing privileges assigned in one PMI domain to be effective in another PMI domain.

The PMI model enables very basic implementations, where privilege is assigned directly by the source of authority (SOA) to the privilege holder through issuance of an attribute certificate. Privilege may also be assigned through public-key certificates but there are limitations to their use in PMI. The model also enables more complex infrastructures that include privilege delegation through intermediary attribute authorities (AA) as well as the use of roles. With roles, a role specification certificate would be issued to a role rather than an individual and contains the specific privileges of the role. Corresponding role assignment certificates are issued to individuals occupying a given role, thereby indirectly assigning the role privileges to those individuals. The same scheme for publishing revocation information about public-key certificates is adapted for use with attribute certificates that are no longer considered trustworthy.

Although the base syntax for attribute certificates was defined in the 3rd edition, the syntax required extending and resulted in (v2) attribute certificate syntax. These revisions enable tighter binding between an attribute certificate and the corresponding public-key certificate used to authentication its holder, as well as issuance of attributes certificates to entities that do not participate in authentication protocols (e.g., software applets). A standard set of extensions was added for PMI to support:

– Basic privilege restrictions and limitations.
– Control of delegation and policy.
– Linking of certificates for role management.
– Identification of SOA entities and publication of privilege definitions.
– Revocation scheme extensions.

The necessary Directory schema definitions to store and retrieve PMI data objects in LDAP and ITU-T X.500 repositories are specified. These objects include source of authority (SOA), attribute authority (AA), attribute certificate holders, CRLs, delegation paths, and privilege policy objects.

4.1.2.3 Directory use of PKI and PMI

The use of PKI, for Directory authentication and for the protection of directory operations and data objects, is outlined in Recommendation ITU-T X.509. However, the details of how PKI relates to specific Directory functions are described within the other specifications in the ITU-T X.500 series (primarily Recommendations ITU-T X.511 and ITU-T X.518). Similarly, the use of attribute certificates for access control to directory information is described in other specifications in the series (primarily ITU-T X.501).

4.1.3 Business benefits

PKI and PMI are being used as the foundation for securing transactions in business-to-business (B2B), business-to-customer (B2C) and government-to-citizen (G2C) environments. Profiles of Recommendation ITU-T X.509 are being defined for specific communities in the Internet, financial, government and other sectors. The basic data structures defined in ITU-T X.509 for certificates and CRLs, through their extensibility schemes, enable application specific extensions, while still supporting fundamental interoperability requirements.

4.1.4 Technologies involved

The standard is based on the use of public-key cryptography for digital signatures and encryption. The standard also makes use of Directory systems, as defined in related specifications within the ITU-T X.500 series and as defined in the IETF LDAP activities.

4.2 Cybersecurity overview

Recommendation ITU-T X.1205, Overview of cybersecurity

4.2.1 Who does this standard affect?

Anyone developing products, profiling application security, or deploying security solutions across the enterprise, or public and private organizations, should read Recommendation ITU-T X.1205.

4.2.2 Summary of standard

Recommendation ITU-T X.1205 provides a taxonomy of security threats from an organizational point of view along with a discussion of the threats at the various layers of a network. The work addresses 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). The Recommendation aims to build a foundation of knowledge that can help secure future networks. Various threat countermeasures are discussed including routers, firewalls, antivirus protection,

intrusion detection systems, intrusion protection systems, secure computing, and audit and monitoring. Network protection principles such as defence-in-depth and access management are also discussed. Risk management strategies and techniques are reviewed, including the value of training and education in protecting the network. Examples of securing various networks based on the discussed techniques are also provided.

4.2.2.1 Cybersecurity definition

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.

4.2.2.2 Layered approach

The work discusses a layered approach to security that enables organizations to create multiple levels of defence against threats. Cybersecurity techniques can be used to ensure system availability, integrity, authenticity, confidentiality, and non-repudiation as well as to ensure that user privacy is respected. Cybersecurity techniques can also be used to establish a user's trustworthiness. Some of the most important current cybersecurity techniques include:

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

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

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

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

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

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

4.2.3 Business benefits

Recommendation ITU-T X.1205 is essential for organizations that are trying to build a modern security infrastructure that can protect the entity against all types of security threats and attacks. The basic concepts in ITU-T X.1205 ensure an organization's internal security objectives are met while still supporting fundamental interoperability requirements and compliance.

4.2.4 Technologies involved

The standard provides a layered security architecture that is independent from any specific implementation.

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

Recommendation ITU-T X.805, Security architecture for systems providing end-to-end communications

4.3.1 Who does this standard affect?

This Recommendation is essential for any entity that is performing comprehensive network security assessment and planning. Recommendation ITU-T X.805 addresses the inherent complex security problems in next generation networks (NGNs) with their division into layers and planes and elements and the need to have at hand a holistic security methodology to systematically engineer security for such systems.

ITU-T X.805 was developed as the framework for the architecture and dimensions in achieving end-to-end security of distributed applications. It provides a comprehensive, multi-layered, end-to-end network security framework across eight security dimensions in order to combat network security threats. The concepts in the ITU-T X.805 standard can be applied to all phases of a network security program. Enterprises and service providers alike can use ITU-T X.805 to provide a rigorous approach to network security throughout the entire lifecycle of their security programs.

4.3.2 Summary of standard

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

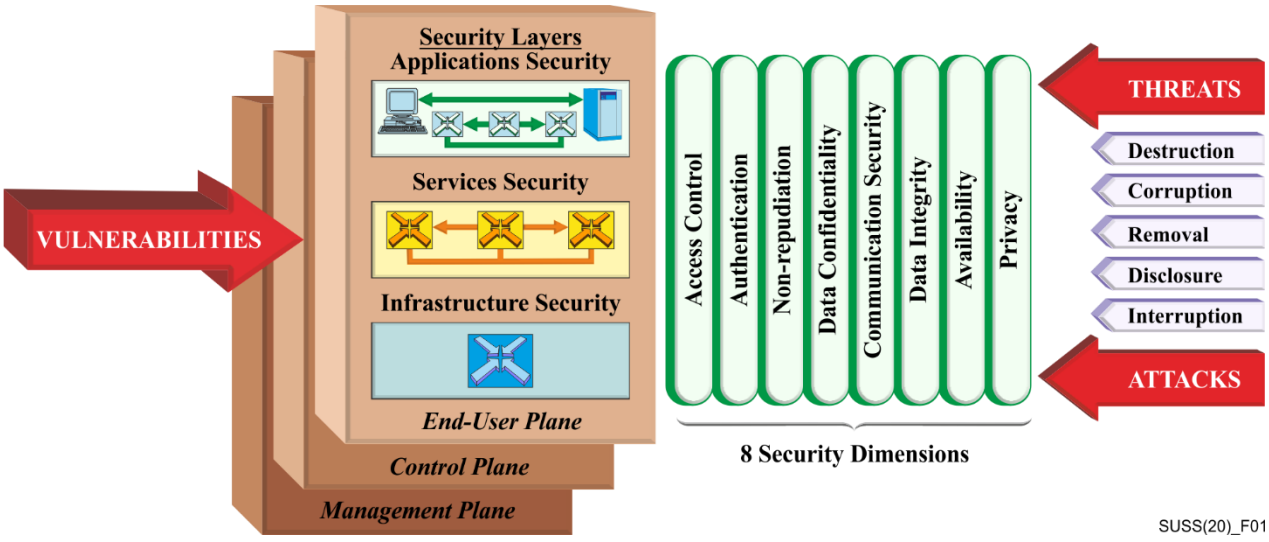

Figure 1 – Security architectural elements in Recommendation ITU-T X.805

A security dimension is a set of security measures designed to address a particular aspect of network security. The basic security services of Recommendation ITU-T X.800 (access control, authentication, data confidentiality, data integrity and non-repudiation) are reflected in the functionalities of the corresponding security dimensions of Recommendation ITU-T X.805 (as depicted in Figure 1).

Recommendation ITU-T X.805 introduces three dimensions (communication security, availability and privacy) that are not in Recommendation ITU-T X.800:

– The communication security dimension, which ensures that information flows only between the authorized end points, i.e., information is not diverted or intercepted as it flows between these end points;

– The availability dimension, which ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network; and

– 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 domain name systems (DNS) names of devices in a service provider network.

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

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

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

– Infrastructure layer, which represents the fundamental building blocks of networks, their services and applications. Examples of components that belong to this layer include individual network elements, such as routers, switches and servers, as well as the communication links between them;

– 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

– 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:

– Management plane, which is concerned with operations, administration, maintenance and provisioning activities such as provisioning a user or a network;

– 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

– 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.

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

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

4.3.3 Business benefits

Recommendation ITU-T X.805 is essential for organizations that are trying to build a modern security infrastructure that can protect the entity against all types of security threats and attacks. The basic concepts in ITU-T X.805 ensure that organization internal security objectives are met while still supporting fundamental interoperability requirements and compliance.

Security is a major concern for enterprises and organizations in adopting Wi-Fi networks. The end objective is to provide an equivalent level of security to wireless networks that is found in wired networks. One key to accomplishing this is applying a standard that is backed by the International Telecommunications Union (ITU). Many vendors in the WIFI area use Recommendation ITU-T X.805 as the standard that provides a framework for building and achieving end-to-end security across a distributed network. The ITU-T X.805 security architecture provides a structured framework that forces the consideration of all possible threats and attacks to provide comprehensive end-to-end network security.

4.3.4 Technologies involved

The standard provides a layered security architecture that is independent from any specific implementation.

In developing ITU-T X.805, vendors worked within the ITU-T to address questions related to which standards can be used for securing the next generation networks. The focus of ITU-T X.805 is on network security design. It reflects a radical shift in security thinking. The focus on design provides a strategy for securing today's and future networks. The standard clearly indicates that individual products themselves do not provide technology services, but products are part of the ecosystem that provides the service and it is the systems that are designed securely from end to end.

Vulnerabilities found across different parts of a network or its elements emphasize the need for a consistent and verifiable security approach. The ITU-T X.805 standard provides organizations with the ability to perform in a consistent manner the task of cataloguing vulnerabilities. This allows an organization the ability to enforce a common set of security capabilities across the entire security services plane even when it has products from different vendors.

4.4 Identity and access management

Current identity and access management systems are based a centralized identity model. In these systems, organizations act as an identity service provider (IdSP) that establishes a point-to-point trusted relationship with each user. The centralized model is a traditional, siloed model. Federation in a centralized model is performed to ease business interactions between differing trust domains. Recommendation ITU-T X.1141 defines the security assertion markup language (SAML). Federation when combined with ITU-T X.1278 (XACML) provides a flexible framework for providing access control for many organizations.

The advances in distributed ledge technologies and the recent standards push at standardizing core foundational technologies for enabling distributed trust on-line has given a great impetus to a slow but steady shift in the market place towards decentralized identity based systems.

4.4.1 Centralized identity

In this model, each organization issues a credential to a user that allows the user to access its services. The organization manages the user's digital identity and decides on the accepted trust relationships. Trust between the user and the IdSP is typically established through the use of shared secrets such as the use of a username and a password. In some cases, shared secrets are augmented with multi-factor authentications such as hardware tokens, biometrics or fast identity online (FIDO) (ITU-T X.1277, ITU-T X.1278) based solutions.

Centralized models have disadvantages, in particular, the IdSP can store and collect data about users and in essence own the user identity and related data. Users have to trust the IdSP to do the right thing when it comes to managing their data. Although end users benefit from the organization's services, in most cases they do not have control over the management of their own identities, personal data or their personal identity attributes.

The centralized identity model requires a user to create and manage separate credentials for each of his business relationships with each IdSP. An organization requires the creation of these identities before a user is permitted access to its resources. This model overwhelms users with many online identities. The lack of mutual authentication at login make this model vulnerable to phishing and credential harvesting attacks. The model encourages users to reuse passwords, which leads to further security risks and vulnerabilities.

The centralized model places a burden on IdSP when it comes to life cycle management of identity. In particular, the model requires each IdSP to perform identity vetting (ITU-T X.1254) as part of the identity enrolment phase in the in identity life cycle management. Identity vetting is needed in order to establish a level of trust in the claimed identity. This process may be repeated during the whole life cycle of a given identity. This step is problematic from a user perspective since the centralized model requires the user to go through the identity vetting step separately with each identity provider. Additionality, data breaches threats increase the risks of account take-over due to the reliance of organizations on centralized data stores that are targeted by hackers on a regular basis.

ITU-T in cooperation with other standards bodies have realized the limitations of centralized identity models and have acted to develop a federated identity model. Federated identity models aim to reduce the burden on users by providing the ability for users to use their identity from one domain in another domain. The security assertion markup language (SAML) (ITU-T X.1141) provides more convenience for individuals by providing single sign on (SSO) functionality.

Federated identity management systems can provide authentication and authorization capabilities across organizational and system boundaries. It requires the establishment of business and trust agreements resulting in the ability that a user identity at one provider is recognized by other providers (members of the federation). In general, trust agreement also include contractual agreement on data ownership, usage of personally identifiable information (PII) and compliance (ITU-T X.1141).

The federation model benefits users since an identity service provider usually provides a single sign-on experience to a user. The federation model reduces the number of separate credentials that a user will need to maintain and acquire. In the federation model relying parties participating in the federation, including their users, are dependent on the availability of given IdSP services and its willingness to stay in the federation. As with the centralized identity model, authentication in the federation model is not mutual and suffers from the same limitations.

A major problem in centralized systems is the reliance on the use of passwords. There are many security vulnerabilities that result from the use of shared secrets such as password. Multi-factor

authentication (MFA) solutions aim towards solving some of the issues of passwords but are not fully immune to phishing and man in the middle attacks. For this reason ITU-T adopted ITU-T X.1277 and ITU-T X.1278 for strong user passwordless authentication that is based on ITU-T X.509 certificates and the use of public-private keys for authentication.

4.4.2 De-centralized identity

Decentralized identity could be implemented using distributed ledger technologies (DLT) or other emerging standards based technologies such as verifiable claims (ITU-T X.1252) and decentralized identifiers (DID (ITU-T X.1252). A decentralized identity model can build on top of a distributed ledger (DLT) and a relationship between a user and an organization [b-W3C-17]. In this model, the user and the organization are peers.

Decentralized identity allows users to assume control and ownership over their identities. The degree of ownership can vary depending on the decentralized model. In the self-sovereign identity (SSI) ITU-T X.1403 model, the concept assumes that entities would be able to have control of their own digital identity.

A decentralized identity model (ITU-T X.1252) consists of decentralized identifiers (DIDs) which are a type of identifier for verifiable, decentralized identity systems. The design of DIDs allows them to be under the control of the DID subject, which makes them independent from any centralized registry, identity provider, or a certificate authority. DIDs are uniform resource locators (URLs) that relate a DID subject to means for trustable interactions with that subject.

The task of resolving a DIDs results with a DID document (DDO), which is a simple document that describes how to use that specific DID. Each DID document contains at least three elements: cryptographic material, authentication suites, and service endpoints. Cryptographic material combined with authentication suites provide a set of mechanisms to authenticate a DID subject (which is the user that is related to the DDO). Examples of authentications options are public keys, and pseudonymous biometric protocols. Service endpoints enable trusted communications with the DID subject.

Verifiable credentials solves the problem of transmitting credentials such as driver's licenses, proofs of age, education qualifications, and healthcare data, over a network in a way that is verifiable, yet protects individual personal data. In this approach, credentials are composed of statements called verifiable claims. The verifiable claims ecosystem is composed of four primary roles:

1) The issuer, who issues verifiable credentials about a specific subject;
2) The holder, who stores credentials on behalf of a subject. Holders are typically also the subject of a credential;
3) The verifier, who requests a profile of the subject. A profile contains a specific set of credentials. The verifier confirms that the credentials provided in the profile are fit-for-purpose;
4) The identifier registry, which is a mechanism that is used to issue identifiers for the subjects.

A claim (ITU-T X.1252) is a statement about a subject, expressed as a subject-property-value relationship. Claims may be merged together to express a graph of information about a particular subject.

When an issuer sends data to a holder, it bundles a set of claims into a data structure called a credential and digitally signs the data structure. When a verifier requests data from a holder, the holder typically bundles a set of credentials into a data structure called a profile and digitally signs the data structure.

Recommendation ITU-T X.1403 develops guidelines for securing identity in a decentralized identity model. The work builds on top of the ITU-T stack of securing distributed ledgers as

described in Recommendation ITU-T X.1401 *Security threats to distributed ledger technology*, and Recommendation ITU-T X.1402 *Security framework for distributed ledger technology*.

4.5 Security assertion markup language

Recommendation ITU-T X.1141, Security Assertion Markup Language (SAML 2.0)

4.5.1 Who does this standard affect?

This standard forms the basis of one of the most successful developments of identity federation technologies in the Internet.

Security assertion markup language (SAML) is a standard that facilitates the exchange of security information among different organizations (with different security domains) to securely exchange authentication and authorization information.

SAML enables single sign on (SSO) capabilities for participating relaying parties. By using SSO an organization can share information about user identities and access privileges in a safe, secure and standardized manner. For this reason, SAML is the preferred identity assertion scheme for cloud and software as a service (SaaS) providers.

4.5.2 Summary of standard

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

Typically, there are a number of service providers that can make use of assertions about a subject in order to control access and provide customized service, and accordingly they become the relying parties of an asserting party called an identity provider. Recommendation ITU-T X.1141 defines three different kinds of assertion statements that can be created by a SAML authority. All SAML-defined statements are associated with a subject.

The three kinds of statements defined in Recommendation ITU-T X.1141 are:

– Authentication: The assertion subject was authenticated by a particular means at a particular time;

– Attribute: The assertion subject is associated with the supplied attributes; and

– Authorization decision: A request to allow the assertion subject to access the specified resource has been granted or denied.

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

A set of profiles have been defined to support single sign-on (SSO) of browsers and other client devices. Figure 2 illustrates the basic template for achieving SSO.

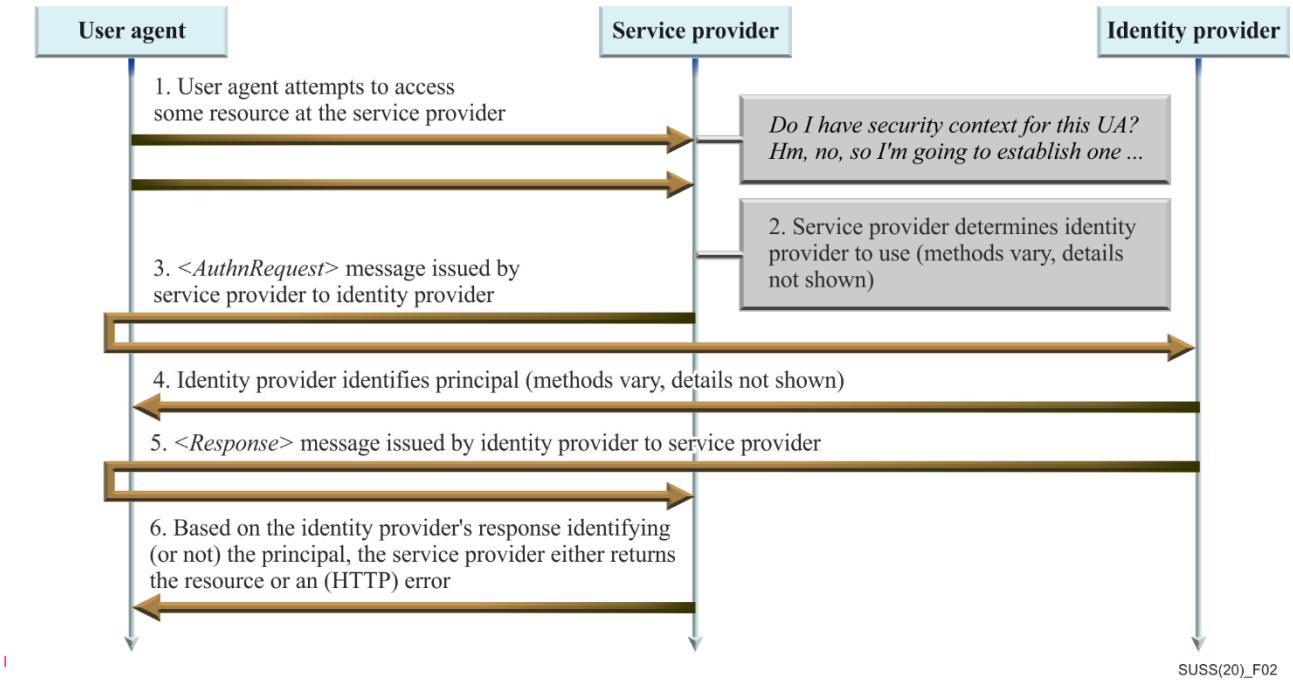

Figure 2 – Basic template for achieving SSO

4.5.3 Business benefits

Recommendation ITU-T X.1141 is essential for organizations that are trying to build a modern federated identity-based security infrastructure. Federation is the dominant direction in identity management today. Federation refers to the task of establishing a set of business agreements, cryptographic trust, and user identifiers or attributes across security domains to enable business interactions.

As cloud and mobile services promise to enable integration between business partners through loose coupling at the application layer, federation does so at the identity management layer through insulating each domain from the details of the others' authentication and authorization infrastructure.

SAML is the preferred solution for single sign-on into cloud applications. SAML-enabled software as a service (SaaS) applications are easier and quicker to user provision in complex enterprise environments, are more secure and help simplify identity management across large and diverse user communities.

4.5.4 Technologies involved

The standard provides a layered security architecture that is independent from any specific implementation.

In the cloud, SAML is the accepted standard for signing into cloud applications. SAML-based solutions eliminate the reliance on passwords for federated single sign on (SSO). SAML uses digital signatures to establish trust between the identity provider and the application. SAML enabled software as a service (SaaS) applications result in fast and secure user provisioning capabilities in IT environments.

SAML is in wide use for single sign-on in the cloud. Many of the SaaS vendors leverage SAML on mobile and desktop versions of their solutions. SAML adoption continues to stay strong. Many enterprises are realizing that the standard provides an important security enhancement by enabling better handle controlling access to sensitive data.

4.6 Universal authentication framework (ITU-T X.1277) and Client to authenticator protocol/Universal 2-factor framework (ITU-T X.1278)

Recommendations ITU-T X.1277 and ITU-T X.1278 are based on the FIDO Alliance (fidoalliance.org) set of specifications that are geared towards solving the use of shared credentials use such as passwords for authentication. The use of passwords for user authentication is problematic and is a major security risk that contributes to many security breaches every year.

Recommendation ITU-T X.1277 *Universal authentication framework (UAF)* describes the FIDO universal authentication framework (UAF) that enables online services and websites, whether on the open Internet or within enterprises, to transparently leverage native security features of end-user computing devices for strong user authentication and to reduce the problems associated with creating and remembering many online credentials.

Recommendation ITU-T X.1278 *Client to authenticator protocol/Universal 2-factor framework (U2F)* describes an application layer protocol for communication between an external authenticator and another client/platform, as well as bindings of this application protocol to a variety of transport protocols using different physical media. Both UAF and U2F protocols may either work alone or together.

4.6.1 Who does this standard affect?

Recommendations ITU-T X.1277 and ITU-T X.1278 in combinations of FIDO Alliance Web AuthN (see W3C Web AuthN) work provides a foundation for solving the security risks and threats associated with password based authentication method.

4.6.2 Summary of standard

This standard affects all consumer and enterprise facing applications developed for private or public entities. Security risks associated with passwords are sever and are a common problem in the industry. Techniques based on the use of multi-factor authentication (see ITU-T X.1254) as a means to enhance password security fail to address phishing based attacks due to their lack of mutual authentication capabilities.

The FIDO protocol as detailed in ITU-T X.1277 and ITU-T X.1278 is based on the use of ITU-T X.509 certificates which develop a protocol for enhancing the security of authentication through the use of public / private key pairs. The FIDO set of protocols support multi-factor authentication (MFA) and public key cryptography. The FIDO protocols use ITU-T X.509 standard public key cryptography techniques to provide very strong authentication solutions. The authentication process starts with a registration step between the user and an online service. During this step, the user's client device creates a new key pair. It retains the private key on the user's device stored in a secure element on the device and registers the public key with the online service. The authentication step is done locally at the device. The authentication step allows the FIDO agent on the device to prove possession of the private key to the service by signing a challenge. The client's private keys can be used only after they are unlocked locally on the device by the user. The local unlock is accomplished by a user friendly and secure action such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second–factor device or pressing a button.

The FIDO protocols are designed from the ground up to protect user data and authentication information. The protocols do not share information about a user since the task of authenticating to get access to the private key on a device is local to that device. Biometric information, if used, does not leaves the user's device.

The universal second factor protocol (U2F) augments the security of existing password authentication mechanisms by adding a second non-phishable factor to the user login. A user logs on using a username and a password, while the protocol prompts the user to present a second factor device for authentication.

The UAF protocol offers true password-less authentication. The UAF protocol is utilized by two entities the service provider that requires a user's authentication and a user that must be authenticated. The relying party (or service provider) in general consists of a web server that provides a front-end interface to users (a mobile server in case of mobile applications), and a FIDO server which handles UAF protocol messages to a user's device. On the client side, the users' computing entity consists of one or more UAF authenticators, the UAF client and user agent software. The UAF protocol delivers many improvements over traditional password based authentication mechanisms. UAF relies on public key cryptography which leads to strong authentication. UAF simplifies user registration and authentication steps. UAF eliminates the need for maintaining passwords which eliminates the need of a user to deal with complex password rules, or going through password recovery procedures. User data stays on the local device which strengthens the user's personal data protection, since all important information is stored locally, on the user's device.

4.6.3 Business benefits

The use of a user name and password in today's online interactions presents a security risk to users and relying parties. A quick examination of major breaches reveals a usual theme: in almost all security breaches, the attack vector has been the breach of some shared secret such as the common password. It is no wonder that the password is considered by far the weakest link in cybersecurity systems. The use of ITU-T X.1277 and ITU-T X.1278 help to eliminate one of the highest risks facing users and businesses on the Internet in terms if cybersecurity fraud, data leakage, account take over, intellectual property theft and financial loses to institutions.

The task of reducing fraud, data breaches, data loss prevention and protection of information security requires the use of strong authentication methods. Current MFA solutions improve on the security of basic password based authentication systems, but in general they are still vulnerable to phishing and man in the middle attacks. The improved security for MFA solutions comes at the expensive of usability and increased friction to end consumers. Balancing of security and usability in particular in a world with increased adoption of mobile devices is an important aspect of a strong authentication solution. In this regards, the protocols in ITU-T X.1277 and ITU-T X.1278 do figure as means of bringing the benefits of PKI security in a usable and user friendly manner.

4.6.4 Technologies involved

The ITU-T X.509 solution as presented in ITU-T X.1277 and ITU-T X.1278 help protect against the security risks for using a shared secret for the purpose of authentication. It particular it addresses the following threats to password based authentication solutions:

1) Phishing and key-loggers:

   Phishing is one of the most successful methods a hacker can use to steal a user password and to circumvent one–time based token (OTP) solutions. Malware solutions that install a key logger on a user device can steal user credentials regardless of whether the password was encrypted or hashed before sending it to the relying party. These methods provide great benefit to hackers since the intruder will be able to capture a password irrespective of how long or complex the password is.

2) Credential stuffing attacks:

   In this form of an attack, the intruder will re-use a phished credential across the sites that the victim usually visits or interacts with. Since most sites will allow the use of an email as the user ID and most people re-use the same password across sites, this type of attack has a great chance of succeeding.

3) Password cracking:

   Passwords require the use of a data store for storing them. Many measures can be used to secure the data store including the task of salting and encrypting the password. However,

the data store becomes the honey pot that attract intruders. These data stores get hacked and the hackers can then use brute force techniques recreate the stolen password. These types of attacks can usually succeed against systems that allow the use of weak passwords and that deploy weak data protection security such as weak slat and hash algorithms.

4) Account takeover:

Account takeover through the use of a password reset is a serious threat to password based systems. In particular to those systems that rely on knowledge based authentication for account recovery. Unfortunately, the task of securing passwords through the demand of using complex passwords results in an increase in password reset attempts by users which in general leads to more vulnerabilities as related to account takeover. Account takeover is a serious threat to user and relying parties.

5) Passwords hygiene:

Users tend to re-use passwords in an attempt to address the ever-increasing number of accounts that they need to manage. Security rules that require the use of complex passwords do not help to protect the users since this encourages password re-use.

6) The problem of default passwords:

Many equipment items such as routers and switches come with a default password that does not require the user to change it during setup. This results in security problems for many devices that that can be hacked by intruders with minimum effort.

The problem with passwords is that they are based on the use of a shared secret. Password based solutions assume that security is achieved through keeping the password secret. These systems rely on the user for validating the authenticity of relying party sites, which in return make the user the security weakest link. Traditional systems realized the above limitations and attempted to solve them with variable degrees of success by using some of the techniques as described below:

1) Multi-factor authentication (MFA):

A variety of two or more factors from different categories (something you know, something you have and something you are) can be made required in addition to standard password authentication to enhance authentication strength. The inclusion of an additional factor of authentication such as an out of band token (for example a PIN via email or short message service) can increase security at the expense of poor user experience. However, due to lack of mutual authentication in the MFA solution, they are still susceptible to man in the middle.

2) Single sign-on and federated solutions:

Some organizations can increase security through the use of federated or single sign-on solutions. Such systems enable the re-use of strong authentication to protect federated accounts. Such solutions are better suited for organizations and not very practical for consumer based systems. Although there is the benefit of enhanced security for federated accounts, they suffer from a significant security threat if the main account is compromised since it means that the security of the whole federation has fallen.

3) Account monitoring and lock out:

Account monitoring is one means of enhancing on password based security solutions. This technique can be used to foil brute-force attacks in particular if throttling is also used to limit the number of attempts an intruder can launch against the system.

4) Behaviour analysis:

Behavioural techniques can detect when an account has been compromised since it will be harder for an intruder to mimic the actions usually taken by a legitimate user. Behaviour can be coarse measures such as the time of day or the geographic location of access patterns or fine coarse such as the expected applications the users can invoke or interact with to

perform their daily work. Behaviour analysis is a secondary means of authentication and is defensive in nature with the aim or reducing the damage once a system has been compromised.

The problems of password based systems is their lack of inherent mutual authentication at the time of access. The dynamics of shared secret authentication work is depicted Figure 3.

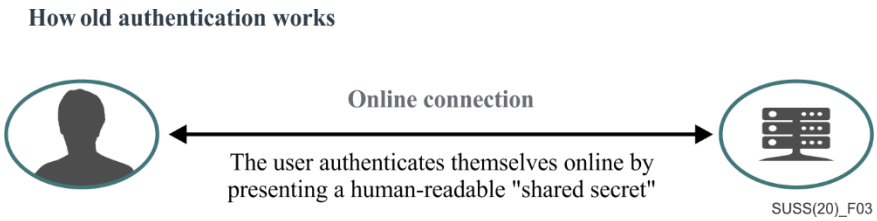

Figure 3 – Shared secret authentication

The work in ITU-T X.1277 and ITU-T X.1278 builds on ITU-T X.509 to transform the authentication process into a method that is based on public key cryptography (PKI) as depicted in the Figure 4.

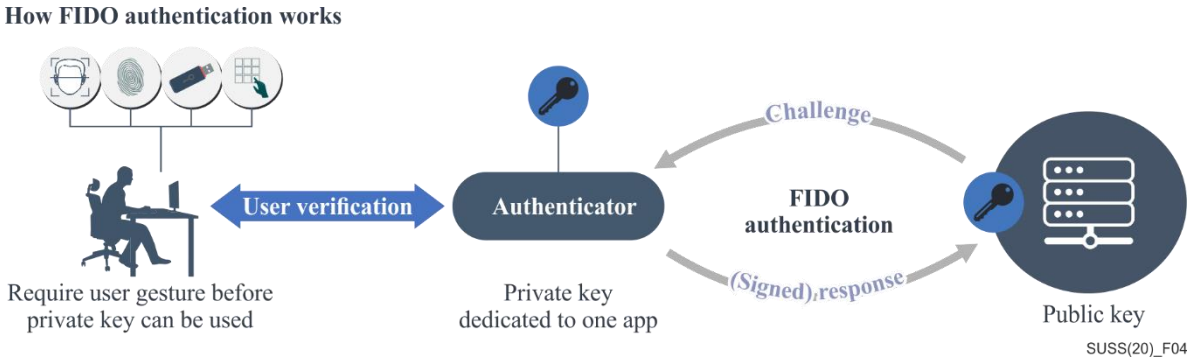

Figure 4 – FIDO authentication

In this process, the user authenticates to a local authenticator using a PIN, fingerprint or facial biometric to validate itself to the local device. These local authenticator stays on the device and is never shared with a relying party. Local authentication is used to proove possession of a private key that is stored on a secure element in the device. During authentication, the relying party sends a one-time challenge to the FIDO authenticator on the device, if local authentication succeeds then the challenge is signed by the private key on the device and is sent back to the relying party. This overall operation of FIDO provides the equivalence of mutual authentication between the user device and the relying party. The FIDO authenticator checks that the requesting relying party ID matches the registered ID of the private key associated by the application. This way, the FIDO protocol eliminates the success of phishing attacks since the check of the correct origin source request is built by the protocol. This flow assumes that device is capable of supporting a secure element topology. The protocol is described in ITU-T X.1277.

In some cases, the device is not capable of providing a hardware based secure element for storing the FIDO private keys. For these types of devices (and in general for any device with added security requirements) ITU-T X.1278 provides the universal second factor protocol (U2F) that enables the deployment if an external security key to store the private key (it basically allows an external device to act as a secure element).

Regardless of which protocol is being used (ITU-T X.1277 or ITU-T X.1278) FIDO authenticators are provisioned on user's device (or external key) through an enrolment step. Current deployments

are based on the user name password flow to credential the FIDO. Once the user is authenticated a FIDO credential is written on the local device. The FIDO flow is then used for authentication and replaces the typical user name password flow. The FIDO flow essentially replaces the password flow to a local authentication flow and on some cases, this is called password-less authentication.

The benefits of a FIDO based solution as specified in ITU-T X.1277 and ITU-T X.1278 are depicted in Figure 5.

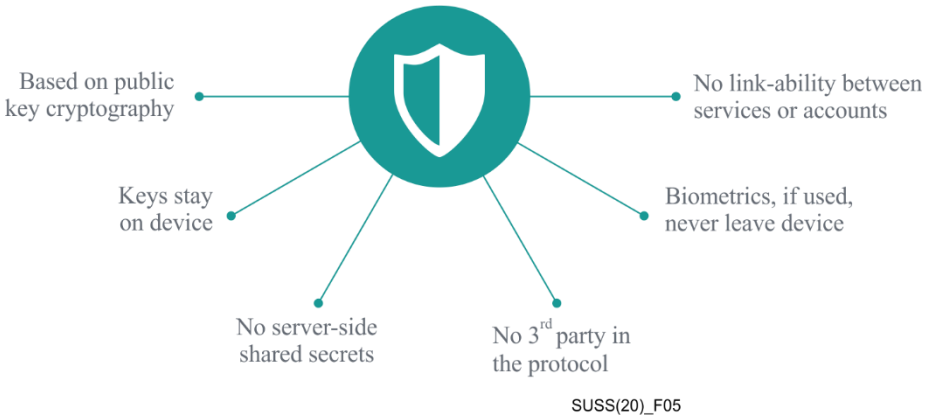

Figure 5 – FIDO benefits

The FIDO solution protects the user's identity related data. The solution provides users protection from linking their accounts across business relationships. Biometric data is local to each device that is used by the user. Private keys never leave the user device or external hardware key in the case of U2F.

4.6.5 Adoption and market acceptance

The FIDO protocols (ITU-T X.1277 and ITU-T X.1278) including the W3C WebAuthn are gaining great momentum in the market place. Support and adoption is increasing. There is a strong push in the industry for supporting password-less authentication.

The finalization of WebAuthN and CTAP meant that major browsers will have built in native support for FIDO authentication on the browser for those devices with the ability to support secure hardware modules such as trusted platform module (TPM), (also known as ISO/IEC 11889). As of today all major browsers are supporting FIDO through WebAuthN. This means that there are billions and billions of devices with native FIDO support.

FIDO is also supported on mobile operating systems by major vendors. Android versions 4.2 and higher has had native support for FIDO and in particular FIDO U2F (ITU-T X.1278). With the finalization of WebAuthn all major Android and IOS will be providing native support for this FIDO protocol. This is a big improvement since the mobile browser will act like a native mobile application of these platforms. Any FIDO credential on these devices will be able to be accessed by the issuing relying party regardless of which is invoked by the user. An important benefit of using FIDO in this fashion is that native fingerprint, facial recognition and other biometric capabilities on Android or IOS will be for the first time available to web based applications. This is important since it allows the same secure credentials to be used by both native applications and web services. This means that a user only has to register their fingerprint with a service once and then the fingerprint will work for both the native application and the web service.

4.7 Decentralized digital identity

Recommendations ITU-T X.1252 and ITU-T X.1403

4.7.1 Who does this standard affect?

Recommendation ITU-T X.1252 provides a taxonomy of digital identity terms and definitions. It also provides a reference framework for the use and adoption of digital identity in identity and access management systems.

Distributed ledger technology and its specific implementations such as blockchain offer a unique opportunity for utilizing a trust infrastructure and a platform that could be useful in enabling trusted federation for exchanging identity attributes and identity information. Recommendation ITU-T X.1401 provides telecom-specific privacy and security considerations for using DLT data in identity management.

4.7.2 Summary of standard

Recommendation ITU-T X.1252 defines what is digital identity for online systems. The work in ITU-T X.1252 takes a close look on how digital identity is currently used in various identity and access management systems (IAM). The work defines digital identity as used in centralized IAM systems and also decentralized systems that could be based on distributed ledger technologies or not.

Recommendation ITU-T X.1252 originally focused on defining digital identity for centralized IAM systems. However, due to the emergence of distributed ledger technologies the work was expanded to include digital identity definitions and models to cover decentralized identity bases systems. The work in ITU-T X.1252 is intended to present a ubiquitous taxonomy to be used by standardization bodies when referencing identity terms.

Recommendation ITU-T X.1403 on the other hand take a closer look at the use of decentralized identity in distributed ledger systems. Recommendation ITU-T X.1403 also takes a closer look at security risks associated with using distributed ledgers for identity data. It provides guidelines for storing identity data on ledger and off ledger. The work develops the foundation of hybrid identity and access management systems that will be needed to be adopted by the future enterprise in order to capitalize on the advances in decentralized identity based systems.

4.7.3 Business benefits

Decentralized identity systems (for example, self-sovereign identity (SSI)) are gaining a lot of momentum in the market place. The foundation of SSI is based on using ledgers as a holder for a digital address that stores a public private key pair to map to a user digital identity. The user in this case proves their identity by proofing that they control the private key associated with the public key of the physical location on the ledger. W3C have standardized decentralized identifiers (see W3C DID) as a standard method to expose decentralized identity on any ledger.

Centralized digital identity is composed of an identifier associated with a set of attributes. Decentralized identity on the other hand is the compilation of all identities (i.e., identifiers and attributes) that extends to all of decentralized domains that a user or individual is in full control of (see Recommendation ITU-T X.1252). For this reason, decentralized identity provides many benefits to end users.

Decentralized identity systems offer end users the promise of better control of their identity data. In particular, the way data is shared, used and who is asking for it and for what reason. Security of end users is also improved, since users need to be involved in the act of access control. In particular, a user needs to prove the control of a private key before identity based services can be performed. This is in sharp contrast to shared secret authentication methods such as user name and password systems that allow an authentication to occur without user participation in the process.

From a business perspective, decentralized identity also provides many benefits to the enterprise. First it offers the opportunity to use a stronger form of no password authentication to end users through the use of mobile devices and digital wallets. The added security translates to reduced risk

for the enterprise of losing customer data. The enterprise also benefits from the reduction of cybersecurity attacks by hackers targeting centralized data stores for the purpose of stealing passwords and user data.

4.7.4 Technologies involved

Distributed ledger technologies (DLTs) (including blockchain) use hashing techniques and digital signatures that are based on public key infrastructure (PKI) (see ITU-T X.509). PKI based systems anchor their trust on a certificate authority (CA). Traditionally, public certificates are used to trust the identity of the holder as asserted by the issuer. So, in a way the certificate is an identity assertion mechanism.

In DLT the trust in the ledger is a function of the security model of the ledger (permissioned, public or a combination of both). In DLT PKI is used to ensure the integrity of the transactions and data. Centralization of PKI is not a requirement. Anonymity of identity, authenticity and integrity of the transaction are met in DLT using ITU-T X.509. DLT represents a very interesting use case of the applicability of ITU-T recommendations and their adaptability to be used in centralized or decentralized systems.

W3C DID and verifiable credential specification also build on the use of ITU-T X.509 and PKI systems to develop a solution that uses private and public keys to assert trust in identity based interactions. W3C DID promotes trust in online interactions by developing technologies that can help entities to assert their on-line identities through the demonstration of them and of the private key of a private-public key pair system. The verifiable credential work allows the user the ability to present trustable assertions to a requesting party that could be validated anonymously using public keys of the issuer. All of these advances are based on Recommendation ITU-T X.509.

4.7.5 Adoption and market acceptance

The adoption of DID and verifiable credentials (VC) solutions in the market place is at an early stage. All indications point towards wider acceptance in the market place. Interoperability is key for successful implementation, in particular, for mobile deployments that are based on digital wallets. In the world of decentralized identity, identity related data gets stored in a digital wallet that could be stored on a smartphone. Everyone in a decentralized identity system can issue, receive, and validate credentials that contain individual claims. Decentralized identify platforms will be able to make these interactions possible without storing personal data outside of the digital wallet.

At this stage, there are at least three types of decentralized identity adoption:

1) Self-sovereign identity systems:
   - Self-sovereign identity (SSI) systems are based on distributed ledgers with a view to operate as general-purpose identity systems. The preferred trust model is based on non-permissioned public ledgers such as Bitcoin, Ethereum, or the Sovrin network. Interoperability among those systems is based on the work that is currently being done at the Hyperledger project including the Hyperledger Indy project.
2) Enterprise adoption:
   - Internal enterprise adoption at this early stage is focused on decentralized identity implementations based on private permissioned ledgers. The main focus in on improving the security of identity life cycle management including improved user experience with know your customer (KYC) during account creation, recovery and deletion in particular in support of the password-less authentication systems. In these implementation, the enterprise either alone or in collaboration with additional trusted partners can be an issuer or a verifier of identity related data.
3) Coalitions, alliances and user claimed identity systems:

– Members of an alliance collaborate together to form trusted identity echo system that can enroll users. The coalition members join as issuers and verifiers and use a permissioned ledger to share verified credentials. Applications include KYC for on-boarding customers. In some instances, some implementations allow users to jump start their identity through the issuance of un-verified identity claims. The system allow the user to gain better credibility through participation in the identity echo system where there will be opportunities for a trusted issuer to validate the self-asserted identity of a user.

4.8 Entity authentication assurance framework

Recommendation ITU-T X.1254, Entity authentication assurance framework

Recommendation ITU-T X.1254 defines three entity authentication assurance levels (AAL1 – AAL3). Concerning the threats for each of the three levels, the Recommendation:

– specifies a framework for managing the three assurance levels;

– provides guidance concerning control technologies that are to be used to mitigate authentication threats, based on a risk assessment;

– provides guidance for mapping the three levels of assurance to other authentication assurance schemas; and

– provides guidance for exchanging the results of authentication that are based on the three levels of assurance.

The Recommendation has been updated to reflect latest advances in passwordless technology that includes the work defined in ITU-T X.1277 and ITU-T X.1278.

4.8.1 Who does this standard affect?

This work affects organizations that are developing products, profiling application security, or deploying security solutions that require authentication. This work affects the foundation of authentication technology at all levels since it applies to entities that could be human, devices, applications or processes. The work provides foundation for performing appropriate secure identity federation, trust relationships and a consistent means for evaluating authentication threats for online transactions. The work is applicable to centralized and decentralized identity models, including distributed ledgers technologies.

4.8.2 Summary of standard

Recommendation ITU-T X.1254, *Entity authentication assurance framework*, defines three levels of entity authentication assurance and the criteria and threats for each of the four levels. A digital identity is the unique representation of an entity engaged in an online transaction. Assurance or confidence, that the digital identity with which one is interacting is consistent with the claimed identity, lies at the heart of online trust, security and access control. Three types of assurance are identified in this Recommendation to contribute to establishing trust in a digital identity: identity assurance, authentication assurance and federation assurance.

Recommendation ITU-T X.1254 provides a framework for authentication assurance. For the purposes of this Recommendation, authentication is the process by which a claimed identity is verified for the purpose of conducting an online transaction. For services in which return visits are applicable, a successful authentication provides reasonable risk-based assurances that the user accessing the service today is the same as that which accessed the service previously.

It is necessary to understand how the services that address the phases and functional components of the digital identity lifecycle interact with each other to support trust and the overall confidence in an online transaction. Such trust is typically expressed as the level of confidence through degrees, or levels of assurance. Recommendation ITU-T X.1254 provides requirements and guidance for the

digital identity authentication assurance phase and component functions of an overall digital identity and authentication assurance framework. Figure 6 depicts the components and describes the three types of assurance:

Assurance component	Descriptions	Activities

IA *Identity assurance*	Robustness of the identity proofing process and the binding between the authenticator and the identity-proofed individual.	• Identity proofing
		  • Resolution
		  • Validation
		  • Verification
		• Enrollment
		• Binding

AA *Authentication assurance*	Confidence that a given claimant is the same as the previously authenticated subscriber.	• Authentication
		• Credential management
		  • Credential issuance
		  • Credential suspension, revocation, and/or destruction
		  • Credential renewal and/or replacement

FA *Federation Assurance*	Combines aspects of the federation model, assertion protection strength, and assertion presentation	• Key management • Runtime decisions • Attribute management

SUSS(20)_F06

Figure 6 – Identity, authentication and federation assurance

– **Identity assurance**: Refers to the processes put in place to verify a subject's association with their real-world identity. Identity assurance is addressed in ISO/IEC TS 29003.

– **Authentication assurance**: Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate. Authentication assurance refers to the processes used to verify that a claimed identity is the same as the one that participated in the registration process and has previously authenticated to the system.

– **Federation assurance**: Refers to the process(es) used to communicate, protect and validate identity assertions being provided across different security domains. Identity federation is the sharing of online identity and authentication information between two or more parties.

4.8.3 Business benefits

An effective identity management system depends on understanding the levels of risks associated with the types of online services offered by the organization. To understand these risks, online service providers can use ITU-T X.1254 concepts to better understand their specific role(s) within their business framework; the nature of their users; and, the types of data and transactions processed by their applications.

Application of structured risk management methodology will result in the following: the identification of risks and threats; decisions as to how they should be treated; and, the inputs needed to select and implement controls. In the area of identity management, specific guidelines exist to help organizations understand how those levels of risk equate to levels of assurance; that is, to the relative degrees of confidence in the integrity of online identities.

Standardizing authentication assurance levels across business and domains enable the secure exchange of data across parties. It reduces fraud, identity theft and the ability of hackers to compromise organizations. When organizations use common standards for authentication assurance, federation and cross business interactions can be conducted in a more secure fashion.

4.8.4 Technologies involved

The standard provides a layered security architecture that is independent from any specific implementation.

4.9 Common alerting protocol

Recommendation ITU-T X.1303bis, Common alerting protocol (CAP 1.2)

4.9.1 Who does this standard affect?

Many integrated public alert and warning systems (IPAWS) are based on this protocol. This protocol touches millions of people on daily basis since it is the foundation for passing warning messages.

Cities and countries can reduce the effect of damage and loss of life if alerts are issued in a timely and appropriate manner. To be effective alerts should reach everyone who needs them. To be economical, many alerting authorities rely on public media and common alerting protocol (CAP) leverages online public media for cost reduction. So CAP affect all agencies that need to alert people and effect all people that rely on those life saving messages.

4.9.2 Summary of standard

The common alerting protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. CAP also provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

Recommendation ITU-T X.1303bis also provides both an XML schema definition (XSD) specification and an equivalent Abstract Syntax Notation 1 (ASN.1) specification (that permits a compact binary encoding) and allows the use of ASN.1 as well as XSD tools for the generation and processing of CAP messages.

CAP defines a digital message format that is compatible with a wide range of existing data networks including TV and radio networks. This Recommendation enables existing systems, such as Recommendation ITU-T H.323 systems, to more readily encode, transport and decode CAP messages.

4.9.3 Business benefits

Standardizing warning messages enable users across any telecommunication network get accurate messages and instructions during all kind of emergencies. CAP allows countries and agencies to reduce the cost and complexity of disseminating emergency signals. Cost reduction can be achieved when an alerting agency can use one CAP message to activate multiple alerting systems with a single input. Additionally, when using CAP protocol by an agency, it can achieve consistency of messaging over multiple channels thus allowing good validation of alert information. CAP is useful for multilingual and special-needs populations.

4.9.4 Technologies involved

The standard provides a layered security architecture that is independent from any specific implementation.

This standard is dependent on ASN.1 technologies.

4.9.5 Adoption

CAP is adopted worldwide. There is a CAP profile per country that can be registered at the World Meteorological Organization (WMO). WMO Technical Regulations, an international framework for standardization and interoperability, consists of standard and recommended practices and procedures adopted by the World Meteorological Congress for universal application by all Members. The CAP register of alerting authorities is established by WMO and ITU-T. WMO Member countries register alerting authorities they recognize and WMO Permanent Representative designates editors to maintain entries.

4.10 Access control markup language (XACML)

Recommendations ITU-T X.1142, *eXtensible Access Control Markup Language (XACML 2.0)*, and ITU-T X.1144, *eXtensible Access Control Markup Language (XACML) 3.0*.

XACML stands for "eXtensible Access Control Markup Language". The standard defines a declarative fine-grained, attribute-based access control policy language, architecture, and a processing model describing how to evaluate access requests according to some rules defined in an enterprise policy repository.

4.10.1 Who does this standard affect?

This standard plays an important role within organizations to provide real-time role-based access control to protect access to all types of resources within any organization.

A major goal of the XACML standard is to encourage the use of common terminology and interoperability between access control implementations as offered by independent vendors. XACML is primarily an attribute based access control (ABAC) system, that provides the ability to include input attributes in the task of evaluating decisions of whether a given user may access a given resource in a particular way at a specific time. Role-based access control (RBAC) can also be implemented in XACML as a specialization of ABAC.

The XACML encourages the separation of the access decision from the point of where those decisions will be used. In this way, it encourages the decoupling of any client from access decision points within the architecture, thus enabling authorization policies to be updated on the fly and in force at all clients immediately.

4.10.2 Summary of standard

Recommendations ITU-T X.1142 and ITU-T X.1144 define the core XACML including syntax of the language, models, context with policy language model, syntax and processing rules. To improve the security of exchanging XACML-based policies, Recommendations ITU-T X.1142 and ITU-T X.1144 also specify an XACML XML digital signature profile for securing data. A privacy profile is specified in order to provide guidelines for implementers. XACML is suitable for a variety of application environments.

Recommendation ITU-T X.1144 which is equivalent to OASIS XACML 3.0 improves the features regarding custom categories, content element, XACML request and response, and XML path. In addition, this Recommendation defines new datatypes and functions: advice elements, policy combination algorithms, scope of XPath expressions, target elements, and variables in the obligation and advice element.

4.10.3 Business benefits

Recommendations ITU-T X.1142 and ITU-T X.1144 are essential for organizations that are trying to build a modern security infrastructure that can enforce risk based access control to protect resources against illegal access.

XACML is an XML based language. Since it is based on XML it is also human readable. This in turn enables users to get an understanding of what it is doing. XACML is designed to be eXtensible where developers can add profiles to cater for specific business requirements and use cases. It is an optimized language for enforcing access control policies that are used in authorizing who can access what and when and for how long.

4.10.4 Technologies involved

The standard provides a layered security architecture that is independent from any specific implementation. XACML provides the following capabilities:

– a flexible architecture that can be plugged into existing policy enforcements frameworks within organizations;
– a modern rich and verbose policy language with the ability to express access control rules in a standardized, interoperable, way;
– a request / response language with build in mechanisms to enable a client to ask questions and to receive an answer in a standardized way; and
– the ability to work in tandem with SAML (Recommendation ITU-T X.1141) in a manner to allow the enforcement of polices and access control in a federated way.

This standard is XML and JSON Web Tokens (IETF RFC JSON) based.

4.11 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

Recommendation ITU-T X.1051, *Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

4.11.1 Who does this standard affect?

For the most part, ITU-T security-related Recommendations focus on the technical aspects of systems and networks. Additionally some aspects of personnel security are identified in Recommendation ITU-T X.1051.

4.11.2 Summary of standard

Recommendation ITU-T X.1051 establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in telecommunications organizations and provides an implementation baseline for information security management to help ensure the confidentiality, integrity and availability of telecommunications facilities and services.

Specific guidance for the telecommunication sector is included on the following topics:

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

– information security aspects of business continuity management; and
– compliance.

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

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

4.11.3 Business benefits

Recommendation ITU-T X.1051 is essential for organizations affected by information security vulnerabilities. The Internet has affected how business is conducted in the business world. Networking, distributed systems and the cloud have facilitated the task of doing business at a global scale. Cyber-attacks are becoming increasingly targeted and coordinated. These attacks have changed the nature of security risks and threats in area such as:

– Unauthorized access to confidential or private data;
– Unauthorized release of protected information;
– Theft of intellectual property rights and innovations;
– Unauthorized changes of information accuracy;
– Destruction of public, personal and organizational reputation and credibility;
– Disruption or prevention of critical public and private online services.

Information and data are one of the most valuable assets for organizations. As such, this data must be protected in a fashion that enables an organization to pass compliance and ethical tests. Organizations should be able to secure device information security management principles, process, and controls to ensure the protection of critical data and infrastructure.

Recommendation ITU-T X.1051 helps organizations to manage risk and security in a manner that allows it to compete in the new digital economy.

4.11.4 Technologies involved

The standard provides a security approach that is independent from any specific implementation.

4.12 Interactive gateway system for countering spam

Recommendation ITU-T X.1243, *Interactive gateway system for countering spam*.

4.12.1 Who does this standard affect?

Technology collaboration has been recognized as a key component in countering spam. Recommendation ITU-T X.1243 illustrates such a system and specifies a technical means for countering inter-domain spam.

The gateway system enables spam notification among different domains, and prevents spam traffic from passing from one domain to another.

Technological advances have virtually eliminated the marginal costs from e-mail communications. This accomplishment means that a few individuals can exploit this efficiency to create a large problem of spam for a wide range of organizations and individuals.

Today's spam problem has generally been characterized as a cost for businesses – creating losses in productivity and requiring investments in more hardware and filtering software. These costs are significant, yet they have been generally characterized as a cost of doing business, and nothing more.

4.12.2 Summary of standard

The Recommendation specifies the architecture for the gateway system, describes basic entities, protocols and functions of the system, and provides mechanisms for spam detection, information sharing and specific actions for countering spam.

Spyware and other deceptive software (e.g., software that performs unauthorized activities) 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. 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 usage. ITU-T X.1243 provides an effective framework for managing and combating spam.

4.12.3 Business benefits

Spam can create a significant burden for network operators. The problems associated with spam are magnified in developing countries, where high volumes of incoming and outgoing spam can cause a large drain on the limited bandwidth that is available in those regions. Spam also represents a significant problem for organizations, email users and operators. Additionally, spam represents an effective vehicle for phishing attacks that result in identity theft and fraud.

Today's spam problems have generally been characterized as a cost for businesses – creating losses in productivity, requiring investments in more hardware, and filtering software.

Recommendation ITU-T X.1243 enables providers and organizations to develop systems that effectively work towards filtering and blocking unwanted spam, thus reducing organizational costs and overheads.

4.12.4 Technologies involved

The Recommendation is technology neutral since it does develop a framework for integrating various technologies that can be combined together for the effective combat of spam.

4.13 Abstract Syntax Notation One (ASN.1)

Abstract Syntax Notation One (ASN.1) specific Recommendations:

– Recommendation ITU-T X.680 | ISO/IEC 8824-1, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

– Recommendation ITU-T X.681 | ISO/IEC 8824-2, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.

– Recommendation ITU-T X.682 | ISO/IEC 8824-3, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.

– Recommendation ITU-T X.683 | ISO/IEC 8824-4, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.

Encoding rules Recommendations:

– Recommendation ITU-T X.690 | ISO/IEC 8825-1, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*

– Recommendation ITU-T X.691 | ISO/IEC 8825-2, *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER).*

– Recommendation ITU-T X.693 | ISO/IEC 8825-4, *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER).*

– Recommendation ITU-T X.694 | ISO/IEC 8825-5, *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1*.

– Recommendation ITU-T X.695 | ISO/IEC 8825-6, *Information technology – ASN.1 encoding rules: Registration and application of PER encoding instructions*.

– Recommendation ITU-T X.696 | ISO/IEC 8825-7, *Information technology – Specification of Octet Encoding Rules (OER).*

– Recommendation ITU-T X.697 : *Information technology – ASN.1 encoding rules: Specification of JavaScript Object Notation Encoding Rules (JER).*

4.13.1 Who does this standard affect?

ASN.1 is a formal notation used for describing data transmitted by telecommunications protocols, regardless of language implementation and physical representation of these data, whatever the application, whether complex or very simple. ASN.1 offers extensibility which addresses the problem of, and provides support for, the interworking between previously deployed systems and newer, updated versions designed years apart. ASN.1 sends information in any form (audio, video, data, etc.) anywhere it needs to be communicated digitally. ASN.1 only covers the structural aspects of information (there are no operators to handle the values once these are defined or to make calculations with). Therefore it is not a programming language.

Though initially used for specifying the email protocol within the Open Systems Interconnection environment, ASN.1 has since then been adopted for a wide range of other applications, as in network management, secure email, cellular telephony (including 3G, LTE and 5G), air traffic control, and voice and video over the Internet. Examples of ASN.1 use include:

– Audio and video over the Internet, electronic commerce, digital certificates, secure email, radio paging, interactive television, financial service systems, networking and computing operating systems use ASN.1 and its encoding rules.

– Third, fourth and fifth generation wireless communications technologies rely on ASN.1 for all the interactions between a mobile device and the carrier's network that make a cellular phone call possible and which support Internet connectivity from a mobile device.

– ASN.1 software is used in Internet browsers.

– ASN.1 is used in cryptography technology used to provide security for credit card purchases over the Internet. Biometrics, automatic money tellers, 800-number call routing to local carriers, plane take-offs and landings all rely on ASN.1. When FedEx tracks a package, it is done thanks to ASN.1.

– Millions of cars and trucks are produced every year using diagnostic monitoring systems that rely on ASN.1 for messages that are used in the detection of faults in production equipment and to dispatch maintenance personnel.

4.13.2 Summary of standard

Communication protocols describe the sequence, the content and the encoding of messages exchanged between computers communicating with each other. ASN.1 is a language for describing

the content and the encoding of each message. ASN.1 as developed by the ITU-T is a mature technology and concepts that are widely used in infrastructures that require efficient and fast communications. ASN.1 has explicit rules and instructions on how any given type of information must be encoded when transferred. ASN.1 is independent of the programming languages used to implement communications. ASN.1 is independent of any hardware or operating system. ASN.1 allows exchange of information among heterogeneous systems.

Recommendation ITU-T X.680 presents a standard notation for the definition of data types and values. A data type (or type for short) is a category of information (for example, numeric, textual, still image or video information). A data value (or value for short) is an instance of such a type. This Recommendation | International Standard defines several basic types and their corresponding values, and rules for combining them into more complex types and values. Recommendations ITU-T X.680 | ISO/IEC 8824-1, Recommedation ITU-T X.681 | ISO/IEC 8824-2, Recommedation ITU-T X.682 | ISO/IEC 8824-3, Recommendation ITU-T X.683 | ISO/IEC 8824-4 together describe Abstract Syntax Notation One (ASN.1), a notation for the definition of messages to be exchanged between peer applications. Rec. ITU-T X.690 | ISO/IEC 8825-1, Recommendation ITU-T X.691 | ISO/IEC 8825-2 and Recommendation ITU-T X.693 | ISO/IEC 8825-4 specify three families of standardized encoding rules, called basic encoding rules (BER), Packed Encoding Rules (PER), and XML Encoding Rules (XER).

Recommendation ITU-T X.690 defines a set of basic encoding rules (BER) that may be applied to values of types defined using the ASN.1 notation. Application of these encoding rules produces transfer syntax for such values. It is implicit in the specification of these encoding rules that they are also used for decoding. This Recommendation defines also a set of distinguished encoding rules (DER) and a set of canonical encoding rules (CER) both of which provide constraints on the basic encoding rules (BER). The key difference between them is that DER uses the definite length form of encoding while CER uses the indefinite length form. DER is more suitable for the small encoded values, while CER is more suitable for the large ones. It is implicit in the specification of these encoding rules that they are also used for decoding.

Recommendation ITU-T X.691 specifies a set of packed encoding rules that may be used to derive a transfer syntax for values of types defined in Recommendation ITU-T X.680. These packed encoding rules are also to be applied for decoding such transfer syntax in order to identify the data values being transferred. The encoding rules specified in Rec. ITU-T X.691:

– are used at the time of communication;
– are intended for use in circumstances where minimizing the size of the representation of values is the major concern in the choice of encoding rules;
– allow the extension of an abstract syntax by addition of extra values, preserving the encodings of the existing values, for all forms of extension described in Recommendation ITU-T X.680 | ISO/IEC 8824-1;
– can be modified in accordance with the provisions of Rec. ITU-T X.695.

Recommendation ITU-T X.693 specifies rules for encoding values of ASN.1 types using the extensible markup language (XML).

Recommendation ITU-T X.695 specifies the rules for applying PER encoding instructions using either type prefixes or an encoding control section. Encoding instructions are a means of modifying the encodings of ASN.1 types for some specified encoding rule (in this case PER). They can be inserted in an ASN.1 specification in square brackets (much like a tag in the Basic Encoding Rules, BER) immediately before the type that they affect (type prefixes), or they can be collected together at the end of an ASN.1 module (an encoding control section). It also specifies the procedures for developing, registering and publishing new PER encoding instructions from time to time.

Recommendation ITU-T X.696 | ISO/IEC 8825-7 specifies two sets of binary encoding rules that can be applied to values of all ASN.1 types using less processing resources than the Basic Encoding

Rules and its derivatives. Recommendation ITU-T X.697 specifies a set of JavaScript Object Notation Encoding Rules (JER) that may be used to derive a transfer syntax for values of types defined in Recommendation ITU-T X.680 | ISO/IEC 8824-1, Recommendation ITU-T X.681 | ISO/IEC 8824-2, Recommendation ITU-T X.682 | ISO/IEC 8824-3, Recommendation ITU-T X.683 | ISO/IEC 8824-4. It is implicit in the specification of these encoding rules that they are also to be used for decoding.

4.13.3 Business benefits

ASN.1 is a critical part of our daily lives. It is deployed in many sectors and industry verticals. It works in the background where a typical user will not be aware of its presence.

4.13.4 Technologies involved

ASN.1 improves on the efficiency of technologies where it can optimize the time it takes for any communication to occur between two end points and it acts to speed up response time. ASN.1 is efficient and can be deployed over any technology stack.

ASN.1 has been in use since 1984, but has been constantly upgraded to meet new demands. In 1988 it was improved to support ITU-T X.509 digital certificates, in 1995 it was improved to support bandwidth and CPU-constrained devices, and in 2002 it was improved to support XML. ASN.1 is used today in a wide range of applications and is deployed in well over a billion computers and embedded systems devices. Every time that you place an 800-number call ASN.1 is used. Every time you buy something on the web ASN.1 is used. Every time you send secure email, ASN.1 is used. Almost every time you use a multimedia product such as Microsoft NetMeeting, ASN.1 is in use. The latest generation of aviation control systems for ground-ground and aircraft-ground communications employs ASN.1. Companies such as Federal Express use ASN.1 in tracking their packages. ASN.1 is used by electric and gas utilities to control the latest generation of substations and transformers.

4.13.5 Technical implications

Many protocols have their implementation based on ASN.1.

1) Aviation

   Air-ground and ground-ground protocols employed by the Federal Aviation Administration and International Civil Aviation Organization are described in ASN.1 and are encoded in PER. The Aeronautical Telecommunication Network (ATN), which has been operational in Europe since 2007, is specified with ASN.1 and uses the compact PER encoding. ASN.1 encoders/decoders are now installed on American Airlines B767 aircraft in the certified ATN compliant avionics from Rockwell Collins.

2) Banking

   – The ANSI standard X9.84 (*Biometric information management and security*) provides strong identification and authentication in electronic communications across uncontrolled public networks, such as the Internet. In the X9.84 standard, the syntax for biometric technology types, processing algorithms, and matching methods are described using ASN.1. The standard strongly recommends that ASN.1 be used in open systems where biometric data is communicated between disparate computing platforms or vendor (biometric) software. Examples of biometric messages using both DER and PER encoding rules are provided.

   – In the USA, the ANSI X.9 committee, which numbers more than 300 members (banks, investors, software companies, and associations) is responsible for developing national standards to facilitate financial operations such as electronic payments on the Internet, secure on-line banking, business messaging, fund transfer, etc. All the standards describing these data transfers are specified in ASN.1.

3) Electronic cards and tags

- Radio-frequency identification (or RFID) is implemented in numerous industrial sectors (person or vehicle identification, stock management, etc.). The electronic tags are actually miniaturized radio emitters that can be read from a few centimetres to several metres off, even though obstacles that would prevent the use of barcodes, for instance.
- The ISO/IEC 7816-4 standard uses BER for exchanging data with integrated circuit cards with contacts. The majority of chip cards and smart cards used in Europe and in the US conform to this standard.

4) Energy

- Electric and gas utilities companies use ASN.1 and BER. ASN.1 and BER-encoded messages are used in controlling the latest generation of substations, transformers, RTU's and IED's, among others.

5) Graphics and file transfer

- In the context of the European research project ESPRIT 2, an application demonstration has shown how the Computer Graphics Metafile (CGM) and file transfer access and management (FTAM) standards can be used together to enable remote access to individual pictures within a CGM.
- There are eight MHEG (Multimedia and Hypermedia information coding Expert Group) object classes that are defined both in ASN.1 and in standard generalized markup language (SGML). These classes can transparently exchange objects encoded in many different formats (JPEG, MPEG, text, etc.), including proprietary formats. MHEG objects can be icons or buttons that trigger actions when clicked, and are independent of the application and of the presentation.

6) Asset management

ISO/TS 55010 and ISO 55001 define the requirements for a management system for asset management.

7) Health and genetics

- The ISO technical committee TC 251 in charge of Health Informatics at the European Committee for Standardization (CEN) published the ENV 12018 standard *"Identification, administrative, and common clinical data structure for Intermittently Connected Devices used in healthcare"* where the data structures are described in ASN.1.
- In the USA, the National Center for Biotechnology Information (NCBI) owns GenBank, a database featuring around 135 million DNA sequences (as of April 2011). Every day the NCBI exchanges deoxyribonucleic acid (DNA) sequence data with its European and Japanese counterparts. The National Library of Medicine designed four databases of scientific publications (the Unified Medical Language System, UMLS) whose exchange formats are specified in ASN.1.

8) Intelligent networks

ASN.1 is used in mobile telephony and wireless networks

- The universal mobile telecommunication system (UMTS), the third-generation cellular telephony technology developed by the 3GPP, heavily relies on ASN.1 and PER for the exchange of control messages between the mobile device and the base station and between different types of nodes within the mobile operator's radio access network.
- LTE, the fourth-generation cellular technology designed by the 3GPP as an evolution of UMTS, also uses ASN.1 for its control messages. So does LTE-Advanced, the successor of LTE.

– IEEE 802.16m, also known as WiMAX Version 2, the successor of IEEE 802.16e (WiMAX), is another wireless communications standard that uses ASN.1 and PER for its control messages.

– TAP3 (transferred account procedure) is the file format used by mobile network operators to exchange billing information about roaming subscribers. A TAP3 file contains charges for the use of the service by each roaming subscriber as well as customer care information to be used in case the subscriber contacts the mobile operator. The TAP3 format is specified in ASN.1.

9) Teleconferencing

– Many protocols related to multimedia are specified using ASN.1. Some examples are audiovisual and multimedia systems (ITU-T H.200 series), videophone over ISDN (Recommendation ITU-T H.320), real-time multimedia communication over the Internet (Recommendations ITU-T H.225, ITU-T H.245, ITU-T H.323), and fax over the Internet (Recommendation ITU-T T.38).

10) Videoconferencing

– In the domain of videoconferencing, the ITU-T T.120 series of ITU-T Recommendations describes a multithread architecture of data communications in the context of a multimedia conference. It describes the establishment of telephone meetings independent of the underlying network as well as the exchange of many types of data (binary files, still images, notes, etc.) among the participants during the meeting. The data protocol is specified in ASN.1 and the encoding is PER.

11) ASN.1 in Fifth Generation networks

5G (5^{th} generation wireless systems) is the newest phase of advanced mobile telecommunications standards with a large scope that extends from mobile broadband services, next generation connected vehicles and automobiles to massively connected devices.

At least two major trends are behind the push for deployment of 5G technologies:

– the increased demand for rich wireless broadband including video and other content rich services, and

– the Internet of things (IoT), where large numbers of smart devices communicate over the Internet.

To meet the above demands, 5G provides improved broadband speed, with low latency, and reliable web connectivity. 5G technology will consist of dense networks of small cells that will complement macro base stations, operating at millimetre wave technologies and employing massive MIMO antenna arrays. The processing components within network equipment and user devices will become more integrated and adaptive.

The fifth generation (5G) technology will fundamentally transform the role that telecommunications technology plays in online business activities. The variety of business models that 5G systems will be able to support enables telecom operators to develop numerous strategies to introduce 5G services. So each operator can choose a migration path from 4G and LTE towards 5G deployment.

Regardless of the migration path into 5G, the core technology will be built on top of core protocols with native support for ASN.1 operations. For example, many of the 3GPP 5G and LTE protocols such as RRC, S1AP, X2AP, NGAP, XnAP, E1AP, F1AP, and LPPa are defined using ASN.1. Table 1 is a partial list of 3GPP protocols using ASN.1:

Table 1 – 3GPP protocols using ASN.1

Name	Abbreviation	Technology
Radio resource control	RRC (UMTS)	UMTS
Radio access network application part	RANAP	UMTS
Radio network subsystem application part	RNSAP	UMTS
Node B application part	NBAP	UMTS
RANAP user adaption	RUA	UMTS
Home node B (HNB) application part	HNBAP	UMTS
Mobile application part	MAP	UMTS
CAMEL application part	CAP	UMTS
Handover interface for lawful interception	LI	UMTS
Radio resource control	RRC (LTE)	LTE
S1 application protocol	S1AP	LTE
X2 application protocol	X2AP	LTE
M2 application protocol	M2AP	LTE Advanced
M3 application protocol	M3AP	LTE Advanced
Radio resource control	RRC (NG)	5G
NG application protocol	NGAP	5G
Xn application protocol	XnAP	5G
E1 application protocol	E1AP	5G
F1 application protocol	F1AP	5G

12) PKI security

– ASN.1 in the PKCS group of cryptography standards, X.400 electronic mail, X.500 and Lightweight Directory Access Protocol (LDAP), H.323 (VoIP), Kerberos, BACnet, Simple Network Management Protocol (SNMP), and third- and fourth-generation wireless communications technologies (UMTS, LTE, and WiMAX 2)

13) Other protocols

– Since its creation in 1992, the ANSI Z39.50 protocol (ISO 10163-1 standard) has been specified in ASN.1 and encoded in BER. A variant of this protocol was used in the wide area information server (WAIS) service to make all kinds of information accessible on the Internet (library catalogues, directories, FTP archives, newsgroups, images, source code, multimedia documents, etc.). It provides facilities for keyword search, for extending a search by including new criteria to be applied to the documents already found, and for downloading selected documents. The Z39.50 protocol is mainly used in libraries and information centres.

– ASN.1 has appeared for quite a long time now in many requests for comments (RFC) that specify traditional Internet protocols. RFC 1189 (*The Common Information Services and Protocols for the Internet*, CMOT and CMIP) and RFC 1157 (*A Simple Network Management Protocol*, SNMP) are two alternative protocols allowing a network to control and evaluate the performance of a remote network element.

4.14 Cybersecurity information exchange framework

ITU-T Recommendations

– Recommendation ITU-T X.1500 / *Overview of cybersecurity information exchange* – Structured cybersecurity information exchange techniques

– Recommendation ITU-T X.1520 / *Common vulnerabilities and exposures* (CVE)

– Recommendation ITU-T X.1521 / *Common vulnerability scoring system* (CVSS)

– Recommendation ITU-T X.1524 / *Common weakness enumeration* (CWE)

– Recommendation ITU-T X.1525 / *Common weakness scoring system* (CWSS)

– Recommendation ITU-T X.1526 / *Language for the open definition of vulnerabilities and for the assessment of a system state*

– Recommendation ITU-T X.1528 series / *Common platform enumeration* (CPE)

– Recommendation ITU-T X.1544 / *Common attack pattern enumeration and classification* (CAPEC)

– Recommendation ITU-T X.1546 / *Malware attribute enumeration and characterization* (MAEC)

– Recommendation ITU-T X.1550 / *Access control models for incident exchange networks*

– Recommendation ITU-T X.1570 / *Discovery mechanisms in the exchange of cybersecurity information*

– Recommendation ITU-T X.1580 / *Real-time inter-network defence*

– Recommendation ITU-T X.1581 / *Transport of real-time inter-network defence messages*

– Recommendation ITU-T X.1582 / *Transport protocols supporting cybersecurity information exchange*

4.14.1 Who does this standard affect?

Cyber threat information gathering and sharing are crucial components of an organization's cyber security threat intelligence program. Cyber threat information can be obtained internally and from external sources through trusted channels.

The CYBEX Recommendations facilitate exchange of information across all stakeholders of cybersecurity. Examples of CYBEX use include:

– National coordination centres for cybersecurity make use of vulnerability information identifiers for public alerting purposes.

– Incident response teams efficiently keep track of vulnerabilities and attack patterns through a set of concise identifiers as predicated by CYBEX.

– System administrators assess presence of vulnerabilities using software tools that employ CYBEX.

– Cloud and network service providers keep track of vulnerabilities in their infrastructure, where they are prioritized according to impact, using the standardized scoring method.

– Embedded and IoT product developers learn typical patterns of software weaknesses through a public knowledge base that is also part of CYBEX.

– Vulnerability researchers collectively maintain knowledge bases of vulnerabilities, each of which can be linked and integrated through common vulnerability identifiers.

The focus of this set of Recommendations resulted from efforts in ITU-T SG17 for studying methods for:

– determining in real time the security integrity of systems and services, and

– collecting and maintaining relevant security incident data in a form suitable for sharing among information assurance, and incident response communities as appropriate.

The studies enabled ITU-T to create and adopt a cybersecurity information exchange techniques (CYBEX) initiative that for most organizations, whether they are owners, operators, or suppliers for critical infrastructure, can benefit from effective exchange of security threats with excellent chance of improving security postures and enhanced regulatory compliance. A guiding principle of the CYBEX framework is collaboration to share information and improve cybersecurity practices and threat intelligence.

4.14.2 Summary of standard

The Cybersecurity information exchange (CYBEX) framework is defined through a series of Recommendations that allows for continual evolution to accommodate the significant activities and specification evolution occurring in numerous cybersecurity forums, and consists of a basic exchange framework with the following extensible functions:

– structuring cybersecurity information for exchange purposes;
– identifying and discovering cybersecurity information and entities;
– requesting and responding with cybersecurity information;
– exchanging cybersecurity information;
– enabling assured cybersecurity information exchange;
– real-time inter-network defence.

The series of Recommendations describes ways in which a common understanding can be reached to enable assured exchange of information for responding to incidents and potentially reducing the risk and exposure caused by vulnerabilities.

The cybersecurity information exchange (CYBEX) framework is intended to accomplish a simple, limited objective, namely a common global means for cybersecurity entities to exchange cybersecurity information. Such entities typically consist of organizations, persons, objects, or processes possessing or seeking cybersecurity information. Most frequently, these entities are computer incident response teams (CIRTs) and the operators or vendors of equipment, software or network based systems.

The cybersecurity information exchanged is valuable for achieving enhanced cybersecurity and infrastructure protection, as well as accomplishing the principal functions performed by CIRTs.

The exchange of cybersecurity information typically occurs within highly compartmentalized trust communities until remedies are devised and available. At such times, knowledge of the threats, vulnerabilities, incidents, risks, and mitigations and the associated remedies are made public. The related specifications included in this framework are intended to facilitate these processes and thereby enhance cybersecurity.

This exchange process is depicted in Figure 7 as consisting of the following functions:

– structuring cybersecurity information for exchange purposes;
– identifying and discovering cybersecurity information and entities;
– requesting and responding with cybersecurity information;
– exchanging cybersecurity information;
– enabling assured cybersecurity information exchanges.

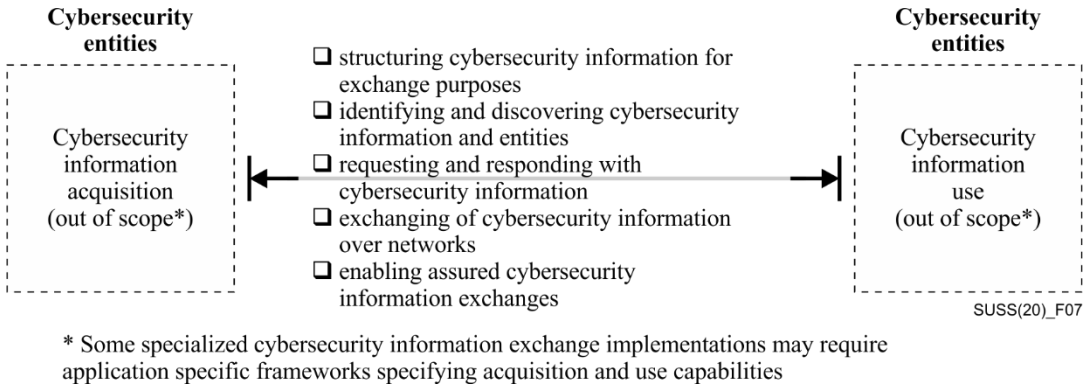

Figure 7 – Framework for the exchange of cybersecurity information

The exchange framework is bi-directional. This bi-directionality allows for verified information requests and responses to facilitate required levels of assurance between the parties or provide certification of delivery.

Subject to agreed policies, the means of acquiring information as well as the uses made of the information are generally out of scope and not treated in this Recommendation. However, some specialized cybersecurity information exchange implementations such as trace-back of attack sources may require application specific frameworks. Such implementations will provide acquisition and use capabilities applicable to that kind of exchanged information and allow for a recursive series of requests and responses to obtain required information. Such implementations also include making cybersecurity measureable and manageable, for example, through the use of security content automation capabilities.

This framework applies to the formats and mechanisms for the exchange of this cybersecurity information and does not mandate in any way its exchange.

4.14.3 Business benefits

Many CYBEX Recommendations are a critical part of cybersecurity operations, as they facilitate communications across diverse cybersecurity entities. They work in the background where a typical user will not be aware of their presence.

For most organizations, whether they are operators, suppliers or even owners of critical security infrastructure, the CYBEX framework well be worth adopting for its stated goal of improving the sharing of risk based security vulnerabilities. The CYBEX framework will deliver additional benefits that include enhanced collaboration and the open discussion of security issues among executives and industry organizations.

4.14.4 Technologies involved

CYBEX can be implemented over any technology stack. In particular, CYBEX can benefit from a modern Web technology stack that facilitates dissemination of information in general. Alternatively, specific implementation can avoid the use of Web-based technology altogether and still benefit from the common identifiers and data structures that are provided by CYBEX.

4.14.5 Technical implications

The CYBEX Recommendations are not dependent on any specific technology, although some of them make use of XML and HTTP. CYBEX is a modular set of Recommendations that broader stakeholders across diverse industries can benefit from, for instance by adopting the full set of Recommendations including exchange protocols, or by adopting part of the set of Recommendations that provide identification and enumerations of cybersecurity information.

4.15 Automotive cybersecurity standards

As vehicles become more autonomous and connect to networks such as the Internet, ensuring the security of their on-board systems has become a top priority for the car industry. ITU-T has a series of Recommendations that aim towards ensuring the security of the whole connected vehicle system. The list of ITU-T Recommendations that are under development for securing the connected vehicles ecosystem are provided below:

– Recommendation ITU-T X.1373 *Secure software update capability for intelligent transportation system communication devices.*

4.15.1 Summary of standard

Vehicle-to-everything (V2X) is a technology that allows vehicles to communicate with moving parts of the traffic system around them. It is also known as connected-vehicle-to-everything communication. The technology has several components.

– One component of this technology is called vehicle-to-vehicle (V2V) which allows vehicles to communicate with one another.

– Another component is vehicle to infrastructure (V2I) which allows vehicles to communicate with external systems such as street lights, buildings, and even cyclists or pedestrians.

The capabilities will expand as technology improves. The ITU-T SG 17 is focused on V2X technology. A summary of the ITU-T Recommendations are provided next:

Intelligent transportation system (ITS)

– Recommendation ITU-T X.1373 *Secure software update capability for intelligent transportation system communication devices*. This Recommendation focuses on secure software updates for intelligent transportation system (ITS) communication devices in order to prevent threats such as tampering of and malicious intrusion to communication devices on vehicles. It contains a basic model of software updates, presents a threat and risk analysis for software updates and gives the resulting security requirements and specifies an abstract data format for update software modules. The scope of the work is depicted in Figure 8:

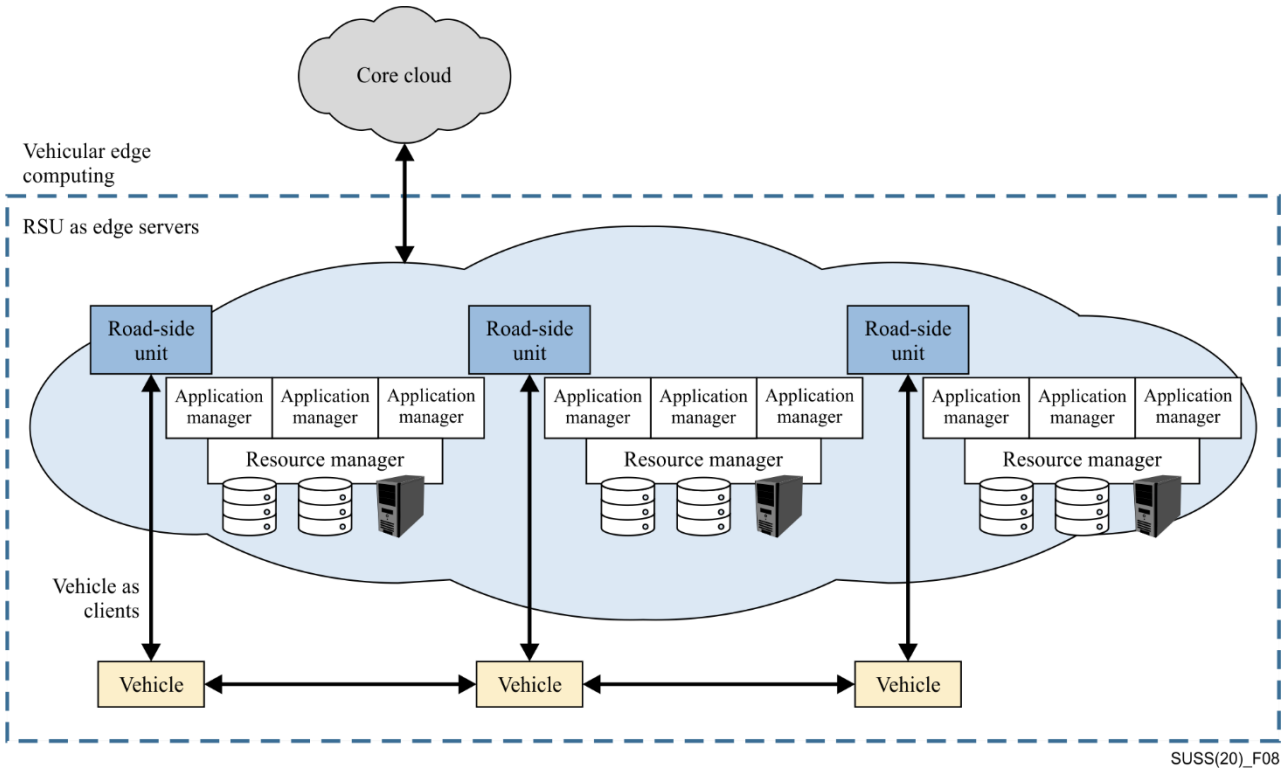

Figure 8 – Connected vehicle

4.15.2 Business benefits

One of the main goals of standardizing a connected vehicle framework is to provide the blue print for a uniform platform that can be used to secure all components in the automotive industry. The industry is new to the concept of connected vehicles and will learn a lot from the experience that is gained in securing current telecom networks.

4.15.3 Technologies involved

Current generations of vehicles deploy many software components in their systems. In many cases those vehicles are also connected to the Internet and external services. This connectivity make these vehicles vulnerable to various types of attacks. Threat modelling is a process that can be used to identify, analyze, and mitigate attacks against a system of interest. Since connected vehicles are new to the market, the maturity, understanding and the development of such threat models are still in their infancy. What is needed is an industry specific threat assessment and remediation analysis (TARA) and spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege (STRIDE), to fit the needs of the automotive industry.

The work on security Recommendations in the ITU-T provides all the foundation for the automotive industry to develop the needed TARA and STRIDE models. Recommendations ITU-T X.509, ITU-T X.805, ITU-T X.1205, ITU-T X.1254, ITU-T X.1277, ITU-T X.1278, ITU-T X.1373 and CYBEX represent a small number of Recommendations that enable creation of well understood and implementable threat models for the connected vehicle industry.

4.16 Security aspects for distributed ledger technologies

The following is a list of applicable Recommendations:

1) Recommendation ITU-T X.1401, *Security threats to distributed ledger technology*.
2) Recommendation ITU-T X.1402, *Security framework for distributed ledger technology*.
3) Recommendation ITU-T X.1403, *Security guidelines for using distributed ledger technology for decentralized identity management*.

4.16.1 Who does this standard affect?

ITU-T is developing a list of new Recommendations that enable the development of consistent threat models for evaluating the security of distributed ledgers. The new Recomemdnations will help in the use of exiting and proven technologies to be used in securing the newly emerging distributed ledger technology.

4.16.2 Summary of standard

One of the most disruptive technologies is distributed ledger technology (DLT), commonmy known as blockchains. The distributed ledgers are a new type of secure database or ledger, shared across multiple sites, countries, or institutions without any centralized controller or trusted third party. This new technology enables development of decentralized applications with no centralized control.

ITU-T Recommendation ITU-T X.1401, *Security threats to distributed ledger technology*, identifies security threats to the technology, categorized into protocols, networks and data. It provides descriptions of threats in terms of targeted components, attacks, attack impact, and attack likelihood. Based on the analysis of security threats, Recommendation ITU-T X.1402, *Security framework for distributed ledger technology*, derives security requirements and capabilities that could mitigate the threats and provides a methodology to develop a framework for a specific DLT application.

The emergence of DLT provides the opportunity for the development of decentralized identity management. Recommendation ITU-T X.1403, *Security guidelines for using DLT for decentralized identity management*, discusses security benefits of decentralized identity, introduces the concept of decentralized identity and an access management system, and provides guidance concerning controls that should be used to mitigate identity data threats.

4.16.3 Business benefits

Distributed ledgers are becoming increasingly important for automation with the digital economy. Identity and access management systems are starting to benefit from the advances in DLT. Many trading systems are being developed to run over blockchain technologies.

DLT based systems can bring many benefits to online interactions. Some of the benefits include:

– Efficiency:
  DLT when combined with smart contracts can help speed up business transactions. Transactions can be automated and settled between business partners using a common platform.
– Auditability:
  Ledgers provide efficient means for recording immutable transactions. As such auditing functions can be performed more efficiently for DLT participants.
– Traceability:
  Supply chain can operate more efficiently since the process of tracking goods can be automated on DLT.
– Transparency:
  Transactions on DLT can be easily verified in a transparent manner. This can enable efficient trade with built-in compliance.
– Security:
  DLT enhances on the security of online transactions through the use of consensus algorithms, data encryption and cryptography.

4.16.4 Technologies involved

ITU-T X.1401-X.1403 are essential Recommendations for securing DLT and do use proven ITU-T security standards.