International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(7 SEPTEMBER 2016)

XSTR-SUSS
Successful use of security standards

Summary

This technical report on the successful use of security standards 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). A number of success factors are identified which, when followed, yield widely commercially accepted standards. This report covers the use of security standards in a variety of applications and introduces readers to the relevance and importance of foundational security standards such as architectural standards, methodology, definitions, and other high-level guidance. The overall focus is to encourage successful and productive use of these standards.

Keywords

ASN.1, authentication, cybersecurity, PKI, SAML, security, spam, trust, XACML

Change Log

This document contains Version 1 of the ITU-T Technical Report on "*Successful use of security standards*" approved at the ITU-T Study Group 17 meeting held in Geneva, 29 August - 7 September 2016.

Editor: Mr Abbie Barbir
Aetna
United States

Tel: +1 3153083840
E-mail: BarbirA@aetna.com

CONTENTS

Page

Page

List of Figures

Page

Technical Report ITU-T XSTR-SUSS

Technical Report ITU-T
Successful use of security standards

1 Scope

This Technical Report focuses on how approved security-related ITU-T Recommendations can be successfully deployed. Both individual Recommendations (such as ITU-T X.805) and families of Recommendations (such as CYBEX) are considered and the potential benefits that can be gained from their use are described.

In selecting the specific standards for inclusion in this 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.

The technical report also serves as promotion tool for successful ITU-T achievements.

2 Glossary

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
CIRTs	Computer Incident Response Teams
CRL	Certificate Revocation List
CYBEX	Cybersecurity Information Exchange
RFC	Requests For Comments
G2C	Government to Citizen
HTTP	Hyper Text Transmission Protocol
ICT	Information and communications technology
IoT	Internet of Things
LDAP	Lightweight Directory Access Protocol
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
RBAC	Role Based Access Control
SaaS	Software as a Service

SAML	Security Assertion Markup Language
SOA	Source Of Authority
SNMP	Simple Network Management Protocol, SNMP)
SSO	Single Sign On
XML	Extensible Markup Language
XSD	XML Schema Definition
UN	United Nations

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 in cross security domains community communications. The use of internationally agreed upon standards as a basis for network security promotes commonality of approaches and provides a cost effective approach for deploying secure solutions as opposed to developing individual approaches for each jurisdiction.

Standardization and the use of common profiles facilitate 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 make it easier for organizations to enhance network defence and resilience.

Security standards play an important role in improving approaches to information security. In particular, they can improve an organization's internal process 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 new technologies or business models.

To be able to mitigate cybersecurity threats at a global level, the task of standardizing processes and procedures becomes essential for enabling and achieving 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 common procedures.

Standardized network security solutions benefit both suppliers and service providers through economy of scale in product development and component interoperability. ITU-T standards act as repositories for the industry best security practices. ITU-T Recommendations provide an impetus for passing down solutions on complex global security challenges in a simple way to those organizations that need to address complex threats and vulnerabilities.

3.1 Evolution of ITU-T security standards

Organizations need to devise a comprehensive plan for addressing its 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 Rec. ITU-T X.1205] aims at securing the cyber environment, a system that may involve stakeholders that belong to many 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 face of the changing nature of threats.

Organizations need to devise a comprehensive plan for addressing its security needs. Security is not one size fit all [see Rec. 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 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 is 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, smart grid, smartphone, 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 network 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. Fundamental concepts of security, including threats, vulnerabilities and security countermeasures, are defined in many ITU-T individual or family of Recommendations.

3.2 Who does the ITU-T security Recommendation 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 the risk environment in the telecom vertical differs 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.

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 cost 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, public and private sector implementations protect citizens and enhance the range of offerings that citizens can trust and get accustomed to enjoy and appreciate.

International security standards as developed by ITU-T can enhance the range of service offerings to citizens and consumers. ITU-T Recommendations can encourage fair competition in the market place in particular in the era of Internet of Things and mobility. Recommendations as developed by ITU-T provide a set of security requirements that act as a baseline that IT security in enterprises can use to determine the 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 cybersecurity solutions across different geographical regions and communities. Standards provides the template for public and private entities to produce internal standardized processes and procedures that are essential for achieving seamless 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 and use of standards is necessary for security and is best done with the involvement and participation of public and private sector in the process. This working principle is important since the cooperation of various stakeholders is essential for the development of successful standards. Since nowadays, the success of cybersecurity initiatives requires the effective collaboration between public and private sectors. In many cases, the private sector service providers are involved in carrying out the implementation of public sector requirements.

The online world does not observe national borders or legal boundaries. It does not share a uniform perception or definition of security and privacy. However, the virtual world and todays 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 to 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 in the subsequent sub-clauses.

3.4.1 Readiness, abilities and effectiveness

ITU-T security Recommendations contains 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 standardized processes and procedures is an essential part of achieving successful cooperation in a cross-border or cross-community environment. In the absence of reliance on common standards, individual organizations would 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 & 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 ensure 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 cost.

ITU-T standards provide a blueprint to enable an organization to design an internal security structure that is secure with a competitive edge. For example, an organization using ITU-T standards 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 auditing and compliance costs. This is because ITU-T profiles and best practices can provide organizational standard blueprints for setting up internal security standards.

Using ITU-T standards can help organization to reduce cost 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 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 sufficient flexibility in the choice of implementation variants while keeping minimal the variety of options relative to the number of mandatory features.

ITU-T also 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, MoUs and other means of collaboration with other bodies to help to identify and bridge the gap among standards and to ensure harmonization and interoperability.

ITU-T standards take into account the benefit of the consumer and focus generating profiles that benefit the targeted audience. For example, in some areas of information security public-key infrastructure (PKI) technology is worked 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 Rec. 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 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.

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 9594-8.

4.1.2.1 Public Key Infrastructure

The basic PKI model consists of public-key certificates being issued by certification authorities (CA) 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 (CA), 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 & limitations.
- Control of delegation & 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 & 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 X.1205 ensure an organization 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 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 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

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

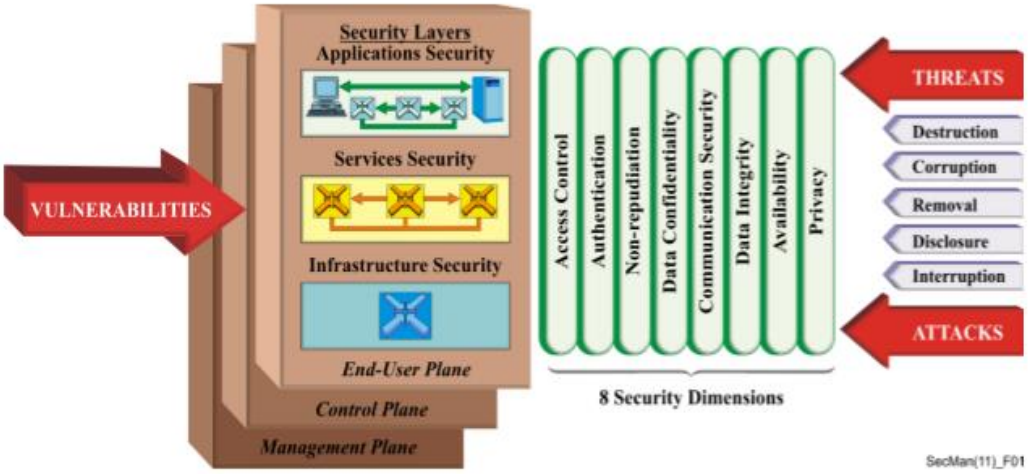

Figure 1 – Security architectural elements in Recommendation ITU-T X.805

A security dimension is a set of security measures designed to address a particular aspect of network security. The basic security services of Recommendation ITU-T X.800 (Access Control, Authentication, Data Confidentiality, Data Integrity and Non-repudiation) are reflected in the functionalities of the corresponding security dimensions of Recommendation ITU-T X.805 (as depicted in Figure 1).

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.

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

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 on which standards can be used for securing the next generation networks. ITU-T X.805's focus 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 eco system 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. ITU-T X.805 standard provides organizations 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 it has products from different vendors.

4.4 Security Assertion Markup Language

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

4.4.1 Who does this standard affect?

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

SAML (Security Assertion Markup Language) 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.

4.4.2 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 TU-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.

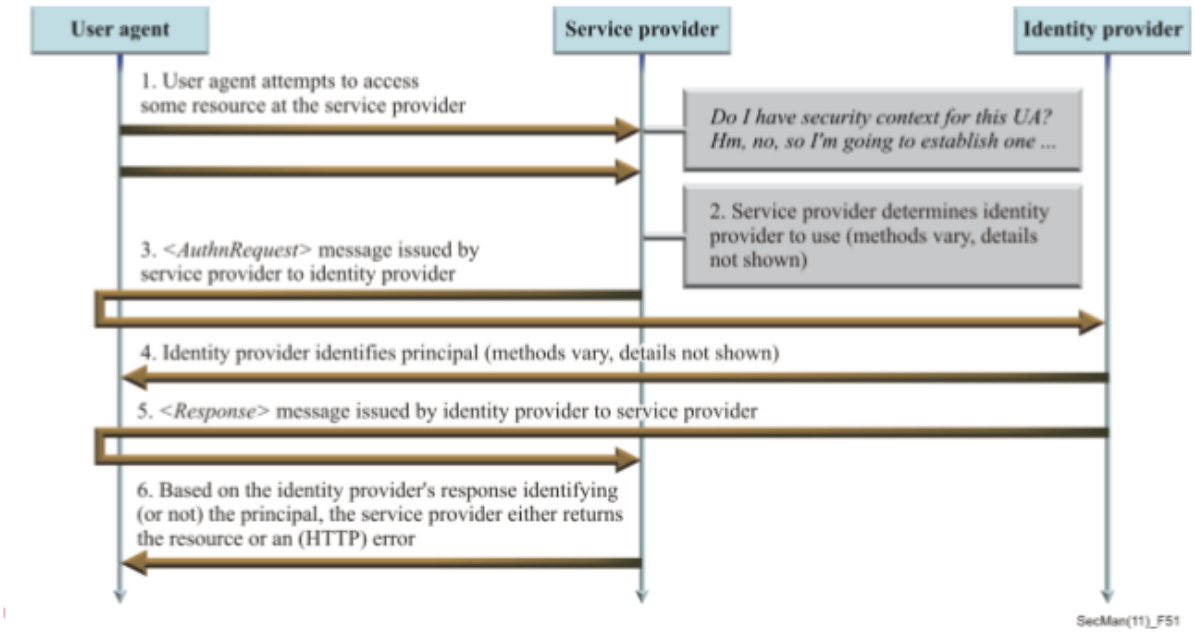

Figure 2 – Basic template for achieving SSO

4.4.3 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.

4.4.4 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.

4.5 Entity authentication assurance framework

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

4.5.1 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 process.

4.5.2 Summary of standard

Recommendation ITU-T X.1254, Entity authentication assurance framework, defines four levels of entity authentication assurance and the criteria and threats for each of the four levels. It provides guidance concerning control technologies to be used to mitigate authentication threats as well as guidance for mapping the four levels of assurance to other authentication assurance schemas and for exchanging the results of authentication based on the four levels of assurance.

4.5.3 Business benefits

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.

4.5.4 Technologies involved

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

4.6 Common Alerting Protocol

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

4.6.1 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.

4.6.2 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.

This Recommendation enables existing systems, such as Recommendation ITU-T H.323 systems, to more readily encode, transport and decode CAP messages.

4.6.3 Business benefits

Standardizing warning messages enable users across any telecommunication network to get accurate messages and instructions during all kind of emergencies.

4.6.4 Technologies involved

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

This standard is dependent on ASN.1 technologies.

4.7 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.

4.7.1 Who does this standard affect?

This standard plays an important role within organization 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 system (ABAC), 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 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 inforce at all clients immediately.

4.7.2 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 (01/2013) 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 element, policy combination algorithms, scope of XPath expressions, target element, variables in the obligation and advice element.

4.7.3 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.

4.7.4 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.

4.8 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

4.8.1 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.

4.8.2 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.

4.8.3 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.

4.8.4 Technologies involved

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

4.9 Interactive gateway system for countering spam

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

4.9.1 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.

4.9.2 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 affective framework for managing and combating spam.

4.9.3 Business benefits

Spam can create a significant burden for network operators. The problems associated with spam is 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 results 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 un-wanted spam, thus reducing organizational cost and overhead.

4.9.4 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.

4.10 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**

Basic Encoding Rules (BER), Packed Encoding Rules (PER), and XML Encoding Rules (XER) 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)**

4.10.1 Who does this standard affect?

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, 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- and fourth-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. ASN.1 messages are used in the detection of faults in production equipment and to dispatch maintenance personnel.

4.10.2 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. ASN.1 is flexible, yet with powerful construct to provide the flexibility of complex implementation.

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, Rec. ITU-T X.681 | ISO/IEC 8824-2, Rec. ITU-T X.682 | ISO/IEC 8824-3, Rec. 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, Rec. ITU-T X.691 | ISO/IEC 8825-2 and Rec. 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 Rec. 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 Rec. 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.

4.10.3 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.

4.10.4 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.

4.10.5 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 centimeters to several meters 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 SGML (Standard Generalized Markup Language). 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. 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 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.
    - The standards for interchange, encoding and storage of digital electro-cardiography developed in the European research project AIM 1 use ASN.1.
7. Intelligent networks
   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.

8. 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 (Rec. ITU-T H.320), real-time multimedia communication over the Internet (Rec. ITU-T H.225, ITU-T H.245, ITU-T H.323), and fax over the Internet (Rec. ITU-T T.38).

9. 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.

10. 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 WAIS service (Wide Area Information Server) 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 canters.

    - 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.

4.11 Cybersecurity information exchange framework

ITU-T Recommendations

- **Rec. ITU-T X.1500 / Overview of cybersecurity information exchange - Structured cybersecurity information exchange techniques**
- **Rec. ITU-T X.1520 / Common Vulnerability Enumeration (CVE)**
- **Rec. ITU-T X.1521 / Common vulnerability scoring system (CVSS)**
- **Rec. ITU-T X.1524 / Common Weakness Enumeration (CWE)**
- **Rec. ITU-T X.1525 / Common Weakness Scoring System (CWSS)**
- **Rec. ITU-T X.1526 / Language for the open definition of vulnerabilities and for the assessment of a system state**
- **Rec. ITU-T X.1528 series / Common Platform Enumeration (CPE)**
- **Rec. ITU-T X.1544 / Common Attack Pattern Enumeration and Classification (CAPEC)**
- **Rec. ITU-T X.1546 / Malware Attribute Enumeration and Characterization (MAEC)**

4.11.1 Who does this standard affect?

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

- National coordination canters 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 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.

4.11.2 Summary of standard

The Cybersecurity information exchange framework (CYBEX) 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.

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 Framework (CYBEX) 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 time, 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 below in Figure 3 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.

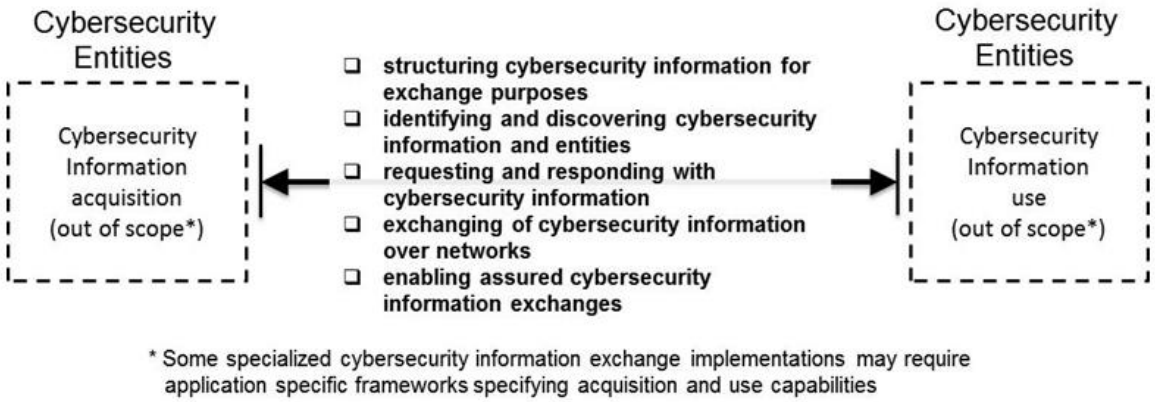

Figure 3 – Framework for the exchange of Cybersecurity information

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.

4.11.3 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.

4.11.4 Technologies involved

CYBEX can be implemented over any technology stack. In particular, CYBEX can benefit from modern Web technology stack that facilitate 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.

4.11.5 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 full set of Recommendations including exchange protocols, or by adopting part of Recommendations that provide identification and enumerations of cybersecurity information.