

Security in Telecommunications and Information Technology

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

October 2004

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

Security in Telecommunications and Information Technology

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

October 2004

Acknowledgements

This manual was prepared with the contribution of numerous authors who either contributed to the generation of the relevant ITU-T Recommendations or participated in the ITU-T Study Group meetings, Workshops and Seminars. In particular, credits should be given to the following contributors: Herb Bertine, David Chadwick, Martin Euchner, Mike Harrop, Sándor Mazgon, Stephen Mettler, Chris Radelet, Lakshmi Raman, Eric Rosenfeld, Neil Seitz, Rao Vasireddy, Tim Walker, Heung-Youl Youm, Joe Zebarth, and to the ITU/TSB counsellors.

© ITU 2004

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

Contents

Acknowledgements

- Contents**..... iii
- Preface**..... vii
- Executive Summary** ix
- 1 Scope of Manual 1
- 2 Basic Security Architectures and Services..... 1
 - 2.1 The Open Systems Security Architecture (X.800)..... 1
 - 2.2 The Lower and Upper Layer Security Models (X.802 and X.803) 2
 - 2.3 The Security Frameworks (X.810-X.816)..... 2
 - 2.4 Security Architecture for Systems Providing End-to-End Communications (X.805)..... 4
- 3 The Fundamentals of Protection: Threats, Vulnerabilities and Risks 6
- 4 Security Requirements for Telecommunication Networks 7
 - 4.1 Rationale 8
 - 4.2 General Security Objectives for Telecommunications Networks..... 8
- 5 Public Key and Privilege Management Infrastructures..... 9
 - 5.1 Secret Key and Public Key Cryptography..... 9
 - 5.2 Public Key Certificates..... 12
 - 5.3 Public Key Infrastructures..... 13
 - 5.4 Privilege Management Infrastructure 13
- 6 Applications 15
 - 6.1 VoIP using H.323 Systems..... 15
 - 6.2 IPCablecom System 24
 - 6.3 Secure Fax Transmission 28
 - 6.4 Network Management Applications..... 31
 - 6.5 E-prescriptions 39
 - 6.6 Secure Mobile End-to-End Data Communications 43
- 7 Availability Dimension and Infrastructure Layer 47
 - 7.1 Path topologies and end-to-end path availability calculations 48
 - 7.2 Enhance the availability of a transport network – Overview 49
 - 7.3 Protection 49
 - 7.4 Restoration 55
 - 7.5 Outside plant 56
- 8 Incident Organization and Security Incident Handling (Guidelines) for Telecommunications Organizations..... 57
 - 8.1 Definitions..... 58
 - 8.2 Rationale 59
- 9 Conclusions..... 60

References	61
Annex A – Catalogue of ITU-T Recommendations related to security	63
Annex B – Security Terminology	85
B.1 List of security-related terms and definitions	86
B.2 Security-related Acronyms.....	98
Annex C – List of Study Groups and Security-related Questions.....	101

Preface

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

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

It is imperative that security be a well-thought-out process at all stages, from system inception and design through implementation and deployment. In the development of standards, security must always be an element of the initial work, and not an afterthought. Failure to consider security adequately during the design phase of standards and systems development can easily result in implementation vulnerabilities. Standards committees have a vital role to play in protecting telecommunications and information technology systems by maintaining an awareness of security issues, by ensuring that security considerations are a fundamental part of specifications, and by providing guidance to assist implementers and users in the task of making communication systems and services sufficiently robust.

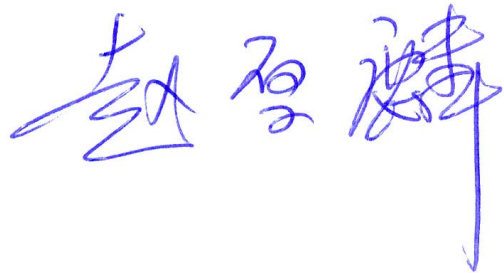
ITU-T has been active in the security work for telecommunications and information technology for many years. However, it has not always been easy to find out what has been covered, and where it can be found. This manual attempts to aggregate all of the available information on ITU-T's work.

The manual is intended as a guide for technologists, middle-level management, as well as regulators, to assist in the practical implementation of security functions. Through several example applications, security issues are explained with a focus on how ITU-T Recommendations address them.

The first version of this Manual, version 2003, was published in December 2003, prior to the World Summit on the Information Society (WSIS). Encouraged by the enthusiastic reception of the ICT community worldwide and viewing the valuable proposals and feedback from the readers, we prepared a new version. This new version, version 2004, has a new structure with additional new material and some areas have been expanded on.

I would like to express my appreciation to the engineers of the ITU Telecommunication Standardization Bureau who, in conjunction with experts from the ITU membership, had completed most of the first version. I would also like to express my appreciation to those who have provided us with valuable proposals and to those who have contributed to the new version. My particular appreciation goes to Mr. Herbert Bertine, Co-Chairman of ITU-T Study Group 17, the leading Study Group on security, and the team of collaborators from Study Group 17 and other ITU-T Study Groups.

I trust that this manual will be a useful guide for those looking to address security issues and I welcome feedback from readers for future editions.



Houlin Zhao
Director,
Telecommunication Standardization Bureau, ITU
Geneva, October 2004

Executive Summary

The communications industry has made a major contribution to improve global productivity and efficiency by the development of communications infrastructures that bridge communities in almost every industrial segment and every part of the world. This has been possible, in large part through the implementation of standards developed by organizations such as ITU-T. These standards ensure interoperability and efficiency of network operations and also lay the foundations for next generation networks. However, while standards have continued to meet end-user and industry needs, the increased use of open interfaces and protocols, the multiplicity of new participants, the sheer diversity of applications and platforms, and implementations that are not always adequately tested have increased opportunities for malicious use of networks. In recent years, a surge in security violations (such as viruses and attacks that have resulted in breaches of confidentiality of stored data) has been observed throughout global networks and has often resulted in major cost impacts. The question then is, how does one support an open communication infrastructure without compromising the information exchanged on it? To a large degree, the answer lies in developing sufficiently robust specifications that security threats to any area of the communications infrastructure can be countered. With this objective, the efforts of standards groups include the development of standardized security architectures and frameworks, standards for security management, security-specific protocols and techniques to secure communications protocols, as well as steps to minimize potential vulnerabilities in communications standards generally.

The purpose of this security manual is to provide an overview of the numerous Recommendations developed by ITU-T – sometimes in collaboration with other Standard Development Organizations – to secure the communication infrastructure and the associated services and applications.

In order to address the multiple facets of security, it is necessary to establish a framework and architecture, in order to have a common vocabulary with which to discuss the concepts.

Section 2 introduces the basic security architectures and elements defined in ITU-T Recommendations along with the eight security dimensions that have been defined to address end-to-end security in networked applications – privacy, data confidentiality, authentication, data integrity, non-repudiation, access control, communication security, and availability. These general principles are used as a basis for many of the other security service and mechanism standards.

Section 3 introduces the fundamental security concepts of threats, vulnerabilities and risks, and explains the relationship between these concepts and their relevance to standards bodies.

Section 4 builds on information in previous sections to develop security requirements for telecommunications networks. In particular, this section discusses the objectives for telecommunications network security and the services that can be used to achieve those objectives.

Section 5 introduces the important concepts of public key and privilege management infrastructures. These infrastructures, and their underlying mechanisms, are particularly important in supporting authentication and authorization services.

ITU-T has developed security provisions in several systems and services defined in its Recommendations and a significant focus of this manual is on applications, as seen in Section 6. These include voice and multimedia applications over IP (H.323 and IPCablecom), health care, and fax. These applications are described in terms of deployment architecture and of how protocols have been defined to meet security needs. In addition to offering security of application information, there is also a need to secure the infrastructure of the network and the management of network services. Examples of standards where security provisions have been defined to address network management aspects are also included in Section 6.

Section 7 deals with the availability dimension and the infrastructure layer of security. These are two of the core competence areas of the ITU-T although they are not always seen as contributing to security. Information is given on availability calculation and ways for enhancing the availability of a transport network. This section concludes with guidance for securing outside plants.

Section 8 outlines guidelines recently approved by ITU-T on incident organization and security incident handling. This issue is commonly agreed to be of prime importance given the development of security threats in the telecommunication and information systems infrastructure.

In addition, this manual contains the current version of the ITU-T Catalogue of Recommendations related to Security Aspects – the list in Annex A is extensive and further demonstrates the breadth of ITU-T work on security. This manual also provides a list of acronyms and definitions related to security and other topics addressed in this document, which were extracted from relevant ITU-T Recommendations and other resources (such as the ITU-T SANCHO database and the Compendium of ITU-T Approved Security Definitions developed by ITU-T Study Group 17). This is provided in Annex B. In Annex C we summarize the security-related work that each of the ITU-T Study Groups does. The material in these Annexes is constantly updated and can be found at www.itu.int/ITU-T.

In conclusion, ITU-T has been proactive – not only in IP-based technologies, but in meeting the needs of many different industry segments where security requirements vary significantly. This manual shows how solutions are available in ITU-T Recommendations both in terms of generic framework and architecture but also for specific systems and applications – which are already globally deployed by network and service providers.

1 Scope of Manual

This manual provides an overview of security in telecommunications and information technologies, describes practical issues, and indicates how different aspects of security in today's applications are addressed by ITU-T. The manual has a tutorial character: it collects security related material from ITU-T Recommendations into one place and explains respective relationships. In this second edition, the manual covers additional aspects of security, in particular those that relate to availability – for which ITU-T has a great deal to offer – and to environmental damage in which area ITU-T is also active. It also includes results achieved on security-related standardization since the first edition. Further, aspects covered are based on existing work, not on work in progress, which will be addressed in future editions of this manual.

The intended audience for this manual includes engineers and product managers, students and academia, as well as regulators who want to better understand security issues in practical applications.

2 Basic Security Architectures and Services

During the communications standardization work of the early 1980s, the need to address elements of security architecture was recognized. This led to the development of the Open Systems Security Architecture (Rec. X.800). However, it was also recognized that this was but the first stage in the development of a suite of standards to support security services and mechanisms. This work, most of which was done in collaboration with ISO, resulted in further Recommendations, including security models and frameworks that specify how particular types of protection can be applied in particular environments. In addition, the need for other security architectures, such as the security architectures for Open Distributed Processing and for Systems Providing End-to-end Communications, was identified. The recently published Recommendation X.805 addresses this need and complements other Recommendations of X.800 series by offering security solutions aimed at providing end-to-end network security.

2.1 The Open Systems Security Architecture (X.800)

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

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

Although X.800 was developed specifically as the OSI security architecture, the underlying concepts of X.800 have been shown to have much broader applicability and acceptance. The standard is particularly important as it represents the first internationally-agreed consensus on the definitions of the basic security services (*Authentication, Access Control, Data Confidentiality, Data Integrity and Non-repudiation*) along with more general (pervasive) services such as *Trusted Functionality, Event Detection and Security Audit and Recovery*. Prior to X.800 there had been a wide range of views on what basic security services were required and what exactly each service would do. X.800 reflects a strong, international consensus on these services. (The basic security services are reviewed in more detail in Section 2.3 below.)

The value and general applicability of X.800 results specifically from the fact that it represents a significant consensus on the meaning of the terms used to describe security features, on the set of security services needed to provide protection for data communications, and on the nature of those security services.

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

2.2 The Lower and Upper Layer Security Models (X.802 and X.803)

The purpose of the Lower and Upper Layer Security Models (Recommendations X.802 and X.803 respectively) is to show how the security concepts developed in the Security Frameworks can be applied to specific areas of Open Systems architectures.

The purpose of the Upper Layers Security Model (X.803) is to provide standards developers with the architectural model for the development of application-independent security services and protocols in the upper layers of 7-layer OSI model. The Recommendation provides guidance on the positioning of, and inter-relationships between security services in the Session, Presentation and Application layers. In particular, the Recommendation describes how security transformation functions (such as encipherment) are addressed at the Application and Presentation layers. In addition, the concept of *security exchange* is introduced. *Security policy* and *security state* are also described.

The Lower Layers Security Model (X.802) provides guidance for the development of security-related protocols and protocol elements appropriate to the lower layers of the OSI model. It describes the basis for security interactions between the lower layers as well as the placement of security protocols.

2.3 The Security Frameworks (X.810-X.816)

The Security Frameworks were developed to provide comprehensive and consistent descriptions of the security services defined in X.800. They are intended to address all aspects of how the security services can be applied in the context of a specific security architecture, including possible future security architectures. The frameworks focus on providing protection for systems, objects within systems, and interaction between systems. They do not address the methodology for constructing systems or mechanisms.

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

2.3.1 The Security Framework Overview (X.810)

The Security Framework Overview introduces the other frameworks and describes common concepts including security domains, security authorities and security policies that are used in all the frameworks. It also describes a generic data format that can be used to convey both authentication and access control information securely.

2.3.2 The Authentication Framework (X.811)

Authentication is the provision of assurance of the claimed identity of an entity. Entities include not only human users, but also devices, services and applications. Authentication can also provide assurance that an entity is not attempting a masquerade or an unauthorized replay of a previous communication. X.800 identifies two forms of authentication: *data origin authentication* (i.e., corroboration that the source of data received is as claimed) and *peer entity authentication* (i.e., corroboration that a peer entity in an association is the one claimed).

The Authentication Framework occupies a position at the top of a hierarchy of authentication standards that provide concepts, nomenclature and a classification for authentication methods. This framework: defines the basic concepts of authentication; identifies possible classes of authentication mechanism; defines the services for these classes of mechanism; identifies functional requirements for protocols to support these classes of mechanism; and identifies the general management requirements for authentication.

Authentication generally follows identification. Information used for identification, authentication and authorization should be protected.

2.3.3 The Access Control Framework (X.812)

Access control is the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. Access Control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications.

The Access Control Framework describes a model that includes all aspects of access control in Open Systems, the relationship to other security functions (such as Authentication and Audit), and the management requirements for Access Control.

2.3.4 The Non-repudiation Framework (X.813)

Non-repudiation is the ability to prevent entities from denying later that they performed an action. Non-repudiation is concerned with establishing evidence that can later be used to counter false claims. X.800 describes two forms of non-repudiation service, namely, *non-repudiation with proof of delivery*, which is used to counter false denial by a recipient that the data has been received, and *non-repudiation with proof of origin* which is used to counter false denial by an originator that the data has been sent. However, in a more general sense, the concept of non-repudiation can be applied to many different contexts including content non-repudiation of creation, submission, storage, transmission and receipt of data.

The Non-repudiation Framework extends the concepts of non-repudiation security services as described in X.800 and provides a framework for the development of these services. It also identifies possible mechanisms to support these services and general management requirements for non-repudiation.

2.3.5 The Confidentiality Framework (X.814)

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

The purpose of the confidentiality service is to protect information from unauthorized disclosure. The Confidentiality Framework addresses the confidentiality of information in retrieval, transfer and management by defining the basic concepts of confidentiality, defining the possible classes of confidentiality and the facilities required for each class of confidentiality mechanism, identifying the management and supporting services required, and addressing the interaction with other security services and mechanisms.

2.3.6 The Integrity Framework (X.815)

Data Integrity is the property that data has not been altered in an unauthorized manner. In general, an integrity service addresses the need to ensure that data is not corrupted or, if it is corrupted, then the user is aware of that fact. Although there are different aspects of integrity (such as data integrity and system integrity), X.800 focuses almost exclusively on data integrity.

The Integrity Framework addresses the integrity of data in information retrieval, transfer and management. It defines the basic concepts of integrity, identifies possible classes of integrity mechanism and the facilities for the class of mechanism, identifies management required to support the class of mechanism, and addresses the interaction of the integrity mechanism and the supporting services with other security services and mechanisms.

2.3.7 The Audit and Alarms Framework (X.816)

A *security audit* is an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures. A *security alarm* is a message generated when a security-related event that is defined by security policy as being an alarm condition has been detected.

The Audit and Alarms Framework defines the basic concepts and provides a general model of security audit and alarms, identifies the criteria for a security audit and for raising alarms, identifies possible classes of audit and alarms mechanisms, defines the services for these classes of mechanism, identifies functional requirements to support these mechanisms, and identifies general management requirements for security audit and alarms.

2.4 Security Architecture for Systems Providing End-to-End Communications (X.805)

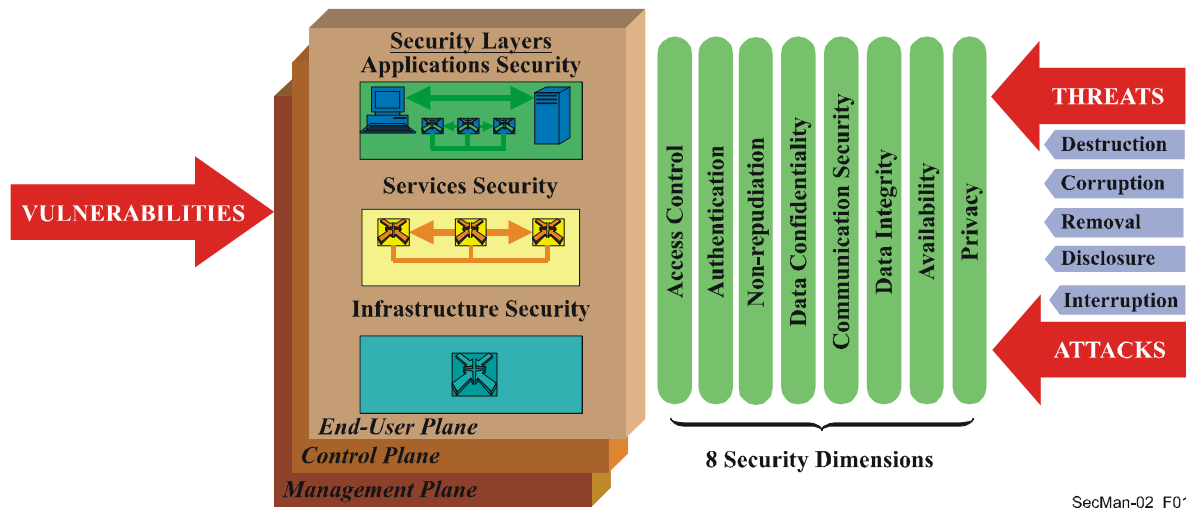
Recently a fresh look was taken at security architecture for networks. The result is Recommendation X.805, which defines a security architecture for providing end-to-end network security. The architecture can be applied to various kinds of networks where the end-to-end security is a concern independently of the network's underlying technology. The general principles and definitions apply to all applications, even though details such as threats and vulnerabilities and the measures to counter or prevent them vary based on the needs of an application.

This security architecture is defined in terms of two major concepts, layers and planes. The first axis, Security Layers address requirements that are applicable to the network elements and systems that constitute the end-to-end network. A hierarchical approach is taken in dividing the requirements across the layers so that the end-to-end security is achieved by building on each layer. The three layers are Infrastructure layer, Services layer and Applications layer. One of the advantages of defining the layers is to allow for reuse across different applications in providing end-to-end security. The vulnerabilities at each layer are different and thus countermeasures are to be defined to meet the needs of each layer. The Infrastructure layer consists of the network transmission facilities as well as individual network elements. Examples of components that belong to the Infrastructure layer are individual routers, switches and servers as well as the communication links between them. The Services layer addresses security of network services that are offered to customers. These services range from basic connectivity offerings such as leased line services to value added services such as instant messaging. The Application layer addresses requirements of the network-based applications used by the customers. These applications may be as simple as email or as sophisticated as collaborative visualization where very high-end video transfers are used in oil exploration, or designing automobiles, etc.

The second axis addresses the security of activities performed in a network. This security architecture defines three Security Planes to represent the three types of protected activities that take place on a network. The Security Planes are: (1) the Management plane, (2) the Control plane, and (3) the End-User plane. These Security Planes address specific security needs associated with network management activities, network control or signalling activities, and end-user activities correspondingly. The Management plane, which is discussed in more details in section 6.4, is concerned with Operations, Administration, Maintenance and Provisioning (OAM&P) activities such as provisioning a user or a network, etc. The Control plane is associated with the signalling aspects for setting up (and modifying) the end-to-end communication through the network irrespective of the

medium and technology used in the network. The End-User plane addresses security of access and use of the network by customers. This plane also deals with protecting end-user data flows.

With Security Layers and Security Planes as the two axes (3 Security Planes and 3 Security Layers), the architecture also defines eight Security Dimensions that are designed to address network security. These dimensions are defined below. From an architectural perspective, these dimensions are applied to each cell of the 3-by-3 matrix formed between the layers and planes so that appropriate countermeasures can be determined. Figure 1 depicts security planes, layers and dimensions of the security architecture. Section 6.4 on Management plane shows how other ITU-T Recommendations address the three cells of the 3-by-3 matrix for the Management plane.



SecMan-02_F01

Figure 1 – Security Architectural Elements in ITU-T Recommendation X.805

X.805 builds on some of the concepts of X.800 and the Security Frameworks (X.810-X.816) which were discussed above. In particular, the functionalities of the basic security services of X.800 (*Access Control, Authentication, Data Confidentiality, Data Integrity and Non-repudiation*), match the functionalities of the corresponding Security Dimensions of X.805 (depicted in Figure 1). In addition, *Communication Security, Availability and Privacy* Security Dimensions of X.805 offer new types of network protection. These eight Security Dimensions are reviewed below.

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

- The *Data Confidentiality* security dimension protects data from unauthorized disclosure. Data confidentiality ensures that the data content cannot be understood by unauthorized entities. Encryption, access control lists, and file permissions are methods often used to provide data confidentiality.
- The *Communication Security* security dimension ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points).
- The *Data Integrity* security dimension ensures the correctness or accuracy of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities.
- The *Availability* security dimension 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. Disaster recovery solutions are included in this category.
- The *Privacy* security dimension provides for the protection of information that might be derived from the observation of network activities. Examples of this information include websites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a service provider network.

The X.805 security architecture can guide the development of comprehensive security policy definitions, incident response and recovery plans, and technology architectures by taking into account each security dimension at each security layer and plane during the definition and planning phase. The X.805 security architecture can also be used as the basis of a security assessment that would examine how the implementation of the security program addresses the security dimensions, layers and planes as policies and procedures are rolled out and technology is deployed. Once a security program has been deployed, it must be maintained in order to keep current in the ever-changing security environment. The X.805 security architecture can assist in the management of security policies and procedures, incident response and recovery plans, and technology architectures by ensuring that modifications to the security program address each security dimension at each security layer and plane.

3 The Fundamentals of Protection: Threats, Vulnerabilities and Risks

In developing any kind of security framework it is very important to have a clear understanding of the assets that need to be protected, the threats against which those assets must be protected, the vulnerabilities associated with the assets and the overall risk to the assets from those threats and vulnerabilities.

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

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

According to X.800, a *security threat* is a potential violation of security. Examples of threats are:

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

Threats may be *accidental* or *intentional* and may be *active* or *passive*. An accidental threat is one with no premeditated intent such as a system or software malfunction or a physical failure. An intentional threat is one that is realized by someone committing a deliberate act. (When an intentional threat is realized it is called an *attack*.) An active threat is one that results in some change of state such as alteration of data or destruction of physical equipment. A passive threat involves no change of state. Eavesdropping is an example of a passive threat.

A *security vulnerability* is a flaw or weakness that could be exploited to violate a system or the information it contains (X.800). A vulnerability enables a threat to be realized.

There are four types of vulnerability: *Threat Model* vulnerabilities originate from the difficulty of foreseeing possible future threats; *Design and Specification* vulnerabilities come from errors or oversights in the design of a system or protocol that make it inherently vulnerable; *Implementation* vulnerabilities are introduced by errors during system or protocol implementation; and *Operation and Configuration* vulnerabilities originate from improper usage of options in implementations or weak deployment policies (such as not enforcing use of encryption in a WiFi network).

A *security risk* is a measure of the adverse effects that can result if a security vulnerability is exploited i.e., if a threat is realized. While risk can never be eliminated, one objective of security is to reduce risk to an acceptable level. In order to do that it is necessary to understand the threats and vulnerabilities and to apply appropriate countermeasures (i.e., security services and mechanisms).

While threats and threat agents change, security vulnerabilities exist throughout the life of a system or protocol unless specific steps are taken to address vulnerabilities. With standardized protocols, protocol-based security risks can be very large and global in scale. Hence it is important to understand and identify vulnerabilities in protocols and to take steps to address vulnerabilities when they are identified.

Standards bodies have both a responsibility and a unique ability to address security vulnerabilities that may be inherent in specifications such as architectures, frameworks and protocols. Even with adequate knowledge about the risks, the vulnerabilities and the threats associated with information processing and communications networks, adequate security cannot be achieved unless security is systematically applied in accordance with the relevant policies, which must be periodically reviewed and updated. In addition, adequate provision must be made for security management and incident handling. This will include identifying responsibility and specified action to prevent, or to react to, any security incident (the provisions, controls, countermeasures, safeguards to be taken or actions to be undertaken). ITU-T is working on new Recommendations covering such aspects of security management.

4 Security Requirements for Telecommunication Networks

This section provides basic considerations on the need for, and characteristics of security features as seen by the users, including operators of telecommunication networks. These considerations are derived from requirements expressed by various parties within the telecommunications market. It points mainly to the work achieved with the approval of *Recommendation E.408, Telecommunication networks security requirements*. This Recommendation provides an overview of security requirements and a framework that identifies security threats to telecommunication networks in general (both fixed and mobile; both voice and data) and gives guidance for planning countermeasures that can be taken to mitigate the risks arising from the threats.

It is generic in nature and does not identify or address requirements for specific networks.

No new security services were considered but rather the use of existing security services defined in other ITU-T Recommendations and relevant standards from other bodies was sought.

Implementing the given requirements would facilitate an international cooperation in the following areas regarding telecommunication network security:

- Information sharing and dissemination;

- Incident coordination and crisis response;
- Recruitment and training of security professionals;
- Law enforcement coordination;
- Protection of critical infrastructure and critical services; and
- Development of appropriate legislation.

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

4.1 Rationale

The requirement for a generic network security framework for international telecommunications has been originated from different sources:

- *Customers/subscribers* need confidence in the network and the services offered, including availability of services (especially emergency services) in case of major catastrophes, including violent civil actions.
- *The Public Community/Authorities* demand security by Directives and Legislation, in order to ensure availability of Services, fair competition and privacy protection.
- *Network Operators/Service Providers* themselves need security to safeguard their operation and business interests, and to meet their obligations to the customers and the public, at the national and international level.

Telecommunication networks security requirements should preferably be based upon internationally agreed security standards as it is beneficial to reuse rather than create new ones. The provisioning and usage of security services and mechanisms can be quite expensive relatively to the value of the transactions being protected. It is therefore important to have the ability to customize the security provided in relation to the services being protected. The security services and mechanisms that are used should be provided in a way that allows such customization. Due to the large number of possible combinations of security features, it is desirable to have *security profiles* that cover a broad range of telecommunication network services.

Standardization will facilitate *reuse of solutions and products* meaning that security can be introduced faster and at lower cost.

Important benefits of standardized solutions for vendors and users of the systems alike are the economy of scale in product development and component interoperation within telecommunication networks with regard to security.

It is necessary to provide security services and mechanisms to protect telecommunication networks against malicious attacks such as denial of service, eavesdropping, spoofing, tampering with messages (modification, delay, deletion, insertion, replay, re-routing, misrouting, or re-ordering of messages), repudiation or forgery. Protection includes prevention, detection and recovery from attacks, as well as management of security-related information. Protection must also include measures to prevent service outages due to natural events (weather, etc.) or malicious attacks (violent actions). Provisions must be made to allow eavesdropping and monitoring as requested by duly authorized legal authorities.

4.2 General Security Objectives for Telecommunications Networks

This section describes the ultimate aim of the security measures taken in telecommunication networks and focuses on what security requirements achieve rather than on how it is done.

The security objectives for telecommunication networks are:

- a) Only authorized users should be able to access and use telecommunication networks.
- b) Authorized users should be able to access and operate on assets they are authorized to access.

- c) Telecommunication networks should provide privacy at the level set by the security policies of the network.
- d) All users should be held accountable for their own but only their own actions in telecommunication networks.
- e) In order to ensure availability, telecommunication networks should be protected against unsolicited access or operations.
- f) It should be possible to retrieve security-related information from telecommunication networks (but only authorized users should be able to retrieve such information).
- g) If security violations are detected, they should be handled in a controlled way in accordance with a pre-defined plan to minimize potential damage.
- h) After a security breach is detected, it should be possible to restore normal security levels.
- i) The security architecture of telecommunication networks should provide a certain flexibility in order to support different security policies, e.g., different strength of security mechanisms.

The term "to access assets" is understood not only to be the possibility to perform functions but also to read information.

It can be shown that by implementing the following security measures the first five of the above-mentioned security objectives for telecommunication networks can be achieved:

- confidentiality;
- data integrity; (surely integrity of system programs is also required)
- accountability, including authentication, non-repudiation and access control; and
- availability.

5 Public Key and Privilege Management Infrastructures

Recommendation X.509, *The Directory: Public Key and Attribute Certificate Frameworks* provide a Public Key Infrastructure (PKI) standard for strong authentication, based on public key certificates and certification authorities. PKI supports the management of public keys to support authentication, encryption, integrity and non-repudiation services. The fundamental technology of a PKI is public key cryptography, which is described below. In addition to defining an authentication framework for PKI, X.509 also provides for a Privilege Management Infrastructure (PMI), which is used to ascertain rights and privileges of users in the context of strong authorization, based on attribute certificates and attribute authorities. The components of PKI and PMI are illustrated in Figure 2.

5.1 Secret Key and Public Key Cryptography

Symmetric (or *secret key*) cryptography refers to a cryptographic system in which the same key is used for both encipherment and decipherment, as illustrated in Figure 3(a). Symmetric cryptosystems require that initial arrangements be made for the individuals to share a unique secret key. The key must be distributed to the individuals via secure means, because knowledge of the enciphering key implies knowledge of the deciphering key and vice-versa.

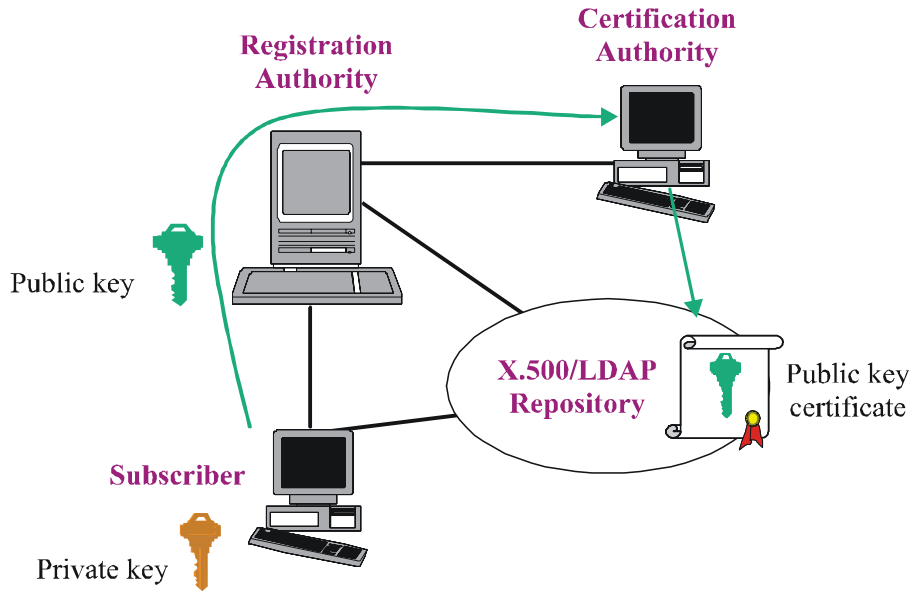
An *asymmetric* (or *public key*) cryptography system involves a pair of keys as illustrated in Figure 3(b) – a public key and a private key. Public keys can be widely distributed but the private key must always be kept secret. The private key is usually held on a smart card or on a token. The public key is generated from the private key and, although these keys are mathematically related, there is no feasible way to reverse the process to deriving the private key from the public key. To send confidential data to someone securely using public key encryption, the sender encrypts the data with the recipient's public key. The recipient decrypts it with their corresponding private key. Public key encryption can also be used to apply a digital signature to data to confirm that a document or message originated with the person who claims to be the sender (or originator). The digital signature is actually

a digest of the data that is produced using the signer's private key and appended to the document or message. The recipient uses the signer's public key to confirm the validity of the digital signature. (Note: some public key systems use two public/private key pairs, one for encryption/decryption, the other for digital signature/verification.).

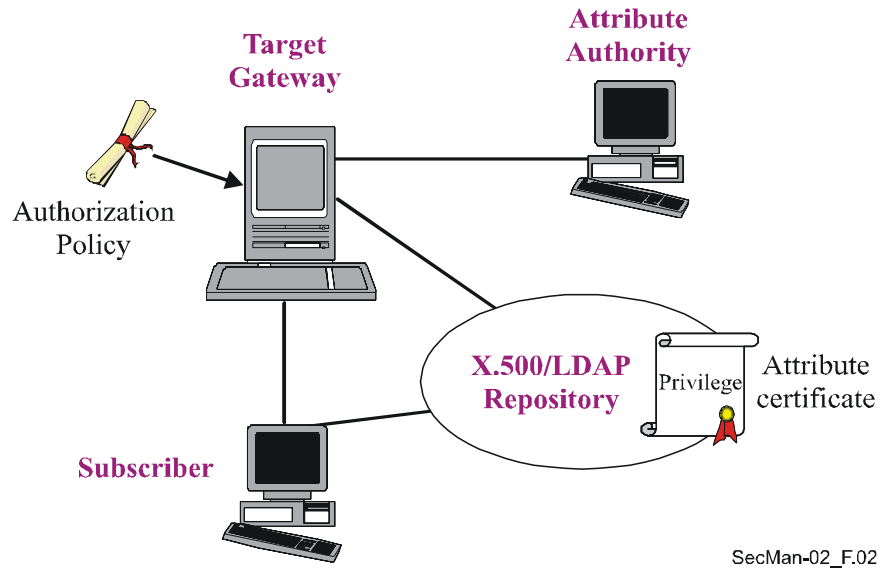
With symmetric encryption, each pair of users must have a different pair of keys and these must be distributed and held securely. With asymmetric encryption, on the other hand, the public encryption keys can be published in a directory and everyone can use the same (public) encryption key to send data to a particular user. This makes asymmetric encryption much more scalable than symmetric encryption. However, asymmetric encryption is costly in terms of computing time, therefore it is not efficient to encrypt entire messages using asymmetric encryption. Thus in practice asymmetric encryption is typically used to exchange symmetric keys which are then used to encrypt the body of the message using a more computationally-efficient symmetric algorithm. When digital signature is required, the message is hashed using a secure one way hash function such as (SHA1 or MD5) and the resulting 160 or 128 bit hash is asymmetrically encrypted using the private key of the sender and appended to the message.

It should be noted that, whether symmetric or asymmetric encryption is used, it isn't possible to route messages to their recipients if the entire message is encrypted, since the intermediate nodes will not be able to determine the recipient's address. Message headers must, therefore, generally be unencrypted.

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



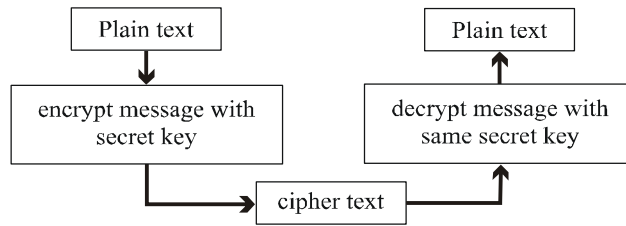
(a) Components of a public key infrastructure



SecMan-02_F.02

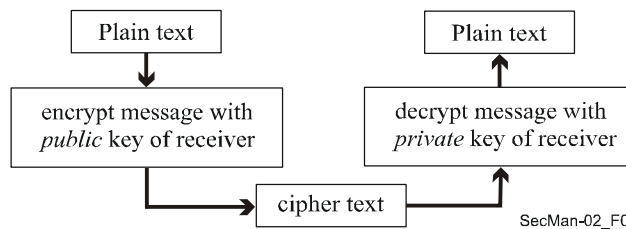
(b) Components of a privilege management infrastructure

Figure 2 – Components of PKI and PMI



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

(a) Symmetric (or secret) Key Encryption



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

(b) Asymmetric (or public) Key Encryption

Figure 3 – Illustration of the symmetric (or secret) and asymmetric (or public) key encryption processes and highlight of features

5.2 Public Key Certificates

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

In order to be able to confirm the validity of a user's public key certificate, a person needs to have access to the valid public key of the CA that issued the certificate in order to verify the CA's signature on the certificate. A CA may have its public key certified by another (superior) CA, so that validating public keys may involve a chain of certificates. Eventually this chain must end somewhere, which is typically when we encounter the certificate of the CA that is our "root of trust". Root CA public keys are distributed as self-signed certificates (in which the root CA is attesting that this is its own public key). The signature allows us to validate that the key and CA name have not been tampered with since the certificate was created. However we cannot take the name of the CA embedded in a self-signed certificate at face value, since the CA inserted the name in the certificate itself. Thus a critical

component of a Public Key Infrastructure is the secure distribution of root CA public keys (as self-signed certificates), in a manner that can assure us that the public key really does belong to the root CA named in the self-signed certificate. Without this, we cannot be sure that someone is masquerading as the root CA.

5.3 Public Key Infrastructures

The main purpose of a PKI is to issue and manage public key certificates, including the self-signed certificates of the root CA. Key management includes the creation of key pairs, the creation of public key certificates, the revocation of public key certificates (for example if a user's private key has been compromised), the storage and archival of keys and certificates, and their destruction once they have come to the end of their life. Each CA will operate according to a set of policies, and Recommendation X.509 provides mechanisms for distributing some of this policy information in the extension fields of the X.509 certificates issued by the CA. The policy rules and procedures followed by a CA are usually defined in a Certificate Policy (CP) and a Certification Practice Statement (CPS), which are documents published by the CA. These documents help to ensure a common basis for evaluating the trust that we can place in the public key certificates issued by CAs, both internationally and across sectors. They also provide us with (part of) the legal framework necessary for building up inter-organizational trust, as well as specifying limitations on the use of the issued certificates.

It should be noted that for authentication utilizing public key certificates, the endpoints are required to provide digital signatures using the associated private key value. The exchange of public key certificates alone does not protect against man-in-the-middle attacks.

5.4 Privilege Management Infrastructure

The early versions of ITU-T Recommendation X.509 (1988, 1993 and 1997), *The Directory: Authentication framework* specified the basic elements needed for Public Key Infrastructures. This included the definition of Public Key Certificates. The revised Recommendation X.509 approved in 2000 contains a significant enhancement on Attribute Certificates and a framework for Privilege Management Infrastructure (PMI). (A PMI manages privileges to support a comprehensive authorization service in relationship with a PKI.) The mechanisms defined allow for setting user access privileges in a multi-vendor and multi-application environment.

The concepts of PMI and PKI are similar, but PMI deals with authorization while PKI concentrates on authentication. Figure 2 and Table 1 illustrate the similarities between the two infrastructures.

Table 1 – Comparison of Privilege Management and Public Key Infrastructure features

Privilege Management Infrastructure	Public Key Infrastructure
Source of Authority (SoA)	Root Certification Authority (Trust Anchor)
Attribute Authority (AA)	Certification Authority
Attribute Certificate	Public Key Certificate
Attribute Certificate Revocation List	Certificate Revocation List
Authority Revocation List for PMI	Authority Revocation List for PKI

The purpose of assigning privileges to users is to ensure that they follow a prescribed security policy established by the Source of Authority. That policy-related information is bound to a user's name within the Attribute Certificate and comprises a number of elements illustrated in Figure 4.

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

Figure 4 – Structure of a X.509 Attribute Certificate

There are five components for the Control of a PMI described in Recommendation X.509, the privilege assenter, the privilege verifier, the object method¹, the privilege policy, and environmental variables (see Figure 5). The techniques enable the privilege verifier to control access to the object method by the privilege assenter, in accordance with the privilege policy.

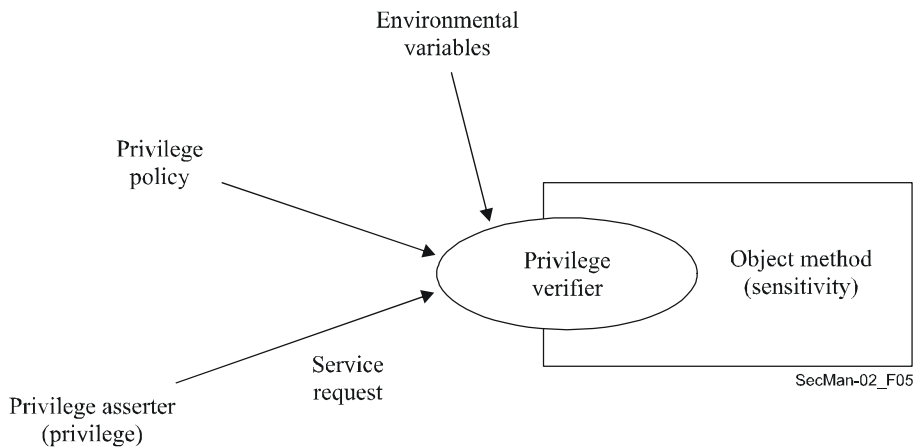


Figure 5 – ITU-T Recommendation X.509 PMI Control Model

When delegation of privilege is necessary for an implementation, there are four components of the delegation model for PMI considered in Recommendation X.509: the privilege verifier, the source of authority, other attribute authorities and the privilege assenter (see Figure 6).

¹ An object method is defined as an action that can be invoked on a resource (e.g., a file system may have read, write and execute object methods).

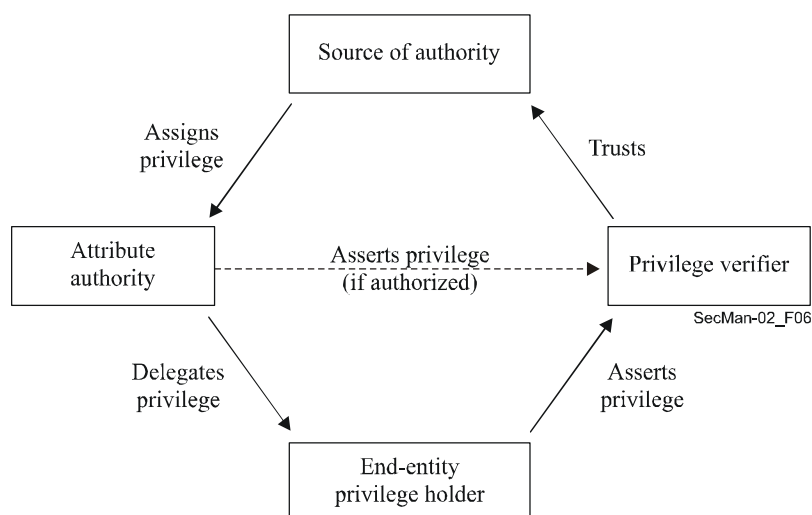


Figure 6 – ITU-T Recommendation X.509 PMI Delegation Model

Recent implementations of authorization schemes following the Role-Based Access Control (RBAC) model consider that the user is given a role. The authorization policy associates a set of permissions to a role. When accessing a resource, the user has his role checked against the policy to enable any subsequent action. The e-prescriptions application described in Section 6.5.2 illustrates the use of an RBAC system.

6 Applications

Applications addressed in this section belong to two distinct classes. The first class focuses on end-user applications. One such example is Voice-over-IP (VoIP), where network architecture and components used to provide this end user-application are described. Security considerations and solutions are discussed for the three planes supporting multi-media applications with VoIP as a special case. Other end-user applications considered here are the IPCablecom system that offers real time IP-based services over a cable network, and fax transmission. Applications that are not specific to the telecommunications industry addressed here include e-health care, in particular a system for e-prescriptions. The second class is focused on network management applications. Security is an important consideration in order to meet quality and integrity of the services offered by the providers. Thus it is imperative that management activities be performed with appropriate privileges and authorization.

6.1 VoIP using H.323 Systems

VoIP, also known as IP telephony, is the provision of services traditionally offered via the Public Switched Telephone Network (PSTN) (circuit-switched) via a network using the IP protocol (upon which the Internet is also based). These services include voice foremost, with the associated supplementary services such as voice conferencing (bridging), call forward, call waiting, multiline, call diversion, park and pick-up, consultation, and follow-me, among many other intelligent network services, and for some also voiceband data. Voice-over-Internet is a particular case of VoIP deployment, in which the voice traffic is carried over the public Internet backbone.

H.323 is an umbrella Recommendation from ITU-T that provides a foundation for audio, video, and data communications over Local Area Networks (LANs) or across IP-based networks, including the Internet, that do not provide a guaranteed Quality of Service (QoS). These networks dominate today's corporate desktops and include packet-switched TCP/IP and IPX over Ethernet, Fast Ethernet and Token Ring network technologies. By complying to H.323, multimedia products and applications

from multiple vendors can interoperate, allowing users to communicate without concern for compatibility. H.323 was the first VoIP protocol ever defined and is considered as the keystone for LAN-based products for consumer, business, entertainment, and professional applications. The core Recommendations that are part of the H.323 system are given below.

- H.323 – "Umbrella" document that describes the usage of H.225.0, H.245, and other related documents for delivery of packet-based multimedia conferencing services.
- H.225.0 – Describes three signalling protocols (RAS, Call Signalling, and "Annex G").
- H.245 – Multimedia control protocol (common to H.310, H.323, and H.324).
- H.235 – Security within H.245-based systems.
- H.246 – Interworking with the PSTN.
- H.450.x – Supplementary services.
- H.460.x – Various H.323 protocol extensions.
- H.501 – Protocol for mobility management and inter/intra-domain communication.
- H.510 – User, terminal, and service mobility.
- H.530 – Security specification for H.510.

ITU-T approved the first version of Recommendation H.323 in 1996. Version 2 was approved in January 1998, and the current version is 5, approved in July 2003. The standard is broad in scope and includes both stand-alone devices and embedded personal computer technology as well as point-to-point and multipoint conferences. Recommendation H.323 also addresses call control, multimedia management, and bandwidth management as well as interfaces between LANs and other networks.

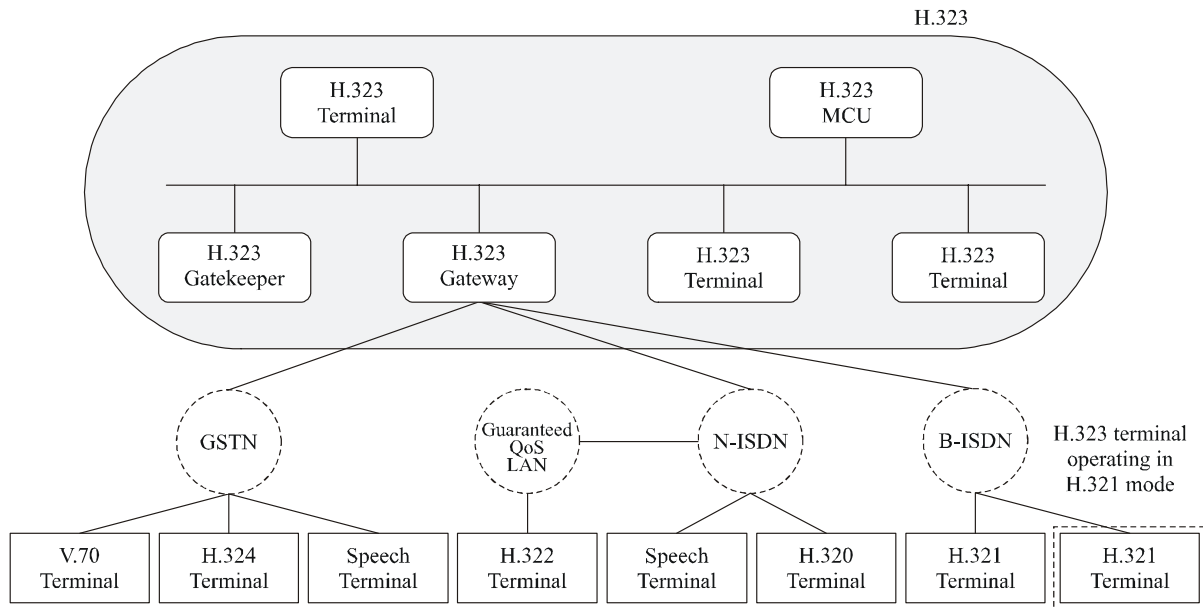
H.323 is part of a larger series of communications standards that enable videoconferencing across a range of networks. Known as H.32X, this series of Recommendations includes H.320 and H.324, which address ISDN and PSTN communications, respectively. This primer provides an overview of the H.323 standard, its benefits, architecture, and applications.

H.323 defines four major components for a network-based communications system: Terminals, Gateways, Gatekeepers, and Multipoint Control Units. Additionally, Border or Peer Elements are also possible. These elements can be seen in Figure 7.

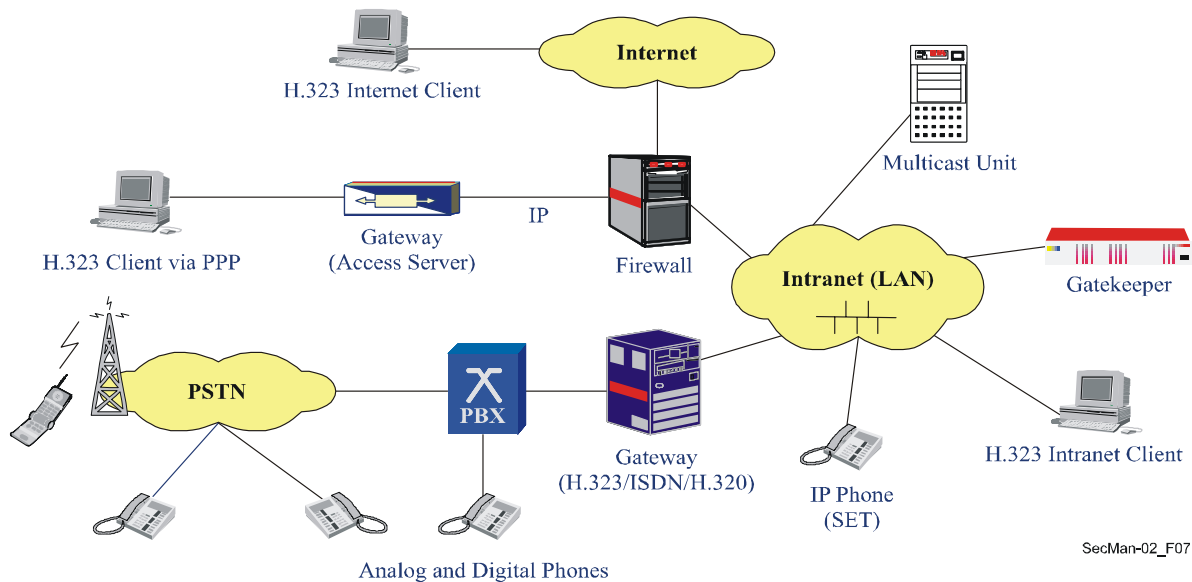
Terminals (T) are the client endpoints on the IP backbone that provide bi-directional communications. H.323 terminals must support voice communications and may support video codecs, T.120 data conferencing protocols, and MCU capabilities. Examples are: IP telephones, video phones, IVR devices, voicemail Systems, "soft phones" (e.g., NetMeeting™).

The *Gateway (GW)* is an optional element in an H.323 conference. Gateways provide many services, the most common being a translation function between H.323 conferencing endpoints and other terminal types. This function includes translation between transmission formats (e.g., H.225.0 to H.221) and between communications procedures (e.g., H.245 to H.242). In addition, the Gateway also translates between audio and video codecs and performs call setup and clearing on both the LAN side and the switched-circuit network side.

A *Gatekeeper (GK)* is the most important component of an H.323-enabled network. It acts as the central point for all calls within its zone and provides call control services to registered endpoints. In many ways, an H.323 gatekeeper acts as a virtual switch, as it performs admission control, address resolution, and may allow calls to be placed directly between endpoints or it may route the call signalling through itself to perform functions such as follow-me/find-me, forward on busy, etc. Associated with the gatekeepers are the *border* (or peer) elements (*BE*), which are responsible to exchange addressing information and participate in call authorization between administrative domains. This functionality will also allow intercommunication between different H.323 "islands" or networks. This is done through the exchange of a series of messages, as illustrated in Figure 8.



(a) H.323 system and its components [Packetizer]



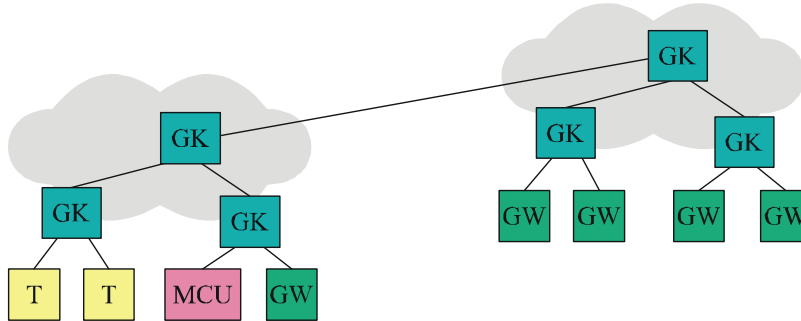
(b) H.323 deployment scenarios [Euchner]

Figure 7 – H.323 system: components and deployment scenarios

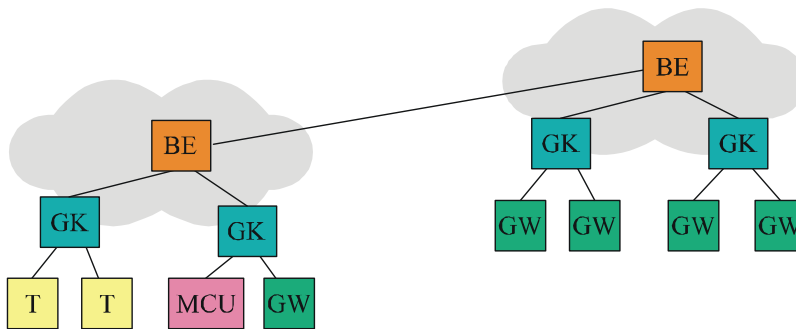
A *Multipoint Control Unit (MCU)* supports conferences between three or more endpoints. Under H.323, an MCU consists of a Multipoint Controller, which is required, and zero or more Multipoint Processors. The Multipoint Controller manages the call signalling but does not deal directly with any of the media streams. This is left to Multipoint Processors, which mixes, switches, and processes audio, video, and/or data bits. Multipoint Controller and Multipoint Processors capabilities can exist in a dedicated component or be part of other H.323 components.

Despite the fact that H.323 was designed from the start as a multimedia protocol, its main application to-date is in the VoIP market. H.323 networks in production today carry billions of minutes of voice and video traffic per month (counting public networks only); most of the VoIP traffic today is being

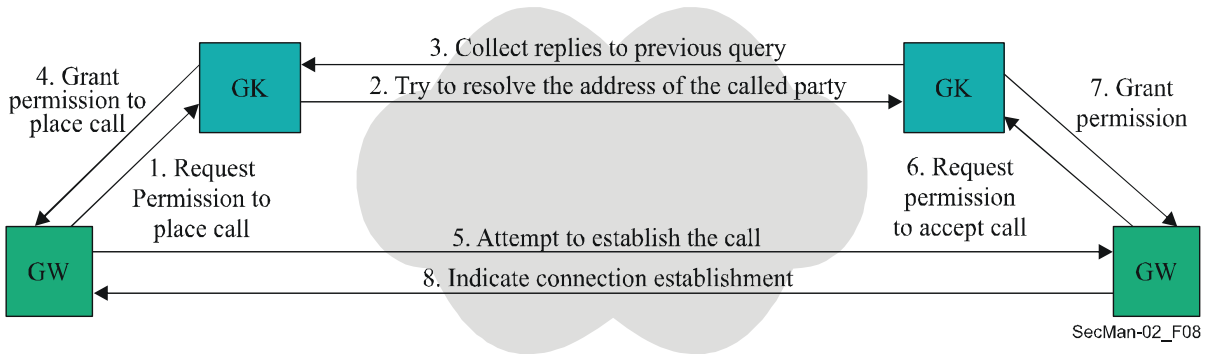
carried by H.323. Currently, it is estimated that VoIP accounts for more than 10 percent of all international long-distance minutes. Also, H.323 video traffic has been steadily on the rise. The main reason for this is the maturity of the protocol and its implementations, and that H.323 has proved to be an extremely scalable solution that meets the needs of both service providers and enterprises, with H.323 products ranging from stacks and chips to wireless phones and video conferencing hardware.



(a) Topology with RAS



(b) Topology with Annex G/H.225.0



(c) High Level Call Flow

Legend: BE: Border Element; GK: Gatekeeper; GW: Gateway; MCU: Multipoint Control Unit; T: Terminal, RAS: Registration, Admission and Status protocol

Figure 8 – Communications between Administrative Domains

The following is a list of the functionalities provided by H.323 systems:

- voice, video, and data conferencing capability;
- communication between various terminal types, including PC-to-phone, fax-to-fax, phone-to-phone and Web calls;

- T.38 fax and modem-over-IP support;
- many supplementary services (call forward, call pickup, etc);
- strong interoperability with other H.32x systems, including H.320 (ISDN) and H.323M (3GPP mobile wireless);
- specification of media gateway decomposition (via the H.248 Gateway Control Protocol);
- support for signalling and media security;
- user, terminal, and service terminal mobility; and
- support for emergency services signalling.

Examples of where H.323 is used are wholesale transit by operators, especially for VoIP backbones (Class 4 switches for voice traffic), and calling card services. In corporate communications H.323 is used for IP-PBX, IP-Centrex, Voice VPN, integrated voice and data systems, WiFi phones, implementation of call centres, and mobility services. For professional communications, it is widely used for voice (or audio) and video conferencing, for voice/data/video collaboration, and distance learning. In a residential environment, uses include broadband audio-visual access, PC-to-phone, delivery of custom news and information.

6.1.1 Security issues in Multimedia and VoIP

As all the elements of an H.323 System can be geographically distributed and due to the open nature of IP networks, several security threats arise, as illustrated in Figure 9.

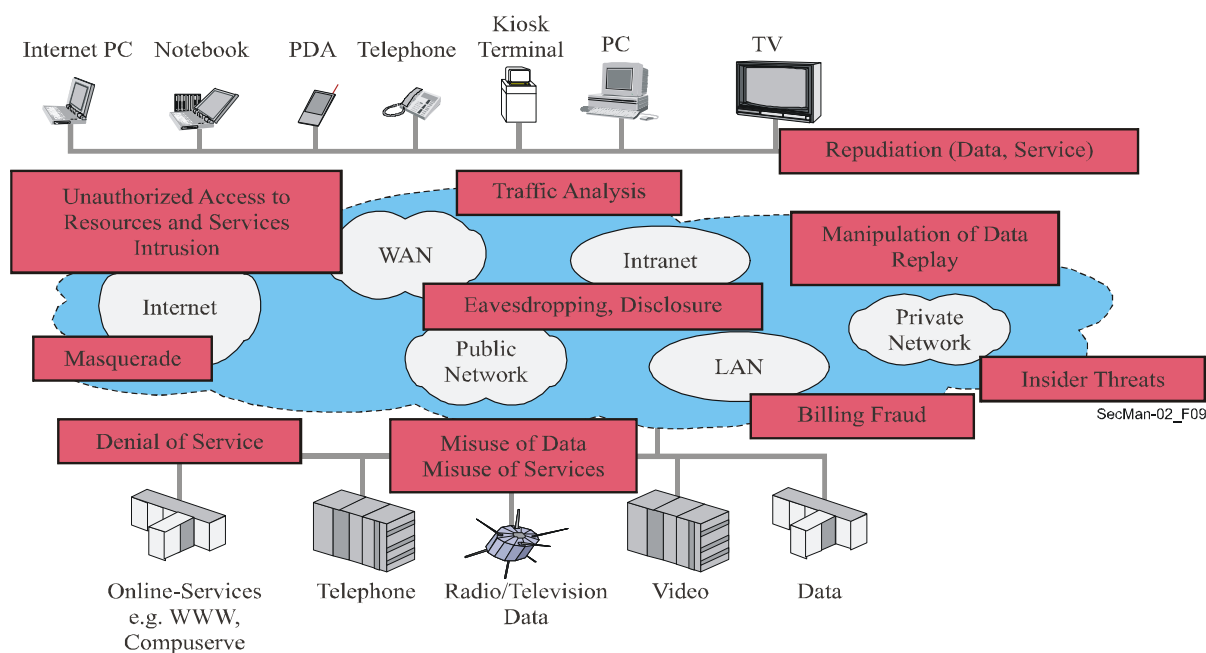


Figure 9 – Security threats in Multimedia communications

The main security issues in multimedia communications and IP telephony in general are further described below [Euchner].

- User and terminal authentication: VoIP service providers require to know who is using their service in order to correctly account and possibly bill the service usage. As a prerequisite for the authentication, the user and/or the terminal have to be identified through some identity. Then a user/terminal has to prove that the claimed identity is in fact the true identity. This typically occurs through strong cryptographic authentication procedures (e.g., protected

password or X.509 digital signatures). Likewise, users may want to know with whom they are phoning.

- Server authentication: Since VoIP users typically communicate with each other through some VoIP infrastructure with involved servers (gatekeepers, multicast units, gateways), users are interested to know if they are talking with the proper server and/or with the correct service provider. This aspect includes fixed and mobile users.
- User/terminal and server authentication counter-security threats, such as masquerade, man-in-the-middle, IP address spoofing and connection hijacking.
- Call authorization is the decision-making process to decide if the user/terminal is actually permitted to use the service resources such as a service feature (e.g., calling into the PSTN) or a network resource (QoS, bandwidth, codec, etc.). Most often authentication and authorization functions come together in order to realize an access control decision. Authentication and authorization help to thwart attacks like masquerade, misuse and fraud, manipulation and denial-of-service.
- Signalling security protection addresses protection of the signalling protocols against manipulation, misuse, confidentiality and privacy. Signalling protocols are typically protected by cryptographic means using encryption as well as integrity and replay protection. Special care has to be given to meet the critical performance requirements of real-time communication using few handshakes and short roundtrips to avoid lengthy call setup times or introduction of speech quality degradation from packet delays or jitter due to security processing.
- Voice confidentiality is realized through encryption of the voice packets; i.e., the RTP payloads and counters eavesdropping of snooped voice data. In general, the media packets (e.g., video) of multimedia applications are encrypted as well. Further advanced protection of media packets also includes authentication/integrity protection of the payloads.
- Key management includes not only all tasks that are necessary for securely distributing keying material among the parties to users and to servers, but also tasks like key updating expired or lost keys. Key management may be a task separate of the VoIP application (password provisioning) or may be integral with signalling when security profiles with security capabilities are being dynamically negotiated and session based keys are to be distributed.
- Interdomain security deals with the problem that systems in heterogeneous environments have implemented different security features because of different needs, different security policies and different security capabilities. As such, there is a need to dynamically negotiate security profiles and security capability negotiation such as cryptographic algorithms and their parameters. This becomes of importance in particular when crossing domain boundaries and different providers and networks are involved. An important security requirement for the interdomain communication is the ability to smoothly traverse firewalls and to cope with constraints from Network Address Translation (NAT) devices.

This list is not comprehensive but core to H.323 security. In practice however, one might face further security issues that are considered outside the scope of H.323 (e.g., security policy, network management security, security provisioning, implementation security, operational security or security incident handling).

6.1.2 How security is provisioned for VoIP

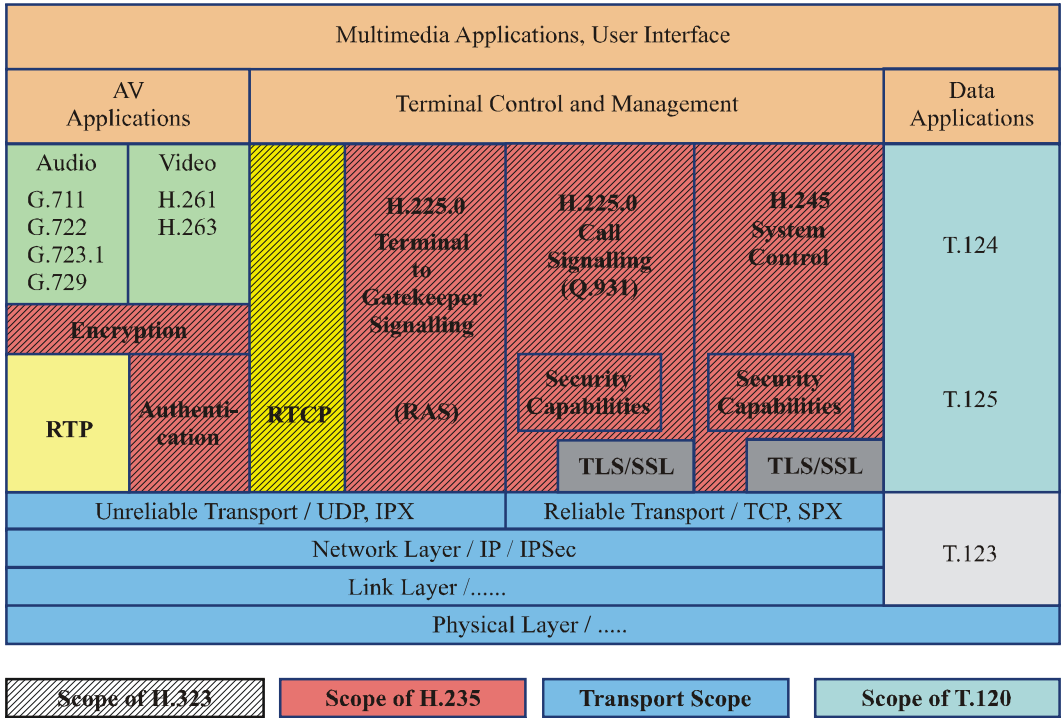
In an H.323 multimedia system, ITU-T Recommendation H.235 defines the security framework including specification of the security mechanisms and security protocols for H.323. H.235 was first introduced for H.323 Version 2 systems in 1998. Since then, H.235 has further evolved over time by consolidating the offered security mechanisms, by adding more sophisticated security algorithms (e.g., high-security, high-speed AES encryption) and by working out useful and efficient security profiles for certain use cases and environments. Amendment 1 to H.235 version 3 is the current ITU-T security Recommendation for H.323-based systems that provides scaleable security for small groups to enterprises and large-scale carriers.

In short, Recommendation H.235 provides cryptographic protection of the control protocols (H.225.0 RAS and call signalling and H.245) as well as cryptographic protection of the audio/video media stream data. Throughout the various stages of H.323 signalling, H.235 provides means to negotiate the desired and required cryptographic services, crypto algorithms and security capabilities. Key management functions for setting up dynamic sessions keys are fully integrated into the signalling handshakes and thereby help to reduce call setup latency. The H.235 key management supports the "classic" point-to-point communication but also multipoint configurations with multicast units (i.e., MCUs) when several multimedia terminals communicate within a group.

H.235 spans a wide palette of security measures that address the different target environments like intra/inter-enterprise and carriers. Depending on the assumptions such as available security infrastructure and terminal capabilities and platforms (simple endpoints or intelligent endpoints), H.235 offers a palette of customized and interoperable security profiles. The available security profiles provide security techniques that range from simple shared-secret profiles including protected password (H.235 Annex D for authentication and message integrity) to more sophisticated profiles with digital signatures and X.509 PKI certificates (H.235 Annex E and Annex F). This allows either for hop-by-hop protection using the simpler but less scalable techniques or for end-to-end protection using the scalable PKI techniques. H.235 Annex I loosens the strict dependency on a Gatekeeper-routed, server-centric architecture and provides security measures towards securing a peer-to-peer model.

H.235 makes use of special optimized security techniques such as elliptic curve cryptography and state-of-the-art AES encryption to meet the stringent performance constraints. Voice encryption when implemented is realized in the application layer by encrypting the RTP payloads. This allows beneficial implementation with small footprint in endpoints through tight interaction with the digital signal processor (DSP) and the voice compression codecs and without dependency on a specific operating system platform. If available and suitable, existing security tools such as available Internet security packages and standards (IPSec, SSL/TLS) can be (re)used in the context of H.235.

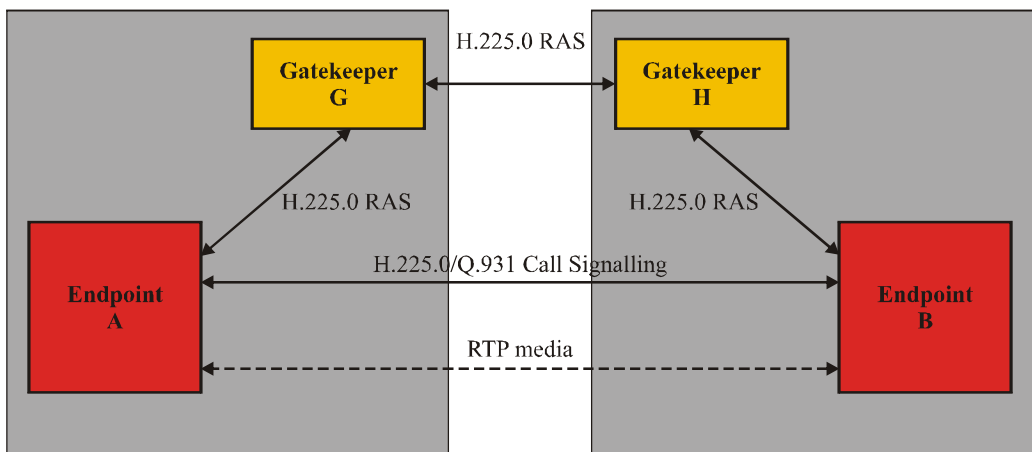
Figure 10 shows the scope of H.235, which encompasses provisions for setting up calls (H.225.0 and H.245 blocks) and bi-directional communication (encryption of RTP payloads containing compressed audio and/or video). The functionalities include mechanisms for authentication, integrity, privacy, and non-repudiation. Gatekeepers are responsible for authentication by controlling admission at the endpoints, and for providing non-repudiation mechanisms. Security on transport and lower layers, based on IP, is beyond the scope of H.323 and H.235, but is commonly implemented using IETF's IP Security (IPSec) and Transport Layer Security (TLS) protocols. In general, IPSec or TLS can be used to provide authentication and, optionally, confidentiality (i.e., encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this, but only the security policy at each end.



SecMan-02_F10

Figure 10 – Security in H.323 as provided by H.235 [Euchner]

While many H.235 security profiles assume the H.323 gatekeeper-routed model, H.235 Annex I is biased more towards secure peer-to-peer communication with the purpose of releasing the involved gatekeepers from routing H.323 signalling tasks and of yielding better scalability and performance in general. In Annex I with its support for direct-routed calls, gatekeepers operate mostly locally within their domain to accomplish user/terminal authentication and to achieve registration, admission, address resolution, and bandwidth control. On the other hand, terminals perform the H.323 call establishment directly between the end points in an end-to-end fashion; as illustrated in the scenario of Figure 11.



SecMan-02_F11

Figure 11 – H.235 Annex I Direct-Routed Scenario

Upon endpoint (EP) A asking GK G for call admission for calling EP B, one gatekeeper (either GK G in corporate environments or GK H in inter-domain environments) generates the end-to-end call signalling key for both endpoints A and B. In a manner very similar to Kerberos (see an application in Recommendation J.191), endpoint A securely obtains the generated key within one security token, while also obtaining another security token with the same key for endpoint B. When making the call, EP A, on one hand, directly applies the key to protect the Call signalling towards EP B but on the other hand also relays the other security token with the key towards EP B. Annex I is able to use the Annex D or Annex F security profiles of H.235.

While H.235 mostly addresses "static" H.323 environments with only limited mobility provisions, a need has been recognized to provide secure user and terminal mobility in distributed H.323 environments beyond inter-domain interconnection and limited gatekeeper zone mobility. ITU-T Recommendation H.530 covers such security needs by addressing security aspects as:

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

Figure 12 illustrates the basic scenario that H.530 addresses where a mobile H.323 terminal (MT) may attach either directly to its home domain via the home gatekeeper (H-GK) or may attach to any foreign gatekeeper (V-GK) in a visited domain. Since the mobile terminal and the user are not known by the visited domain, the visited gatekeeper first has to query the authentication function (AuF) in the home domain where the MT is subscribed and known. Thus, the visited domain delegates the task of authentication to the AuF in the home domain and lets the AuF accomplish authentication and decide upon authorization. In addition, the AuF assures the V-GK a cryptographic binding of the MT and V-GK dynamic key using an embedded cryptographic security protocol within H.530. The AuF securely responds back its decision to the visited gatekeeper that occurs during the terminal registration phase.

Communication between visited and home domain uses the generic H.501 protocol for H.323-based mobility management and intra/inter-domain communication. Upon reception of the AuF authentication and authorization decision, the visited gatekeeper and the MT agree on a fresh dynamic link key that they both share during their security association. This link key is used for protection of any further H.323 signalling communication between MT and V-GK; the multimedia signalling communication occurs locally to the visited domain and does not require interaction with the home domain.

H.530 takes a very simplistic security architecture into account where the MT shares only a pre-configured shared secret (e.g., a subscription password) with its AuF in the home domain but does not require the MT to share any a priori security associations with any visited domains. Security protection among the entities within domains as well across domains require only symmetric shared secrets; such could be established via interdomain service level agreements for example. H.530 re-uses existing H.235 security profiles such as H.235 Annex D for securing H.501/H.530 signalling messages across domains.

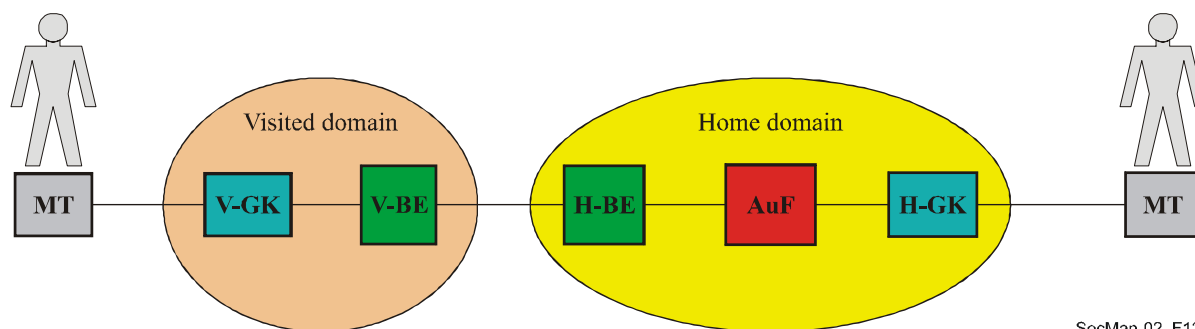


Figure 12 – H.530 Scenario

In order to provide stronger security for systems using personal identification numbers (PINs) or passwords to authenticate users, H.235 Annex H provides the framework for use of public-key methods to secure use of the PINs/passwords. One specific profile is presently defined which exploits the Encrypted Key Exchange method to negotiate a strong shared secret, protected from passive or active (man-in-the-middle) attacks. The framework permits the definition of new profiles using other public-key-based negotiation methods.

In the interest of better convergence with SIP, there are currently active and ongoing standardization activities within Study Group 16 that aim to use the secure real-time protocol (SRTP, RFC 3711) within H.235. One approach will be to use the IETF MIKEY key management within H.235 for end-to-end SRTP media key distribution.

Another, complementary approach will be to signal SRTP keying parameters in the clear end-to-end assuming some secure transport underneath; similar to the approach taken by SDP-sdescriptions in the IETF.

In addition to H.235, H.350 and H.350.2 provide for scalable key management using LDAP and SSL3. ITU-T Recommendation H.350.x provides several important capabilities that enable enterprises and carriers to securely manage large numbers of users of video and voice over IP services. H.350 provides a way to connect H.323, SIP, H.320 and generic messaging services into a directory service, so that modern identity management practices can be applied to multimedia communications. Further, the architecture provides a standardized place to store security credentials for these protocols.

H.350 does not alter the security architectures of any particular protocol. However, it does offer a standardized place to store authentication credentials where appropriate. It should be noted that both H.323 and SIP support shared secret authentication (H.235 Annex D and HTTP Digest, respectively). These approaches require that the call server have access to the password. Thus, if the call server or H.350 directory is compromised, passwords also may become compromised. These weaknesses may be due to weaknesses in the systems (H.350 directory or call servers) and their operation rather than in H.350 per se.

It is strongly encouraged that call servers and an H.350 directory mutually authenticate each other before sharing information. Further, it is strongly encouraged that communications between H.350 directories and call servers or endpoints be established over secure communication channels such as SSL or TLS.

It should be noted that access control lists on LDAP servers are a matter of policy and are not a part of the standard. System administrators are advised to use common sense when setting access control on H.350 attributes. For example, password attributes should only be accessible by the authenticated user, while address attributes might be publicly available.

6.2 IPCablecom System

The IPCablecom system enables cable television operators to provide IP-based real-time services (e.g., voice communications) over their networks that have been enhanced to support cable modems. The architecture of the IPCablecom system is defined in ITU-T Recommendation J.160. At a very high level, the IPCablecom architecture considers three networks: the "J.112 HFC access network", the "Managed IP network" and the PSTN. The Access Node (AN) provides connectivity between the "J.112 HFC access network" and the "Managed IP network". Both the Signalling Gateway (SG) and the Media Gateway (MG) provide connectivity between the "Managed IP network" and the PSTN. Figure 13 illustrates the reference architecture for IPCablecom.

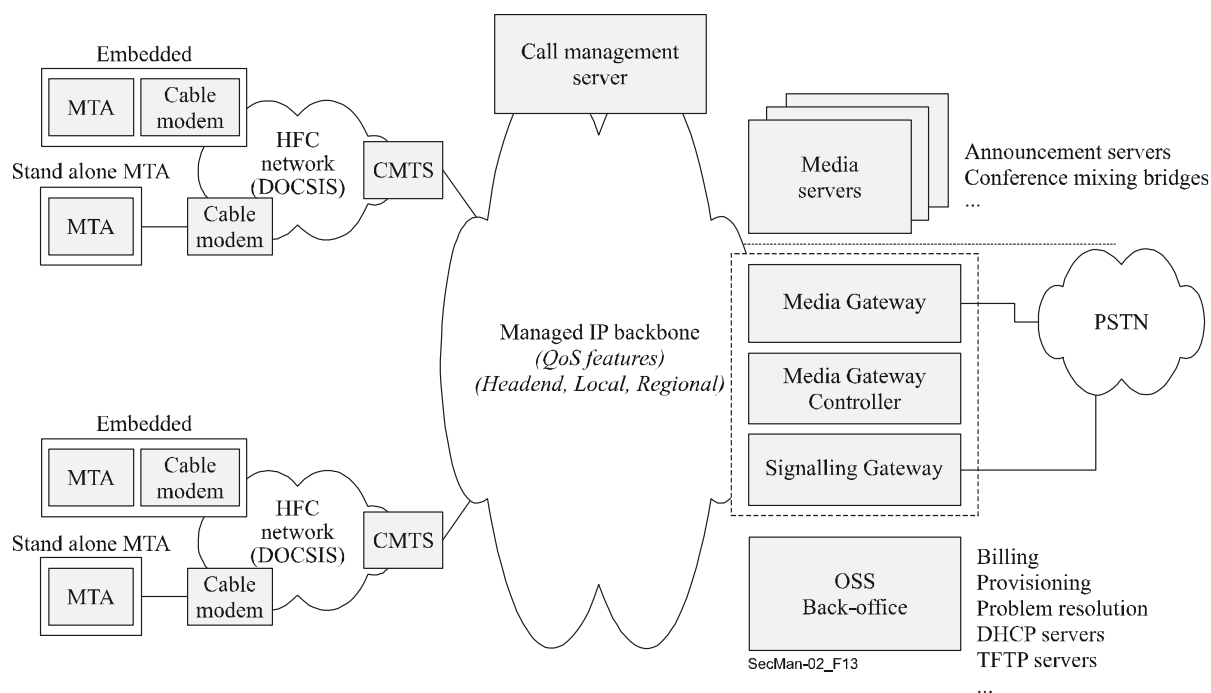


Figure 13 – IP Cablecom reference architecture [J.165]

The J.112 hybrid fiber-coaxial cable (HFC) access network provides high-speed, reliable and secure transport between the customer premises and the cable head-end. This access network may provide all J.112 capabilities including Quality of Service, and interfaces to the physical layer through a Cable Modem Termination System (CMTS).

The Managed IP network serves several functions. First, it provides interconnection between the basic IP Cablecom functional components responsible for signalling, media, provisioning, and quality of service establishment. In addition, the managed IP network provides long-haul IP connectivity between other Managed IP and J.112 HFC networks. The Managed IP network includes the following functional components: Call Management Server, Announcement Server, Signalling Gateway, Media Gateway, Media Gateway Controller, and several Operational Support System (OSS) back-office servers.

The *Call Management Server* (CMS) provides call control and signalling-related services for the media terminal adapter (MTA), access node, and PSTN gateways in the IP Cablecom network. The CMS is a trusted network element that resides on the managed IP portion of the IP Cablecom network. *Announcement Servers* are logical network components that manage and play informational tones and messages in response to events that occur in the network. The *Signalling Gateway* function sends and receives circuit-switched network signalling at the edge of the IP Cablecom network. For IP Cablecom, the Signalling Gateway function only supports non-facility-associated signalling in the form of SS7 (Facility-associated signalling in the form of multi-frequency tones is directly supported by the media gateway function). The *Media Gateway Controller* (MGC) receives and mediates call signalling information between the IP Cablecom network and the PSTN. It maintains and controls the overall call state for calls requiring PSTN interconnection. The *Media Gateway* (MG) provides bearer connectivity between the PSTN and the IP Cablecom IP network. Each bearer is represented as an endpoint and the MGC instructs the MG to set up and control media connections to other endpoints on the IP Cablecom network. The MGC also instructs the MG to detect and generate events and signals relevant to the call state known to the MGC. The *OSS back office* contains business, service, and network management components supporting the core business processes. The main functional areas for OSS are fault management, performance management, security management, accounting management, and configuration management. IP Cablecom defines a limited set of OSS functional

components and interfaces to support MTA device provisioning and Event Messaging to carry billing information.

6.2.1 Security Issues in IPCablecom

Each of IPCablecom's protocol interfaces is subject to threats that could pose security risks to both the subscriber and the service provider. For example, the media stream path may traverse a large number of potentially unknown Internet service and backbone service providers' wires. As a result, the media stream may be vulnerable to malicious eavesdropping, resulting in a loss of communications privacy.

6.2.2 Security mechanisms in IPCablecom

Security in IPCablecom is implemented in the lower stack elements and hence mostly uses mechanisms defined by the IETF. The IPCablecom architecture addresses these threats by specifying, for each defined protocol interface, the underlying security mechanisms (such as IPsec) that provide the protocol interface with the security services it requires. In the context of the X.805 architecture, the overview of the security services for IPCablecom address all the nine cells resulting from the three planes and layers in Figure 1. For example, the services of the signalling protocols for the control plane are supported by IPsec. The management infrastructure security is achieved through the use of SNMP v3.

The security services available through IPCablecom's core service layer are authentication, access control, integrity, confidentiality and non-repudiation. An IPCablecom protocol interface may employ zero, one or more of these services to address its particular security requirements.

IPCablecom security addresses the security requirements of each constituent protocol interface by:

- identifying the threat model specific to each constituent protocol interface;
- identifying the security services (authentication, authorization, confidentiality, integrity, and non-repudiation) required to address the identified threats;
- specifying the particular security mechanism providing the required security services.

The security mechanisms include both the security protocol (e.g., IPsec, RTP-layer security, and SNMPv3 security) and the supporting key management protocol (e.g., IKE, PKINIT/Kerberos). Also, IPCablecom core security services include a mechanism for providing end-to-end encryption of RTP media streams, thus substantially reducing the threat to privacy. Figure 14 provides a summary of all the IPCablecom security interfaces. If the key management protocol is missing, it means that it is not needed for that interface. IPCablecom interfaces that do not require security are not shown in Figure 14.

The IPCablecom security architecture divides device provisioning into three distinct activities: subscriber enrolment, device provisioning and device authorization. The *subscriber enrolment* process establishes a permanent subscriber billing account that uniquely identifies the MTA to the CMS via the MTA's serial number or MAC address. The billing account is also used to identify the services subscribed to by the subscriber for the MTA. Subscriber enrolment may occur in-band or out-of-band. The actual specification of the subscriber enrolment process is out of scope for IPCablecom and may be different for each service provider. For *device provisioning*, the MTA device verifies the authenticity of the configuration file it downloads by first establishing SNMPv3 security (using Kerberos-based Authentication and Key management) between itself and the Provisioning Server. The Provisioning Server then provides the MTA with the location of the configuration file, and a hash of the configuration file. The MTA retrieves the configuration file, performs a hash on the configuration file, and compares the result with the hash that was provided by the Provisioning Server. The configuration file has been authenticated if the hashes match. The configuration file may be optionally encrypted for privacy (SNMPv3 privacy must also be enabled in order to securely pass the configuration file encryption key to the MTA). *Device authorization* is when a provisioned MTA Device authenticates itself to the Call Management Server, and establishes a security association with

that server prior to becoming fully operational. Device authorization allows subsequent call signalling to be protected under the established security association.

Both signalling traffic and media stream can be protected. All signalling traffic, which includes QoS signalling, call signalling, and signalling with the PSTN Gateway Interface, will be secured via IPsec. IPsec security association management will be done through the use of two key management protocols: Kerberos/PKINIT and IKE. Kerberos/PKINIT will be used to exchange keys between MTA clients and their CMS server; IKE will be used to manage all other signalling IPsec SAs. As regards the media streams, each media RTP packet is encrypted for privacy, and authenticated to verify the integrity and the origin of the packet. The MTAs have an ability to negotiate a particular encryption algorithm, although the only required encryption algorithm is AES. Each RTP packet may include an optional message authentication code (MAC). The MAC algorithm can also be negotiated, although the only one that is currently specified is MMH. The MAC computation spans the packet's unencrypted header and encrypted payload.

Keys for the encryption and MAC calculation are derived from the end-to-end secret and optional pad, which are exchanged between sending and receiving MTA as part of the call signalling. Thus, the key exchanges for media stream security are secured themselves by the call signalling security.

Security is also provided for the OSS and billing system. The SNMP agents in IPCablecom devices implement SNMPv3. The SNMPv3 User Security Model [RFC 2274] provides authentication and privacy services for SNMP traffic. SNMPv3 view-based access control [RFC 2275] may be used for access control to MIB objects.

The IKE key management protocol is used to establish encryption and authentication keys between the Record Keeping Server (RKS) and each IPCablecom network element that generates Event Messages. When the network IPsec Security Associations are established, these keys must be created between each RKS (primary, secondary, etc.) and every CMS and AN. The key exchange between the MGC and RKS may exist and is left to vendor implementation in IPCablecom Phase 1. The Event Messages are sent from the CMS and AN to the RKS using the RADIUS transport protocol, which is in turn secured by IPsec.

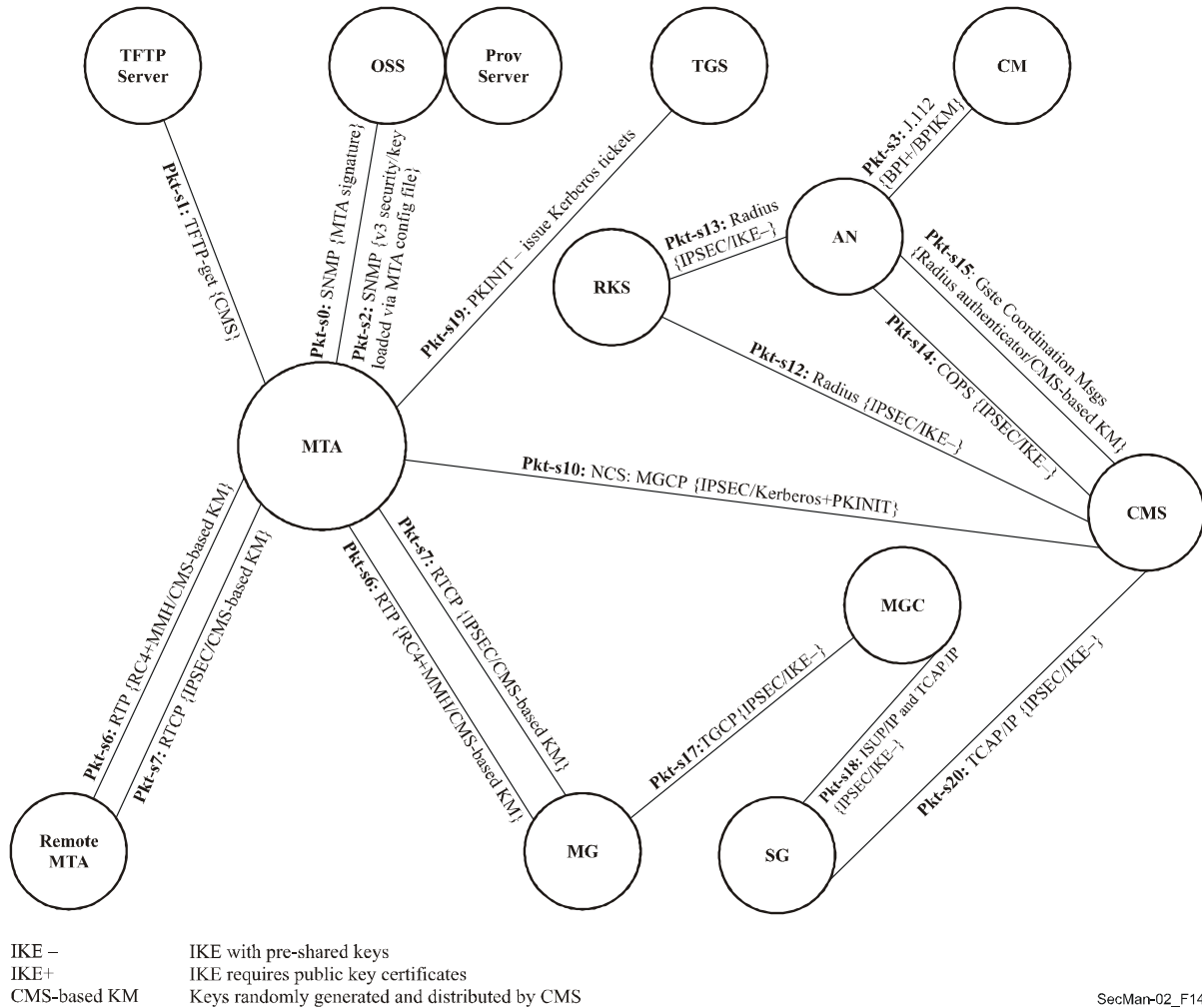


Figure 14 – IPcablecom security interfaces (labelled as <label>: <protocol> { <security protocol> / <key management protocol> })

6.3 Secure Fax Transmission

Facsimile is a very popular application. Initially defined for transmission over the PSTN (ITU-T Recommendation T.4), then for ISDN (ITU-T Recommendation T.6), more recently it received extensions for transport over IP networks (including the Internet) for non real-time transmission (email relay) using ITU-T Recommendation T.37 and for real-time (using RTP) using ITU-T Recommendation T.38. Two typical security issues faced by fax transmission – regardless of whether PSTN, ISDN, or IP – concerns authentication (and sometimes non-repudiation) of a connection, and the confidentiality of the data transmitted. T.37 and T.38 however have made these issues even more important due to the distributed nature of the IP network.

ITU-T Recommendation T.36 defines two independent technical solutions that may be used in the context of secure facsimile transmission for encrypting the documents exchanged. The two technical solutions are based upon the HKM/HFX40 algorithms (Annex A/T.36) and the RSA algorithm (Annex B/T.36). Even though both limit session keys to 40 bits (due to national regulations at the time of approval of the Recommendation, 1997), a mechanism is specified to generate a redundant session key (from a 40-bit long session key), for algorithms that require longer keys. Annex C/T.36 describes the use of the HKM system to provide secure key management capabilities for facsimile terminals by means of one way registration between entities X and Y, or of secure transmission of a secret key between entities X and Y. Annex D/T.36 covers the procedures for the use of the HFX40 carrier

cipher system to provide message confidentiality for facsimile terminals. Finally, Annex E/T.36 describes the HFX40-I hashing algorithm, in terms of its use, the necessary calculations and the information to be exchanged between the facsimile terminals to provide integrity for a transmitted facsimile message as either a selected or pre-programmed alternative to the encryption of the message.

Additionally, T.36 defines the following security services:

- Mutual authentication (mandatory).
- Security service (optional), which includes Mutual authentication, Message integrity, and Confirmation of message receipt.
- Security service (optional), which includes Mutual authentication, Message confidentiality (encryption), and Session Key establishment.
- Security service (optional), which includes Mutual authentication, Message integrity, Confirmation of message receipt, Message confidentiality (encryption), and Session Key establishment.

Four service profiles are defined based on these security services defined above, as shown in Table 2 below.

Table 2 – Security profiles in Annex H/T.30

Security services	Service profiles			
	1	2	3	4
Mutual authentication	X	X	X	X
<ul style="list-style-type: none"> • Message integrity • Confirmation of message receipt 		X		X
<ul style="list-style-type: none"> • Message confidentiality (encryption) • Session Key establishment 			X	X

6.3.1 Fax security using HKM and HFX

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

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

Key management is provided using the HKM system defined in Annex B/T.36. Two procedures are defined: the first being registration and the second being the secure transmission of a secret key. Registration establishes mutual secrets and enables all subsequent transmissions to be provided securely. In subsequent transmissions, the HKM system provides mutual authentication, a secret session key for document confidentiality and integrity, confirmation of receipt and a confirmation or denial of document integrity.

Document confidentiality is provided using the cipher defined in Annex D/T.36. The cipher uses a 12-decimal digit key, which is approximately equivalent to a 40 bit session key.

Document integrity is provided using the system defined in Annex E/T.36 and Recommendation T.36 defines the hashing algorithm including the associated calculations and information exchange.

In the registration mode, the two terminals exchange information which enables entities to uniquely identify each other. This is based upon the agreement between the users of a secret one-time key. Each entity stores a 16-digit number which is uniquely associated with the entity with which it has carried out registration.

When it is required to send a document securely, the transmitting terminal transmits the 16-digit secret number associated with the receiving entity together with a random number and an encrypted session key as a challenge to the receiving entity. The receiving terminal responds by transmitting the 16-digit key associated with the transmitting entity along with a random number and a re-encrypted version of the challenge from the transmitting entity. At the same time it transmits a random number and an encrypted session key as a challenge to the transmitting entity. The transmitting terminal responds with a random number and a re-encrypted version of the challenge from the receiving entity. This procedure enables the two entities to mutually authenticate each other. At the same time, the transmitting terminal transmits a random number and the encrypted session key to be used for encrypting and hashing.

After transmission of the document, the transmitting terminal transmits a random number and an encrypted session key as a challenge to the receiving entity. At the same time, it sends a random number and encrypted hash value, which enables the receiving entity to ensure the integrity of the received document. The receiving terminal transmits a random number and the re-encrypted version of the challenge from the transmitting entity. At the same time, it sends a random number and encrypted Integrity Document to act as confirmation or denial of the integrity of the received document. The hashing algorithm used for document integrity is carried out on the whole document.

An override mode is provided, which does not involve the exchange of any security signals between the two terminals. The users agree on a one-time secret session key to be entered manually. This is used by the transmitting terminal to encrypt the document and by the receiving terminal to decrypt the document.

6.3.2 Fax security using RSA

Annex H/T.30 specifies the mechanisms to offer security features based on the *Rivest, Shamir & Adleman* (RSA) cryptographic mechanism. For details on the RSA algorithm, see [ApplCryp, pp.466-474]. The coding scheme of the document transmitted with security features may be of any kind defined in Recommendations T.4 and T.30 (Modified Huffman, MR, MMR, Character mode as defined in Annex D/T.4, BFT, other file transfer mode defined in Annex C/T.4).

The basic algorithm used for the digital signature (authentication and integrity type services) is the RSA using a pair "public key"/"secret key".

When the optional confidentiality service is offered, the token containing the session key "Ks", used for enciphering the document, is encrypted also by the means of RSA algorithm. The couple of keys used for this purpose called ("encipherment public key"/"encipherment secret key") is not the same one as that used for authentication and integrity types services. This is for decoupling the two kinds of use.

The implementation of RSA used in Annex H is described in ISO/IEC 9796 (Digital signature scheme giving message recovery).

For encipherment of the token containing the session key, the rules of redundancy when processing the algorithm RSA are the same ones as those specified in ISO/IEC 9796. It should be noted that some administrations may require the *Digital Signature Algorithm* (DSA) mechanism [ApplCryp, pp.483-502] to be implemented in addition to RSA.

By default, *certification authorities* are not used in the scheme of Annex H/T.30, however they may optionally be used to certify the validity of the public key of the sender of the facsimile message. In such a case, the public key may be certified as specified in the Recommendation X.509. The means to transmit the certificate of the public key of the sender is described in Annex H, but the precise format

of the certificate is left for future study and the actual transmission of the certificate is negotiated in the protocol.

As a mandatory feature, a *registration mode* is provided. It permits the sender and the receiver to register and store the public keys of the other party in confident manner prior to any secure facsimile communication between the two parties. Registration mode can avoid the need for the user to enter manually in the terminal the public keys of its correspondents (the public keys are fairly long, 64 octets or more).

Because the registration mode permits the exchange of public keys and allows them to be stored in the terminals, it is not necessary to transmit them during the facsimile communications.

As described in this annex, some signatures are applied on the result of a "hash function".

The hash functions that can be used are either (SHA-1, *Secure Hash Algorithm*), an algorithm which comes from the National Institute of Standards and Technology (NIST) in the USA, or MD-5 (RFC 1321). For SHA-1, the length of the result of the hashing process is on 160 bits, and for MD-5, the length of the result of the hashing process is on 128 bits. A terminal conforming to Annex H/T.30 may implement either SHA-1, MD-5, or both. The use of one algorithm or the other is negotiated in the protocol (see further).

The encipherment of the data for provision of the confidentiality service is optional. Five optional encipherment schemes are registered in the scope of Annex H/T.30: FEAL-32, SAFER K-64, RC5, IDEA and HFX40 (as described in Recommendation T.36). In some countries, their use may be subject to national regulation.

Other optional algorithms may also be used. They are chosen conforming to the ISO/IEC 9979 (Procedure for registering cryptographic algorithms).

The capability of the terminal to handle one of these algorithms and the actual use of a particular one during the communication is negotiated in the protocol. A session key is used for encipherment. The basic length of a session key is 40 bits. For algorithms that use a 40-bit session key (e.g., HFX40), the session key "Ks" is the key actually used in the encipherment algorithm, and for algorithms which require keys longer than 40 bits (e.g., FEAL-32, IDEA, SAFER K-64 requiring respectively: 64 bits, 128 bits and 64 bits), a redundancy mechanism is performed to get the necessary length. The resultant key is called the "redundant session key". The "redundant session key" is the key which is actually used in the encipherment algorithm.

6.4 Network Management Applications

As noted in the section on requirements for security framework, it is imperative to secure the management traffic used to monitor and control the telecommunications network. The management traffic is categorized usually in terms of information required to perform fault, configuration, performance, accounting and security management functions. The area of security management deals with both setting up a secure management network as well as managing the security of information related to the three security planes and layers of the security architecture. The latter is described in the this section.

Traditionally in telecommunications network, management traffic is often transmitted on a separate network which carries only the network management traffic and not users' traffic. This network is often referred to as the Telecommunications Management Network (TMN) described in ITU-T Recommendation M.3010. TMN is separated and isolated from the public network infrastructure so that any disruptions due to security threats in the end-user plane in the public network do not spread to TMN. As a result of this separation, it is relatively easy to secure the management network traffic because access to this plane is restricted to authorized network administrators, and traffic is restricted to valid management activities. With the introduction of next generation networks, traffic for end-user application may sometimes be combined with management traffic. While this approach minimizes costs by requiring only a single integrated network infrastructure, it introduces many new security challenges. Threats in the end-user plane now become threats to the management and control planes. The management plane now becomes accessible to the multitude of end-users, and many types of malicious activities become possible.

To provide a complete end-to-end solution, all security measures (e.g., access control, authentication) should be applied to each type of network activity (i.e., management plane activity, control plane activity, and end-user plane activity) for the network infrastructure, network services, and network applications. A number of ITU-T Recommendations exist which focus specifically on the security aspect of the management plane for network elements (NE) and management systems (MS) that are part of the network infrastructure.

While there are many standards as described below to secure the management information required to maintain the telecommunications infrastructure, another area that falls within management relates to environments where different service providers need to interact to offer end-to-end services such as leased line to customers crossing geographical boundaries, or regulatory or government institutions in support of disaster recovery.

6.4.1 Network Management Architecture

The architecture for defining the network management of a telecommunications network is defined in Recommendation M.3010 and the physical architecture is shown in Figure 15. The management network defines interfaces that determine the exchanges required to perform the OAM&P functions at different levels.

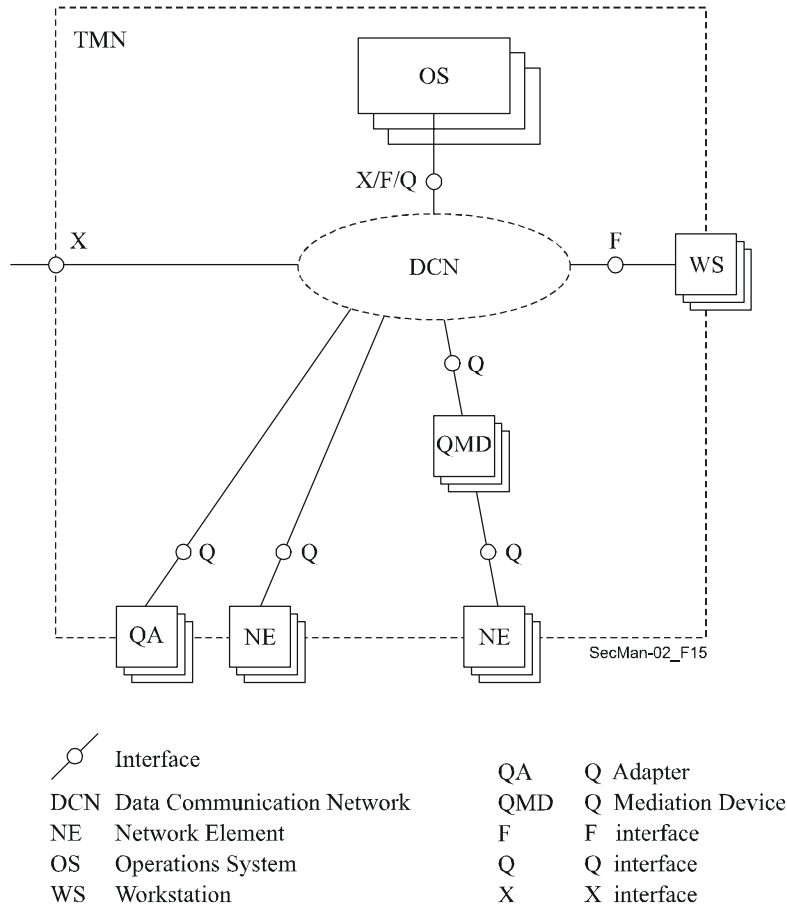


Figure 15 – Example of Physical Architecture in M.3010

From a security perspective, the requirements for the different interfaces vary. The Q interface lies within a single administrative domain, while the X interface lies between different administrative domains that may be owned by different providers. While the need for security services is present for both Q and X, the countermeasures required for the X interface are more robust and necessary. An overview of the security threats, vulnerabilities and security measures for these interfaces is given in ITU-T Recommendation M.3016, with aspects specific to the X interface being detailed in ITU-T Recommendation M.3320. The protocol aspects for the different communication layers are specified in ITU-T Recommendations Q.811 and Q.812.

There are two facets when discussing security in the context of management. One of them relates to the management plane for an end-to-end activity (e.g., VoIP services). Management activity that requires administering users should be performed in a secure manner. This is referred to as *security of management information* exchanged over the network to deploy an end-to-end application. The second facet is management of security information. Irrespective of the application, e.g., VoIP or trouble-reporting activity between two service providers, security measures such as use of encryption keys should also be managed. This is often referred to as *management of security information*. The PKI defined in the previous section is an example of this facet. ITU-T Recommendation M.3400 defines a number of functions related to both these facets.

Using the framework from X.805, several Recommendations addressing management functions are available for the three cells of the management plane (refer to Figure 1). The sub-sections below illustrate some of these Recommendations and show how they address the security needs. In addition to the Recommendations for the three layers of the management plane, there are others that define generic or common services such as reporting alarms when there is a physical security violation, audit functions, and information models defining levels of protection for different targets (i.e., management entities).

6.4.2 Management Plane and Infrastructure Layer Intersection

This cell addresses how to secure the management activity of infrastructure elements of the network, namely transmission and switching elements and links connecting them as well as the end systems such as servers. As an example, the activities such as provisioning the network element should be performed by an authorized user. An end-to-end connectivity may be considered in terms of access network(s) and core network(s). Different technologies may be used in these networks. Recommendations have been developed to address both access and core networks. One such case discussed here is the Broadband Passive Optical Network (BPON) used in the access. Administering the user privileges for such an access network is defined using Unified Modelling Methodology in Recommendation Q.834.3 and management exchange using CORBA (Common Object Request Broker Architecture) is specified in Q.834.4. The interface described in these Recommendations is the Q interface shown in Figure 15. It is applied between the Element Management System and the Network Management Systems. The former is used to manage individual network elements and thus is aware of the internal details of the hardware and software architectures of the elements from one or more suppliers whereas the latter is performing the activities at the end-to-end network level and span multiple supplier management systems. Figure 16 shows the various objects used for creating, deleting, assigning, and using access control information for users of the Element Management System. The user permission list contains for each authorized user the list of management activities that are permitted. The Access Control Manager verifies the user Id and password of the user of the management activity and grants the access to the functionality allowed in the permission list.

6.4.3 Management Plane and Services Layer Intersection

The intersection between the management plane and services layer pertains to securing the activities involved in monitoring and controlling the network resources provisioned for delivering services by the provider. ITU-T Recommendations address two aspects for this intersection. One aspect is assuring that appropriate security measures are available for services available in the network. An example of this aspect is assuring that only valid users are allowed to perform the operations associated with provisioning a service. The second aspect is defining which administrative and management exchanges are valid. Such a definition will help to detect security violations. When there are security violations, they are often managed using specific management systems.

An example of a Recommendation addressing the first aspect, management activity of a service, is ITU-T Recommendation M.3208.2 on connection management. The service customer who owns pre-provisioned links uses this service to form an end-to-end leased circuit connection. This connection management service allows a subscriber to create/activate, modify and delete the leased circuits within the limits of the pre-provisioned resources. Because the user provisions the end-to-end connectivity, it is necessary to assure that only authorized users are allowed to perform these operations. The security dimensions defined for the management activity associated with this service is a subset of the eight discussed in section 2.3. These are peer entity authentication, data integrity control (to prevent unauthorized modification of data in transit), and access control (to assure one subscriber does not gain access maliciously or accidentally to another subscriber's data).

ITU-T Recommendation M.3210.1 is an example of a Recommendation that defines the administrative activities associated with the management plane for wireless services. This corresponds to the second aspect discussed above.

In a wireless network, as the users roam from the home network to the visited network, they may traverse different administrative domains. The services defined in ITU-T Recommendation M.3210.1 describe how the fraud management domain in the home location collects appropriate information about a subscriber once registered on the visited network. Scenarios a) and b) in Figure 17 show initiation of the monitoring management activity either by the home network or by the visited network. The fraud detection system in the home network requests information on the activities when a subscriber registers to a visited network until leaving the network on deregistering from the network. Profiles may then be developed related to usage based on call detail records and tracking (analyzing) at the service level or for a subscriber. Fraud detection system can then analyze and generate appropriate alarms for fraudulent behavior.

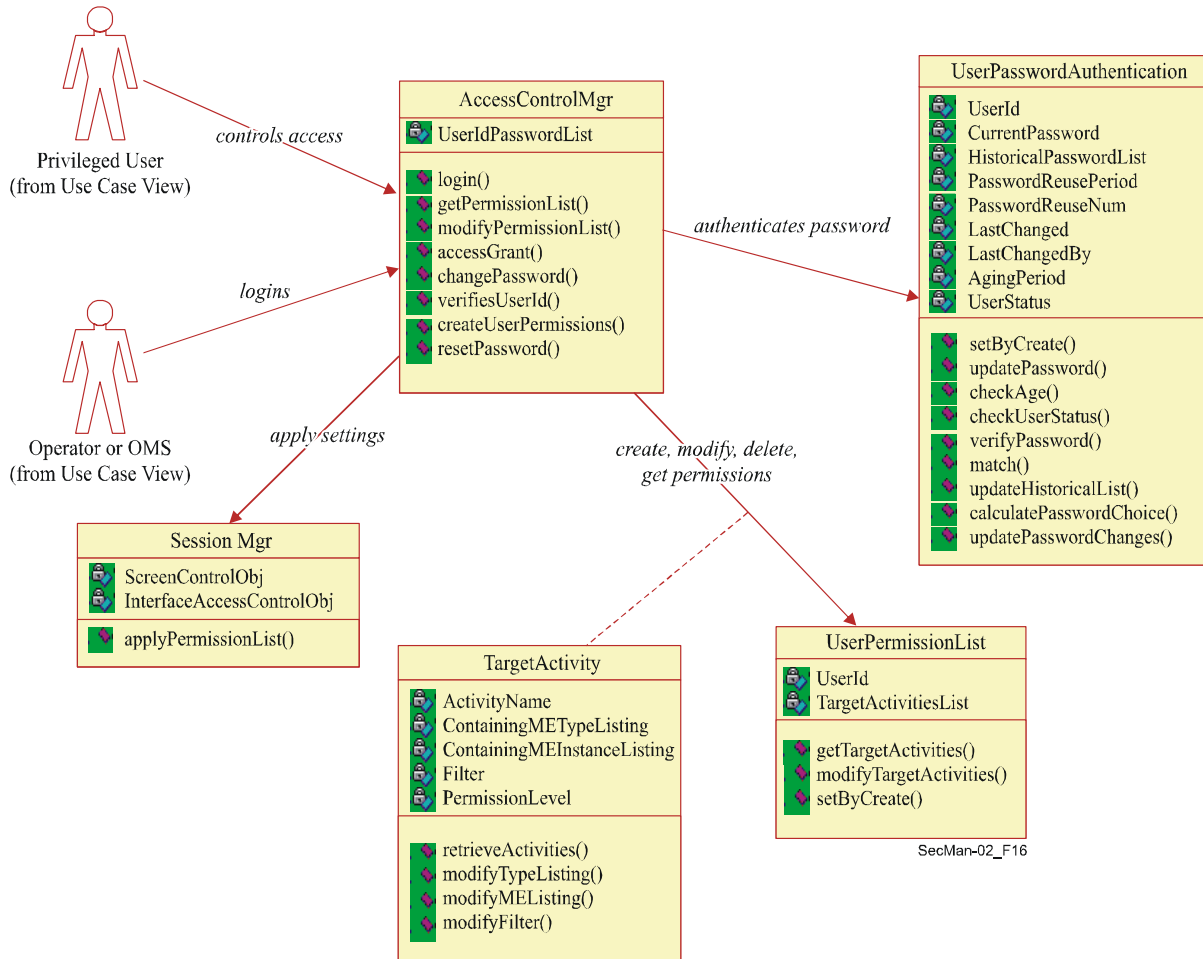


Figure 16 – Administering User Privileges in Q.834.3

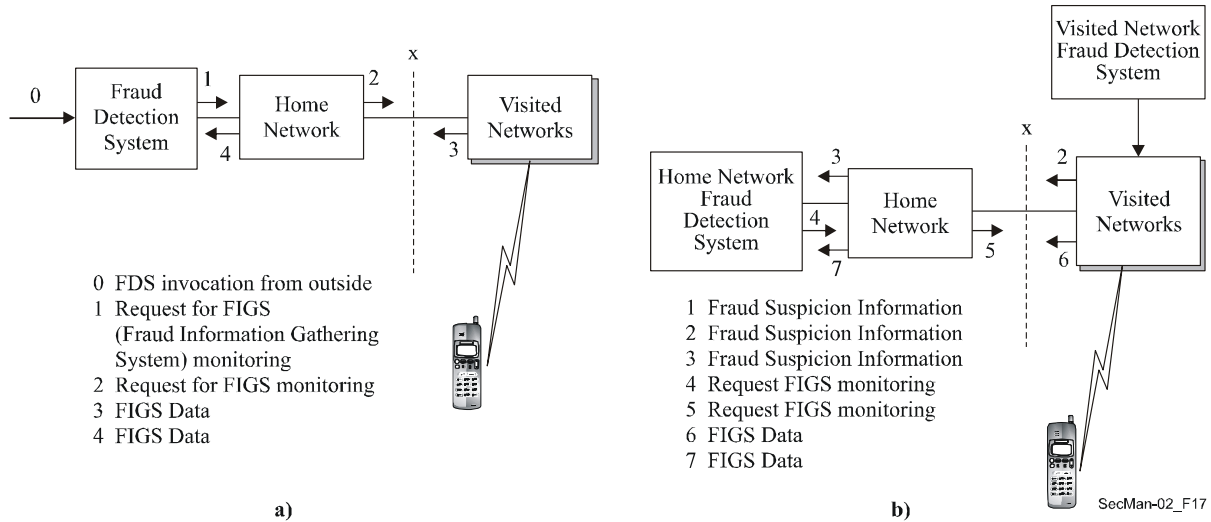


Figure 17 – Fraud Management for Wireless Services from Recommendation M.3210.1

6.4.4 Management Plane and Application Layer Intersection

The third cell corresponding to the intersection of management plane and application layer corresponds to securing end-user network-based applications. The applications such as messaging and directory have been defined in the Recommendations of the X.400 and X.500 series.

Another class of applications where management activities are to be secured is management applications themselves. This statement appears to be circuitous and best explained using examples. The end user for these applications is the management (operations) personnel in the service provider's administration. Consider the case where one service provider uses connection services from another provider in order to offer an end-to-end connectivity service. Depending on the regulatory or market environment, some service providers may offer access services, and others, referred to as *inter-exchange carriers*, may offer long-distance connectivity. The inter-exchange carriers lease access services from the local provider for end-to-end connectivity across geographically distributed locations. When a loss of service is encountered a management application called trouble report administration is used to report troubles between management systems. The user of these systems as well as the application itself requires authorization to report troubles on the services. Authorized systems and users should perform necessary actions for retrieving the status of the reported troubles. Figure 18 illustrates the interactions that must be carried out in a secure manner. Similar to administering mailboxes for email application, access privileges are administered to prevent unauthorized access to trouble reports. A service provider is permitted to report troubles only on the services they lease and not on services leased by a different provider.

Recommendation X.790 defines this management application and uses mechanisms such as access control list, two-way authentication to secure the activities. This application along with the security mechanisms for authentication has been implemented using these Recommendations and have been deployed.

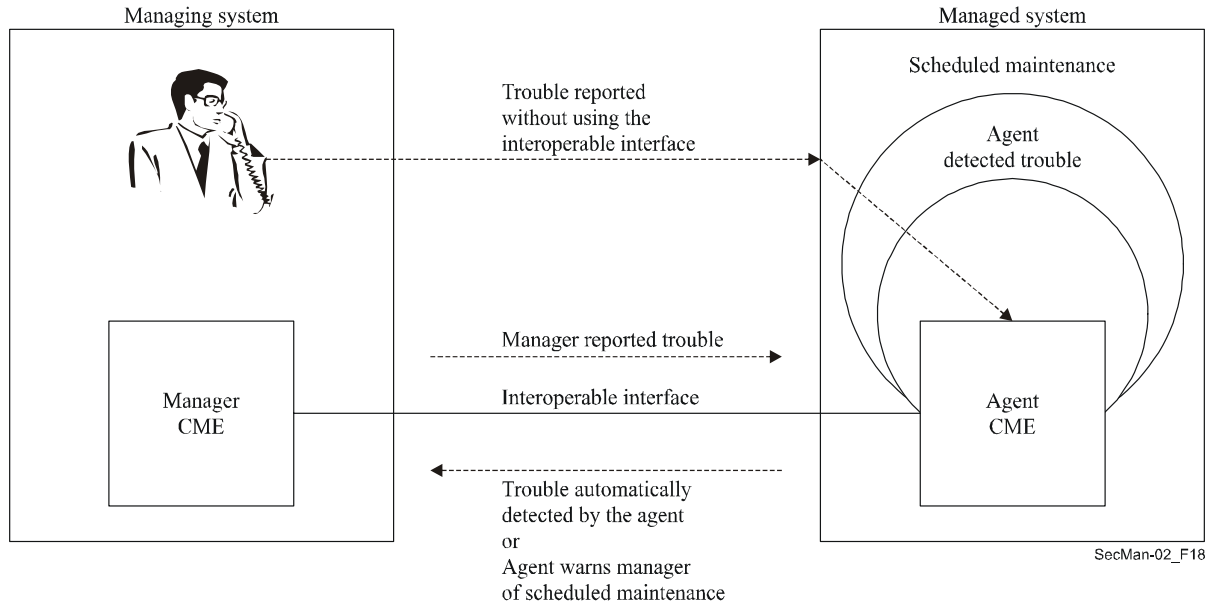


Figure 18 – Trouble Management Report Creation defined in ITU-T Recommendation X.790

6.4.5 Common Security Management Services

Recommendations X.736, X.740 and X.741 define common services that are applicable for all three cells of the management plane when Common Management Information Protocol (CMIP) is used at the interface. A brief description of the services included in these recommendations is described below. Note that all these functions are appropriately considered to be management plane activities.

6.4.5.1 Security Alarm Reporting Function: Alarm Reporting in general is a key function in management interfaces. When a failure is detected either resulting from the operational perspective (a failure of the circuit pack) or a violation of the security policy an alarm is reported to managing system. The alarm reports include a number of parameters so that managing system is able to determine the cause of the failure and take corrective action. The parameters for any event includes a mandatory field called event type and a set of other fields referred to as event information. The latter consists of information such as the severity of the alarm, probable causes for the alarm, detector of the security violation, etc. The alarm causes are associated with event types as shown in the table below.

Table 3 – Security alarm causes

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

These alarm causes are explained further in X.736. Several of the alarm causes relate to threats discussed in the earlier sections.

6.4.5.2 Security Audit Trail Function: In order for a security management user to record and have an audit trail of the security violations, Recommendation X.740 identifies a number of events subject to audit trail. These are connections, disconnections, security mechanism utilizations, management operations and usage accounting. The model uses the logging mechanism defined Recommendation X.735, a general log to record any event generated at the managed system. As a result of the audit trail function two events are defined that pertain to security violations. These are service report and usage report. Service report pertains to provision, denial or recovery of a service. The usage report is used to indicate that a record containing statistical data relevant to security has been created. As with any event a number of cause values have been defined relative to the service report. These are for example request for service, denial of service, service failure, service recovery, etc. New event types may be defined if appropriate because the two noted in the recommendation may not be sufficient in the future.

6.4.5.3: A very detailed definition for the model associated with assigning access control to various managed entities is described in Recommendation X.741. The requirements satisfied by the access control definitions in this Recommendation include protecting management information from unauthorized creation, deletion, modification, allowed operations on the entities are consistent with the access rights for the initiators of the operations, and prevent the transmission of management information to unauthorized recipients. Various levels of access controls are defined to meet the above requirements. For management operations, provisions in the recommendation facilitates access restrictions at multiple levels: managed entity as a whole, attributes of the entity, values of attributes, context of the access and actions on the entity. A number of schemes such as access control list, capability based, label based and context based have been identified and an access control policy may apply one or more of these schemes. In this model based on the policy and the access control information (ACI), decision to permit or otherwise the requested operation is determined. ACI includes for example, rules, identity of the initiator, identities of the targets to which access is requested, information pertaining to the authentication of the initiator etc. The model is very feature rich and in any application all capabilities may not be required.

6.4.5.4 CORBA based Security services: While X.700 series Recommendations assumed the use of CMIP as the management interface protocol, there have been other trends in the industry that introduced the use of Common Object Request Broker based protocol, services and object models for the management interfaces. Recommendation Q.816 defines a framework for using these services in the context of management interfaces. To support the security requirements for these interfaces, this recommendation refers to OMG specification of Common Services for Security.

6.5 E-prescriptions

The provision of health care requires, and generates, a wide variety of data and information, which need to be collected, processed, distributed, accessed and used – securely and respectful of strict ethical and legislative rules. This is particularly vital for clinical and managerial information, but also important for other types of information such as epidemiological, literature and knowledge database information.

The sources of these types of data and information are within and outside the Health Care infrastructure and located at varying distances from their respective users. In practice, users require and generate a mix of these types of information and at differing stages of their respective functions, e.g., a physician may consult a knowledge database while examining a patient and would make a relevant entry onto the patient's record, which may be used for billing purposes.

Health care encounters and transactions are multi-faceted. They occur, for example, between a patient and a physician; between two physicians; between a physician and an expert consultant; between a patient and a health institution such as a test laboratory, a pharmacy or a rehabilitation centre. Such encounters may occur in one's own community, in another part of the country or abroad. All such encounters require data and information prior to the actual start of the encounter, and generate the same during the encounter or soon thereafter. Such data and information could be in differing volumes, at differing times and in differing forms such as voice, numbers, text, graphics and static or dynamic images, and are often a judicious mix of these.

The sources and repositories of such data and information could spread over differing locations and would take differing forms, for example, complete patients records, hand-written prescriptions, and reports by a physician, a consultant or a laboratory.

Traditionally, all such encounters were face to face, and the spoken and the written word were the main modes of communications and medical record keeping, while transport was mainly by public and private services using road, rail or air transportation. As the telephone services network grew, it became the communication network of the health professionals and institutions, nationally and internationally, until the advent and growth of modern tools of health Telematics.

The uses of technology in the clinical/medical aspects of the Health Care services steadily grew and included instrumentation and equipment, particularly sensing and measuring equipment, laboratory services, static and dynamic imaging. With the growth of the uses of such technologies and of the variety and sophistication of these, it was inevitable that many of such technological services became separated from the mainstream Health Care institutions – separated in distance and more significantly in management. So, the communications between such technology-based services and the mainstream Health Care services became an important consideration in the efficacy and economy of such services.

The popular use of information and communications technologies (ICT) by the health sector started over 25 years ago with simple electronic messaging (E-mail) carrying purely alphanumeric notes and reports. Just as voice communications was the main motive for the installation of telephones in physician's cabinets and Health Care institutions, E-mail was the main initial justification for the installation of modern telecommunication links. And, as E-mail services grew, so did the demands on their performance and geographic coverage: more locations at more speed and with more bandwidth to cater for the growing attachments to the e-mail messages. The past ten years have witnessed an exponential growth in the uses of e-mail in the health sector, within and between countries, even in the poorest countries, particularly over the Internet. For example, e-Transactions are taking over those functions that do not really require face-to-face encounters, such as preparing and sending

prescriptions and reports, fixing appointments and scheduling services, referring patients and, where the telecommunications services performance permit, also transmitting medical images and their associated expert readings, either written or oral.

Another level of sophistication of the uses of ICT is Telemedicine, which is "the provision of medical care using audio, visual and data communications", including the actual diagnosis, examination and even care of a patient who is remotely located. Telemedicine is an important and growing field and is expected to change many of the traditional approaches in Health Care; indeed it is the start of a new paradigm in medical care.

Another area that is relatively speaking not recent, but will usefully expand with the spread of Telematics support, is the access to and uses of knowledge-based systems. These systems, which are also known as expert systems and decision support systems, are systems that provide expert advice and guidance on medico-scientific issues and procedures. For example, given a patient's coordinates and symptoms, it could provide diagnostic support, suggest additional tests or propose a treatment.

All the above-cited developments are also having a major impact on the relevant Management Information Systems (MIS) needed for and used in the health sector, e.g., Hospital MIS. These are no more systems for the administrative management of hospital care to patients, from admission to discharge/transfer, but include a multitude of intelligent, medical-staff-friendly interfaces to, for example, clinical decision support systems, Telemedicine links, Website portals, etc.

Two other recognized realities of Health Care staff and patients should also be cited: their mobility and their need for having their hands free and thus dedicated to the medical care itself. The mobility feature means that they can get to the medical information required, e.g., an Electronic Patient Record, or to a tool or instrument, from any remote location and whenever necessary subject to their verification, within a building or a town, but also within whole countries and between countries. And, the hands free feature means that solutions have to be found for identification and authorization that do not engage the medical worker in a manual intervention, e.g., to open a door or to key onto a computer keyboard.

Thus, Health Care is a profoundly information-intensive sector, in which the collection, flow, processing, presentation and distribution of health, and health-related, data and information, are key to the efficacy, efficiency and economy of the operations and development of the Health Care services, within a country and between countries.

A crucial requirement is that all such flow must be fulfilled securely and confidentially, and in strict adherence to ethical and legal rules and regulations.

6.5.1 PKI and PMI considerations for e-health applications

Through its chaining of certification authorities, the PKI reproduces a hierarchical structure of the real world, whether it is a geopolitical hierarchy (regions-countries-states-localities), or thematic (Health-Medicine-Surgery-Specialized surgery-suppliers, etc.). Furthermore, due to the fact that the health sector is ubiquitous, hierarchical far-reaching and increasingly interactive across frontiers, the definition of a standardized PKI/PMI for health is becoming a manifest necessity.

The technical interoperability of health systems has to be assured by the exhaustive use of technology standards. Most security solutions providers have already adopted standards such as ITU-T Recommendation X.509. Being user authentication a critical application that is dependent on local information, the freedom to choose a given PKI and PMI should not affect the capacity of the user to interoperate with persons certified by other PKI/PMI in the health sector (which of course extends to at least a minimum standardization regarding access control and other related policies of the health sector). To achieve this, different strategies can be put in place that could include the cross-recognition of the different infrastructures or the use of a common root. The adoption of technology standards, the technical interoperability of the different infrastructures and the standardization of certain policies will guaranty a fully efficient and integrated environment for the worldwide health transactions.

6.5.2 Salford's E-prescription System

The E-prescription system described in [Policy] is a good example of applied PKI and PMI applied to e-health. Given the large numbers of professionals involved in the Electronic Transmission of Prescriptions (ETP) programme in the UK (34,500 general practitioners, 10,000 prescribing nurses rising to 120,000 over the next few years, 44,000 registered pharmacists and 22,000 dentists), and the very few authorizations that are actually required (i.e., various permission levels for prescribing, dispensing, and entitlements to free prescriptions), then role-based access controls (RBAC) seem to be the ideal authorization mechanism to use for ETP. When this is coupled with the number of potential patients in the UK (60 million), and the fact that free prescriptions account for 85% of prescribed items [FreePresc], then RBAC should also be used to control access to free prescriptions if possible. Given the very large numbers of people who need to be authorized/entitled, it is essential that the management of roles be distributed to competent authorities, rather than try to have it centralized, otherwise the system will become unmanageable.

Each professional has an authoritative body who grants them the right to engage in their profession. In the UK, the General Medical Council is responsible for registering doctors, and for striking them off the list in cases of professional misconduct. The General Dental Council performs the same role for dentists, the Nursing and Midwifery Council for nurses, and the Royal College of Pharmacy for pharmacists. In the above ETP system the allocation of roles is given to these bodies, since it is a function that they are already performing well.

Created in June 2001, the Department for Work and Pensions (DWP) has taken over the responsibilities of the former Departments of Social Security, and Education and Employment. It is responsible for paying unemployment benefits and pensions, and along with the Prescription Pricing Authority (PPA), determining entitlement to free prescriptions. Many people are entitled to free prescriptions including: people aged 60 and over, children under age 16, young people aged 16, 17 or 18 in full-time education, people or their partner in receipt of Income Support or Jobseeker's Allowance, people named on a current National Health System (NHS) Low Income Scheme Full Help Certificate (HC2), expectant mothers, women who have given birth in the past 12 months, and war disablement pensioners. Consequently the management of this entitlement is distributed between different branches of the DWP and the PPA.

Each professional is allocated a role attribute certificate by their professional body, and this is stored in the LDAP directory belonging to that professional body. The ETP system will be able to make authorized decisions about prescribing and dispensing if it has access to those LDAP directories. Similarly, if the DWP allocates role attribute certificates to people who are entitled to free prescriptions for various reasons, and stores these in its LDAP directory (or directories), then the ETP system will be able to make decisions about entitlement to free prescriptions by accessing this LDAP directory, without the pharmacist needing to quiz the patient about their entitlement. The latter will only be needed in cases when a patient becomes newly entitled, for example when a pregnant woman is first diagnosed by her general practitioner, and the DWP has had insufficient time to create the official attribute certificate.

These roles are subsequently used by an authorization decision engine (such as PERMIS, see www.permis.org) to determine whether doctors are allowed to prescribe, pharmacists to dispense, and patients to receive free prescriptions, according to the ETP policy. Each ETP application (prescribing system, dispensing system, PPA system) reads in the ETP policy at initialization time, then when specific professionals request actions, such as prescribe or dispense, the authorization decision engine fetches the persons role from the appropriate LDAP directory, and makes its decision according to the policy. Thus users can gain access to multiple applications, and all they need to possess is a PKI key pair. The issuing of role attribute certificates can take place without the user's involvement, and they don't need to worry about how or where they are stored and used by the system.

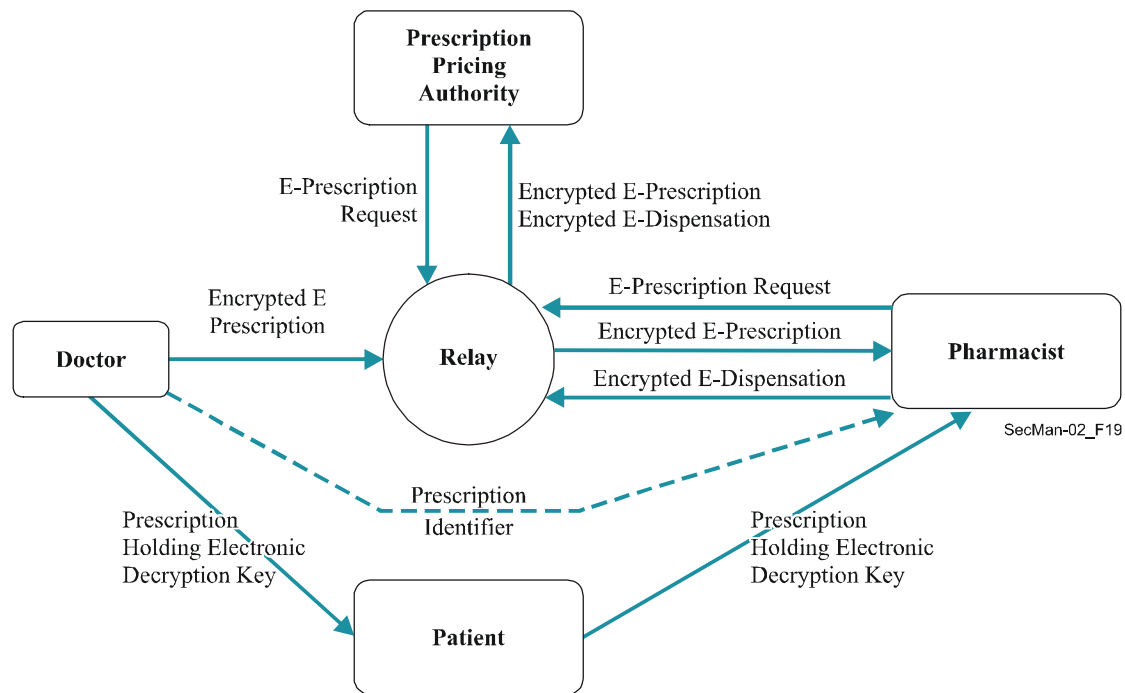


Figure 19 – The Salford Electronic Prescription System

Figure 19 contains an example of an implementation of an e-prescription system in the UK, which illustrates several of the key security issues for its implementation. At heart of the system is a security infrastructure that provides not only strong authentication (i.e., a PKI using public key certificates) but also strong authorization (i.e., a PMI in which the specific rights that medical professionals have are granted because of their roles stored in attribute certificates. Traditional models use access control lists buried in each particular application (e.g., medical records, prescription databases, insurance, etc.), requiring users (doctors, pharmacists, patients, etc.) to obtain and administer possibly several different security tokens (e.g., username/passwords, cards, etc.). In the new model where PKI and PMI are available, the user only needs a single token – the user's public key certificate – in order to benefit from the different services and resources that are geographically and/or topologically distributed. The user's attribute certificates are held within the system and not by the user, and are moved between components as desired to grant access. Because the attribute certificates are digitally signed by their issuers, they cannot be tampered with during these transfers.

In the example of Figure 19, electronic prescriptions are created by the doctor, digitally signed (for authentication purposes), symmetrically encrypted using a random session key (for confidentiality), then sent to a central storage location. The patient is given a paper prescription containing a bar code that holds the symmetric encryption key. The patient then goes to a pharmacy of his choosing, hands over the prescription, the pharmacist scans in the barcode then retrieves the prescription and decrypts it. The patient ultimately controls who is authorized to dispense his prescription, as in the current paper-based system. But this is not enough. It is also necessary to have controls on who is authorized to prescribe and dispense which drug sets, and who is entitled to free prescriptions.

Although the description above indicates a tightly integrated system, it might actually be distributed, such that the doctor attribute directory is different from the system that authenticates the pharmacists, or stores the dispensation rights and policies, etc., which rely on trusted third parties to authenticate and authorize the different players. Even though proprietary solutions to PKI and PMI might be applicable, the use of standardized solutions such as ITU-T Recommendation X.509 enable today more generalized and global access to e-prescriptions.

6.6 Secure Mobile End-to-End Data Communications

Mobile terminals with data communications capabilities (like IMT-2000 mobile phone, laptop PC or a PDA with a radio-card) have been widely distributed and the provision of various application services (e.g., mobile e-commerce) for mobile terminals connected to the mobile network are emerging. In the e-commerce environment, security is necessary and even more, essential.

There are many security areas under investigation from a mobile operator's point of view (e.g., security architecture for the IMT-2000 mobile telephone network). However, it is also important to investigate from the mobile user's point of view and application service provider's (ASP) point of view.

When investigating the security in mobile communications from the mobile user's and the ASP's point of views, the security aspects of mobile end-to-end data communications between a mobile terminal and an application server is one of the most important aspects.

In addition, for the mobile system that connects a mobile network to an open network, security investigation in the upper layers (applications, presentation and session layers) of the OSI Reference Model is needed because there are various possible implementations of mobile networks (e.g., IMT-2000 mobile telephone network, wireless LAN, Bluetooth) or open networks.

6.6.1 Framework of security technologies for mobile end-to-end data communications

Recommendation X.1121 describes models of secure mobile end-to-end data communications between mobile terminals and application servers in the upper layers. Two types of security models are defined for a security framework for mobile end-to-end data communications between a mobile user and an ASP: a General model and a Gateway model. A mobile user uses the mobile terminal to get access to various mobile services from ASPs. An ASP provides a mobile service to mobile users through an application server. The mobile security gateway relays packets from mobile terminals to the application server, transforms a mobile network-based communication protocol to an open network-based protocol, and vice versa.

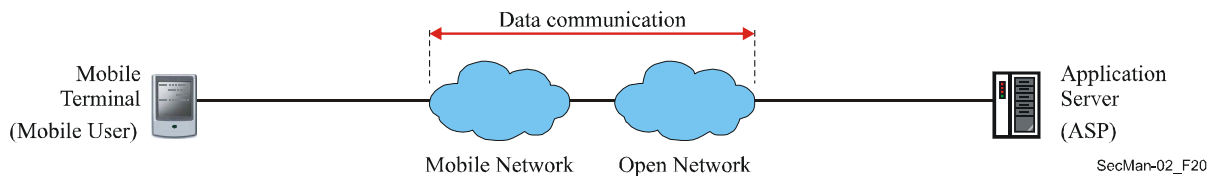


Figure 20 – General model of end-to-end data communication between a user and an ASP

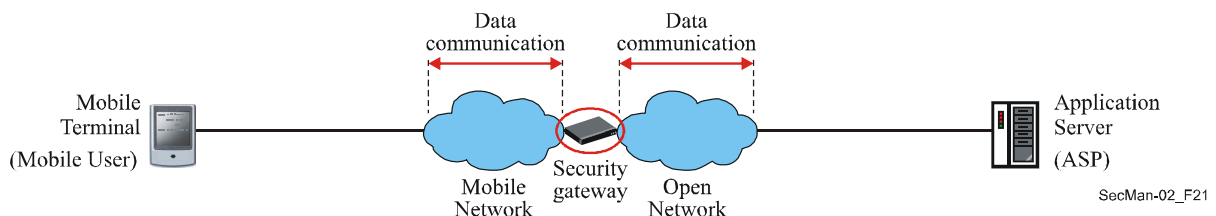


Figure 21 – Gateway model of mobile end-to-end data communication between a mobile user and an ASP

Recommendation X.1121 also describes security threats for mobile end-to-end data communications and the security requirements from the mobile user's and the ASP's point of views in both models. There are two types of threats: one general type present in any open network, and another specific

mobile-oriented type of security threats. Figure 22 depicts the threats in a mobile end-to-end data communication network.

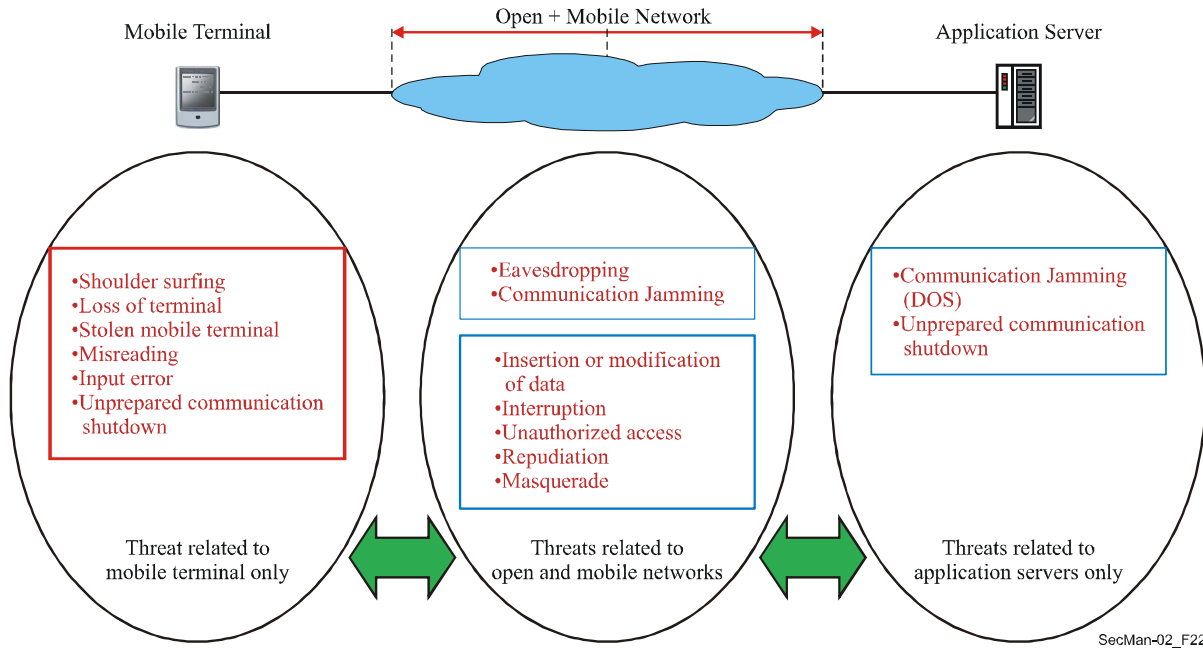


Figure 22 – Threats in the mobile end-to-end communications

In addition, Recommendation X.1121 identifies the locations where the security technologies are implemented, when required for each entity and the relationship between entities in a mobile end-to-end data communication.

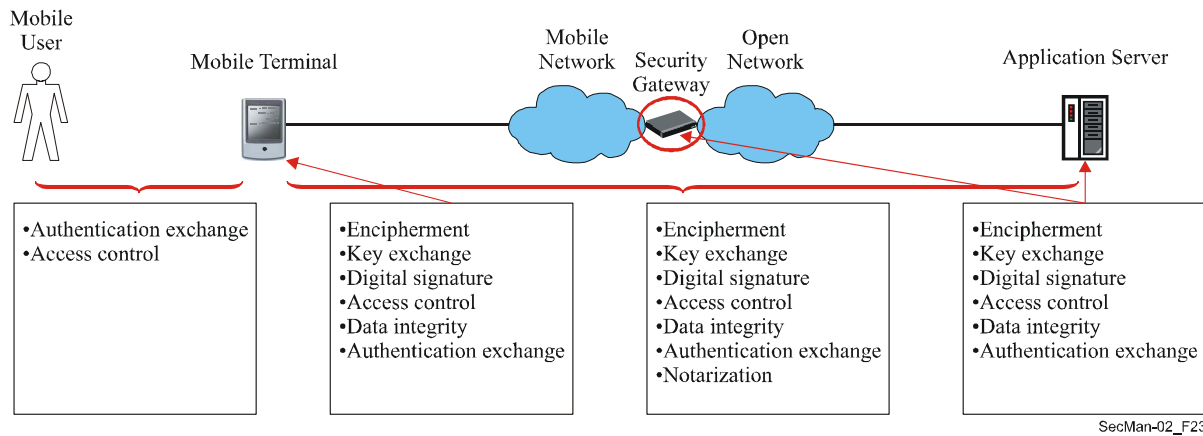


Figure 23 – Security function required for each entity and relation between entities

6.6.2 PKI considerations for Secure Mobile End-to-End Data Communications

This section relates to Recommendation X.1122. Although PKI technology is a very useful technology for protecting mobile end-to-end data communications, some characteristics specific to mobile data communications may require the PKI technology to be adapted when constructing secure mobile systems. Two types of PKI models were defined to provide security services in mobile end-to-end communications. One relates to a general PKI model, in which there is no security gateway function present in a mobile end-to-end data communication, the other relates to a gateway PKI model, in which there is a security gateway to interface with the mobile network and the open network.

Figure 24 depicts the general PKI model for mobile end-to-end communications. This involves four entities. The mobile user's CA issues mobile user's certificate to the mobile user and manages the repository for storing the certificate revocation list (CRL) that has been already issued by the user CA. The mobile user's validation authority (VA) provides an online certificate validation service to the mobile user. The ASP's CA issues ASP's certificate to the application service provider and manages the repository for storing the certificate revocation list that has been already issued by the ASP's CA. The ASP's validation authority provides an online certificate validation service for ASP certificates.

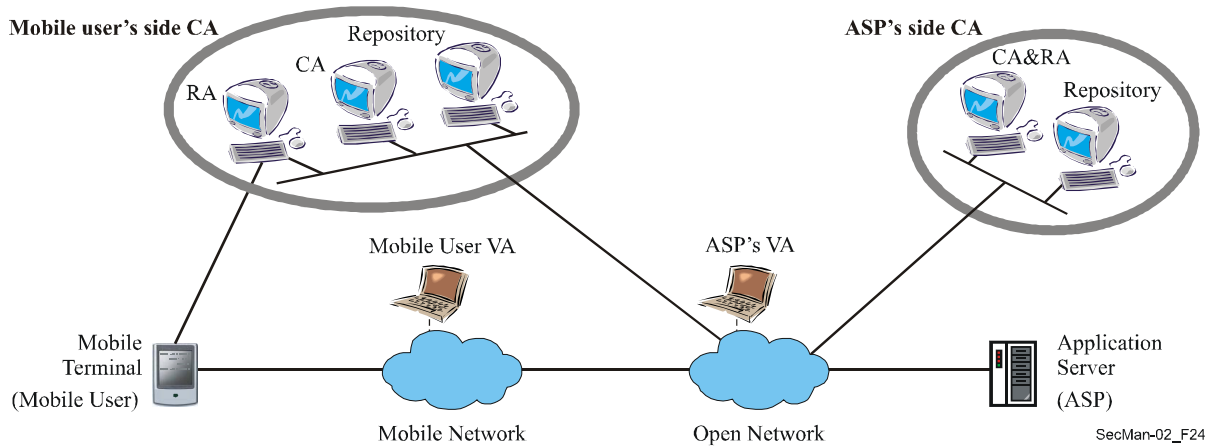


Figure 24 – General PKI model for mobile end-to-end data communications

There are two certificate issuance methods depending on the generation location of public/private key. One is a method in which the cryptographic key pair is generated and fabricated at the factory of the mobile terminal, the other is a method in which the cryptographic key pair is generated in the mobile terminal or the tamper-free token like smart card attached to the mobile terminal. Figure 25 depicts the procedure for mobile terminal to acquire the certificate utilizing the certificate management procedure, where the cryptographic key pair is generated in the mobile terminal.

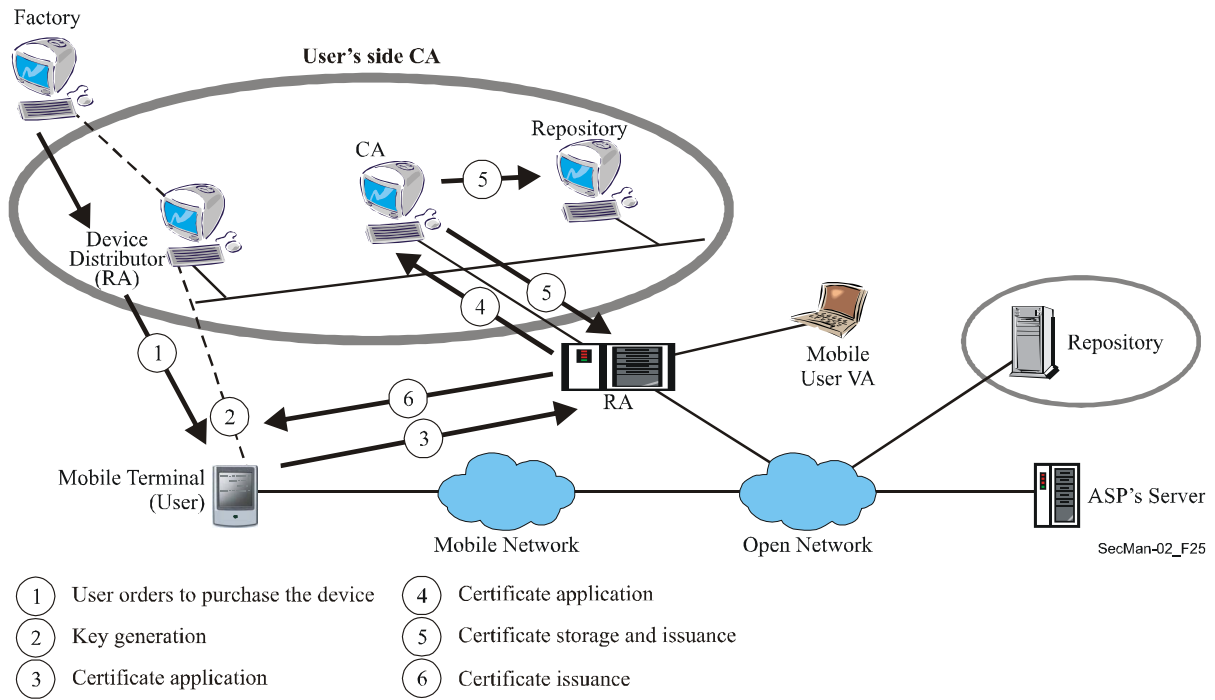


Figure 25 – Certificate issuance procedure for mobile terminal

The mobile terminal has a limited computational power and memory size. As a result, online certificate validation scheme is preferable to the off-line certificate validation scheme based on the CRL. When the mobile terminal receives the message-signature pair with the certificate chain and wants to check the validity of the signature, the certificate should be used after the validity of certificate should be checked using the certificate validation scheme. Figure 26 depicts the on-line certificate validation procedure for the mobile terminal.

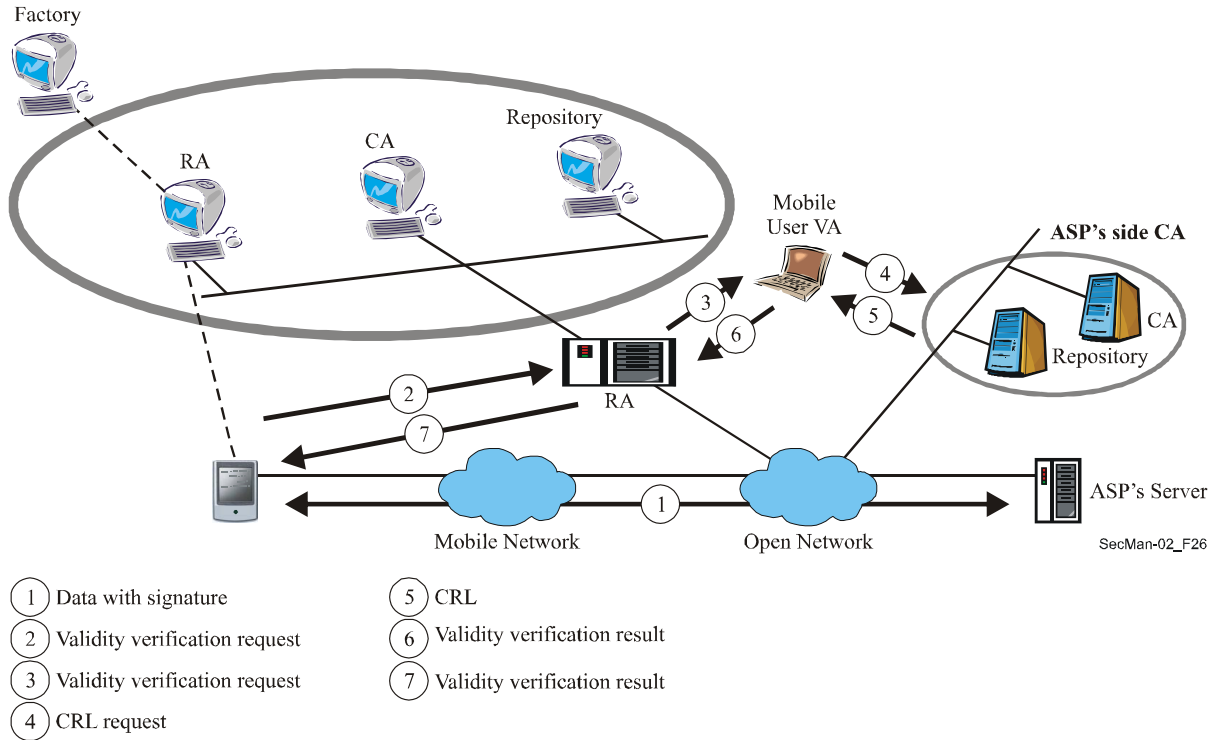


Figure 26 – Certificate validation procedure for mobile end-to-end data communications

The PKI system for a mobile end-to-end communication can be used for two usage models: One can be used for session layer, and the other can be used for application layer. Session layer usage model provides security services such as client authentication, server authentication and confidentiality and integrity service. Application layer usage model provides a non-repudiation service and a confidentiality service for a mobile end-to-end data communication.

As a conclusion, Recommendation X.1122 describes considerations for constructing secure mobile systems based on PKI from the following point of view: interoperability with existing PKI based system in open network, PKI use in the mobile environment (include key generation issues, certificate application and issuance issues, certificate use issues and CA issues) and PKI general (include lifecycle management of certificate issues). It can be used as a guideline document when constructing secure mobile systems based on PKI technology.

7 Availability Dimension and Infrastructure Layer

Recommendation X.805, introduced in section 2 refers to:

- security dimensions as a set of security measures designed to address a particular aspect of the network security; and
- security layers. The security dimensions are applied to a hierarchy of network equipment and facility groupings, which are referred to as security layers.

The availability security dimension 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. Disaster recovery solutions are included in this category.

The infrastructure security layer consists of the network transmission facilities as well as individual network elements protected by the security dimensions. The infrastructure layer represents the fundamental building blocks of networks, their services and applications. Examples of components

that belong to the infrastructure layer are individual routers, switches and servers as well as the communication links between individual routers, switches and servers.

The functional, implementation or operational requirements specified by the ITU-T as part of the concepts above are numerous and diverse. They may relate to error performance, congestion control, failure reporting and corrective actions, and many others. The remaining part of this section provides some different views on requirements related to telecommunication networks aiming at limiting the risks and consequences of unavailability on transmission resources.

In order for a telecommunication network operator to select an appropriate network topology with regards to availability objectives, a reference to Annex A to Recommendation G.827, *Examples of path topologies and end-to-end path availability calculations* is proposed.

7.1 Path topologies and end-to-end path availability calculations

Figures 27 and 28 illustrate the basic path topologies that can be built using predefined path elements.

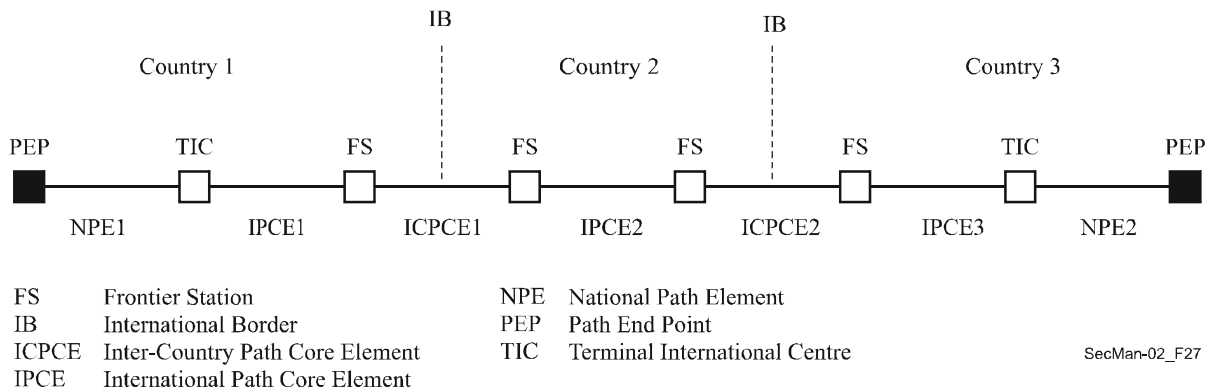


Figure 27 – Example of a simple basic path without protection

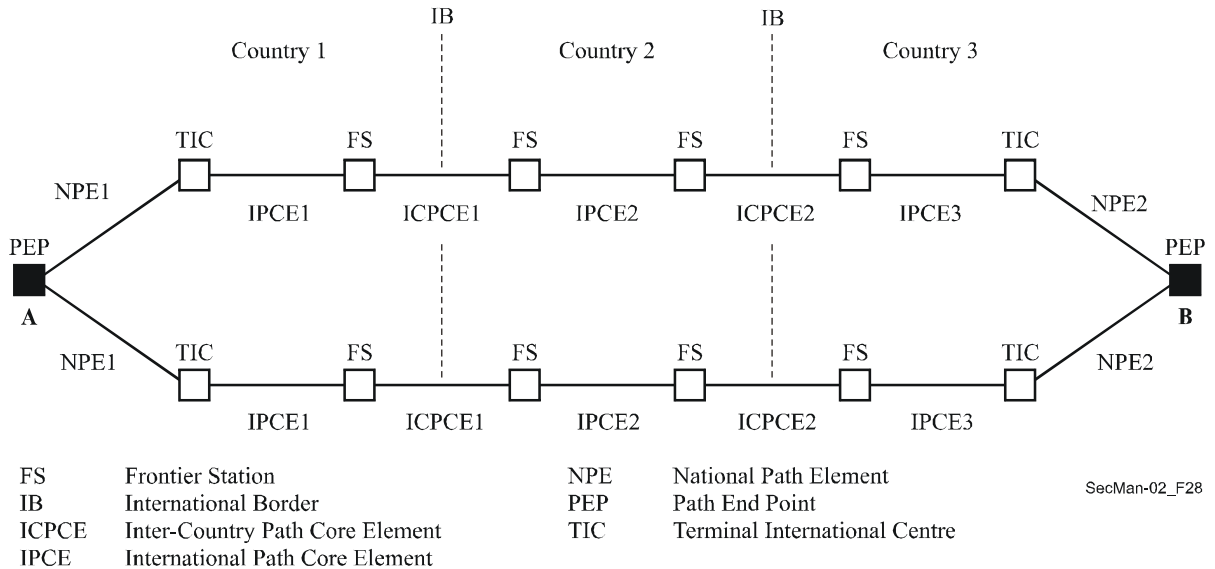


Figure 28 – Example of a path with end-to-end protection

Figure 27 shows a simple basic path without protection and Figure 28 shows the addition of an end-to-end protection path which should have a separate routing for maximum protection.

This form of protection is called 1+1. Each path is a two-way connection with the transmit signal from each end permanently connected to both paths and a switching device at each receiver to select the best signal.

A more economical arrangement is to use one protection path to protect several other paths. This is known as a 1:n arrangement and requires selection switches at both transmitters and receivers.

For the purposes of end-to-end availability calculations, it is more convenient to use the unavailability ratio. Recommendation G.827 in its Annex A provides some basic principles to evaluate the availability for simple basic path (Figure 27), 1+1 end-to-end protection (Figure 28) or 1:n protection ratio topologies.

Section 7.3 provides more complex topologies, e.g., Synchronous Digital Hierarchy (SDH) ring topology showing that traffic can be rerouted around a failed link but the protection route depends upon the switching capabilities of the various nodes on the ring and may not be the shortest distance between two nodes. For more complex topologies, the problem of evaluating the availability is rather difficult. Several papers given in Appendix I to Recommendation G.827 address the issue.

7.2 Enhance the availability of a transport network – Overview

Sections 7.2 to 7.4 describe the architectural features for the more common approaches used to enhance the availability of a transport network. The enhancement is achieved by the replacement of failed or degraded transport entities with other dedicated or shared resource entities. The replacement is normally initiated by the detection of a defect, performance degradation or an external (e.g., network management) request.

Protection – This makes use of pre-assigned capacity between nodes. The simplest architecture has one dedicated protection entity for each working entity (1+1). The most complex architecture has m protection entities shared amongst n working entities (m:n). Protection switching may be either unidirectional or bidirectional. Bidirectional protection switching takes switching actions for both traffic directions, even when the failure is unidirectional. Unidirectional protection switching takes switching actions only for the affected traffic direction in the case of a unidirectional failure.

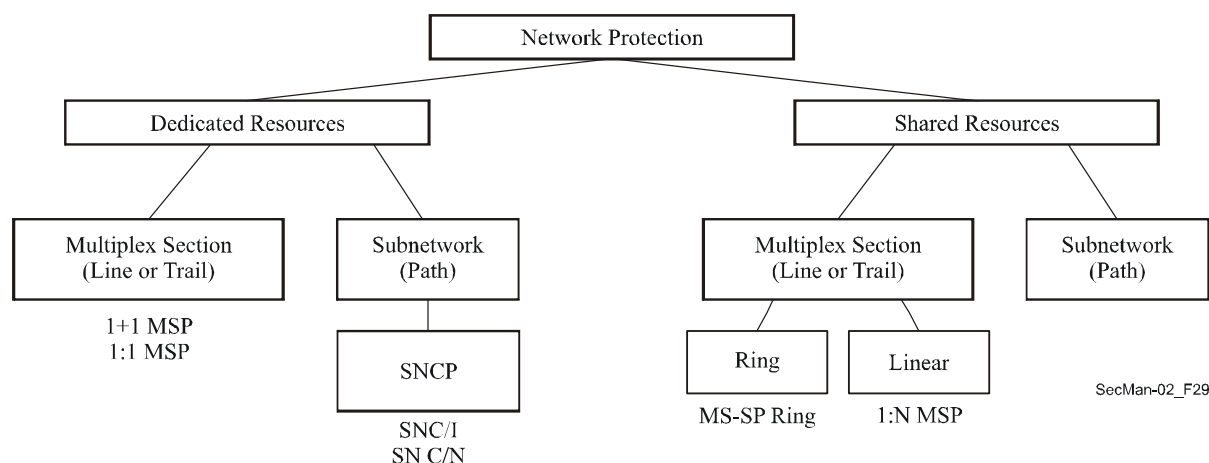
Restoration – This makes use of any capacity available between nodes. In general the algorithms used for restoration will involve re-routing. When restoration is used some percentage of the transport network capacity will be reserved for re-routing of working traffic.

Recommendation G.805 provides key information on these aspects.

7.3 Protection

High service availability can only be achieved by using a network infrastructure with high reliability and high survivability. Thus if there is a fault with the high reliability equipment, there needs to be the ability to switch to an alternate source of the signal (protection channel).

There are two types of protection. There is *Equipment Protection*, where there are redundant circuit packs. Thus if there is a hard failure on the circuit pack, then another one is automatically switched in. There is also *Network Protection*. Network protection protects against fiber cuts by having alternate paths for the signal to go. These alternate paths may be either Dedicated or Shared. These mechanisms are shown in Figure 29.



SNC/I Subnetwork Connection Protection/ Inherent monitoring
 SNC/N Subnetwork Connection Protection/ Non-intrusive monitoring
 SNCP Subnetwork Connection Protection
 1+1 MSP Multiplex Section 1+1 Protection Switching
 1:N MSP Multiplex Section 1:N Protection Switching
 MS-SPRing Multiplex Section Shared Protection Ring

Figure 29 – Protection Switching Variations

Protection mechanisms can be uni-directional or bi-directional. They can also be either revertive or non-revertive. These terms are defined in Recommendation G.780.

Unidirectional protection is defined as "For a unidirectional fault (i.e., a fault affecting only one direction of transmission), only the affected direction (of the trail, subnetwork connection (SNC), etc.) is switched." This means that only a local decision on the receiver side (local node) is done without considering the status of the remote node when making a protection switch. This is in case of a unidirectional failure (i.e., a failure affecting only one direction of transmission), only the affected direction is switched to protection.

Bidirectional protection is defined as "For a unidirectional fault, both directions (of the trail, subnetwork connection, etc.), including the affected and unaffected direction, are switched." This means that the local and the remote status is considered when making a protection switch. This is in case of a unidirectional failure (i.e., a failure affecting only one direction of transmission), both directions including the affected direction and the unaffected direction, are switched to protection.

Revertive (protection) operation is defined as "In revertive operation, the traffic signal (service) always returns to (or remains on) the working SNC/trail if the switch requests are terminated; i.e., when the working SNC/trail has recovered from the defect or the external request is cleared." This means that in the revertive mode of operation, the signal on the protection channel is switched back to the working channel when the working channel has recovered from the fault.

Non-revertive (protection) operation is defined as "In non-revertive operation, the traffic signal (service) does not return to the working SNC/trail if the switch requests are terminated." This means that in non-revertive mode of operation (applicable only to 1+1 architectures), when the failed working channel is fault-free again, the selection of the normal or protected traffic signal from the protection channel is maintained.

The most common forms of protection are:

- 1:1 MSP (Multiplex Section 1:1 Protection Switching, see 7.3.1)
- 1+1 MSP (Multiplex Section 1+1 Protection Switching, see 7.3.2)
- MS-SPRing (Multiplex Section Shared Protection Ring, see 7.3.3)
- SNCP (Sub Network Connection Protection, see 7.3.4)

These protection mechanisms will be discussed in further detail. However, a common set of reference Recommendations applies, G.841 (characteristics), G.842 (interworking), G.783 (functional models), G.806 (defects) and G.808.1 (Generic Protection Switching).

7.3.1 Multiplex Section 1:1 Protection Switching

The network diagram is shown in Figure 30.

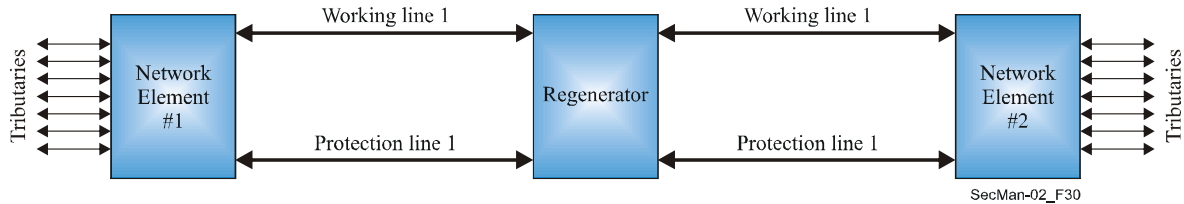


Figure 30 – Network Diagram for 1:1 Protection Switching

In 1:1 protection switching, there is one protection channel for every working channel. The protection channel may be carrying other traffic that can be preempted.

A diagram of the inside of Network Element is shown in Figure 31.

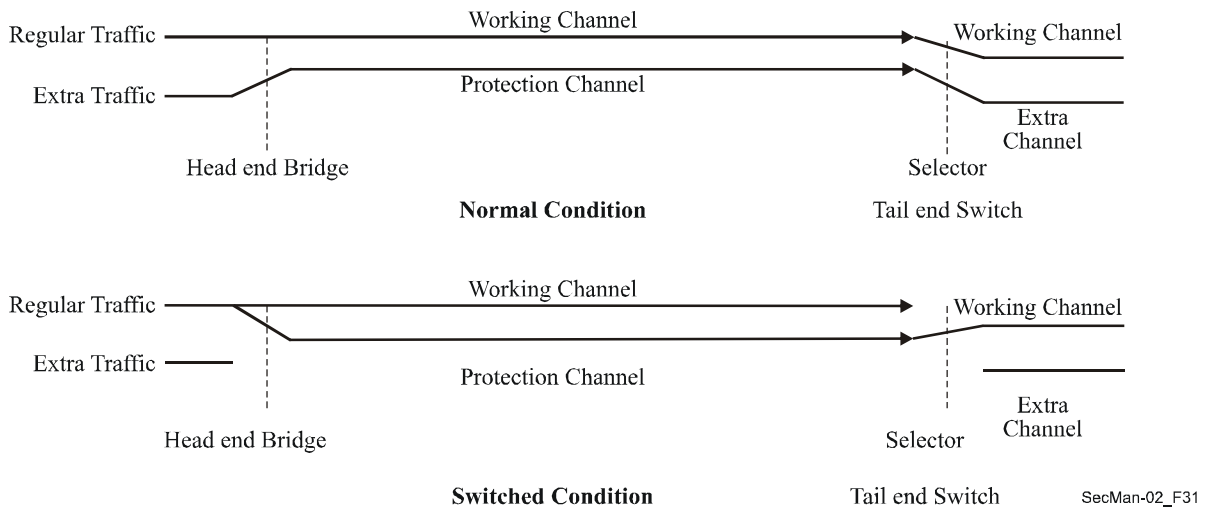


Figure 31 – Multiplex Section 1:1 Linear Protection

In normal conditions, "Extra Traffic" can be carried on the protection Channel. However if the correct K1/K2 bytes are received (activating the protection function), then the "Regular Traffic" is bridged onto the protection channel at the "Head End" and switched at the "Tail end". The control is done via K1 and K2 bytes on the protection channel.

This corresponds to Line protection at the Synchronous Transport Module, level N (STM-N level (N>=1)).

The conditions that can initiate a switch are Forced Switch and a number of defect or failure conditions (e.g., Signal Fail, Loss of Signal, Loss of Frame, Excessive Errors, Signal Degrade). Details are given in Recommendation G.806.

7.3.2 Multiplex Section 1+1 Protection Switching

The network diagram is shown in Figure 32.

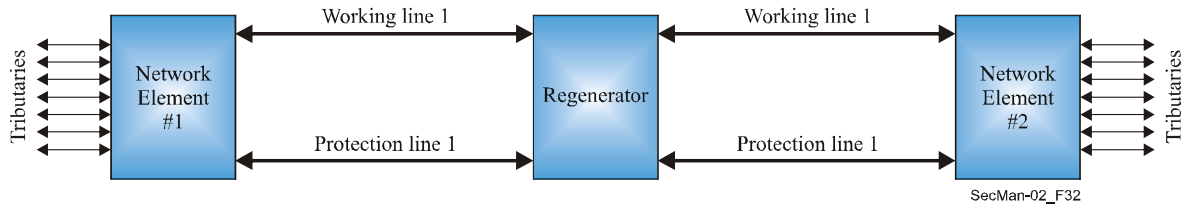


Figure 32 – Network Diagram for 1+1 Protection Switching

In 1+1 protection switching, there is one protection channel for every working channel. The protection channel is carrying a copy of the working channels signal.

A diagram of the inside of Network Element is shown in Figure 33.

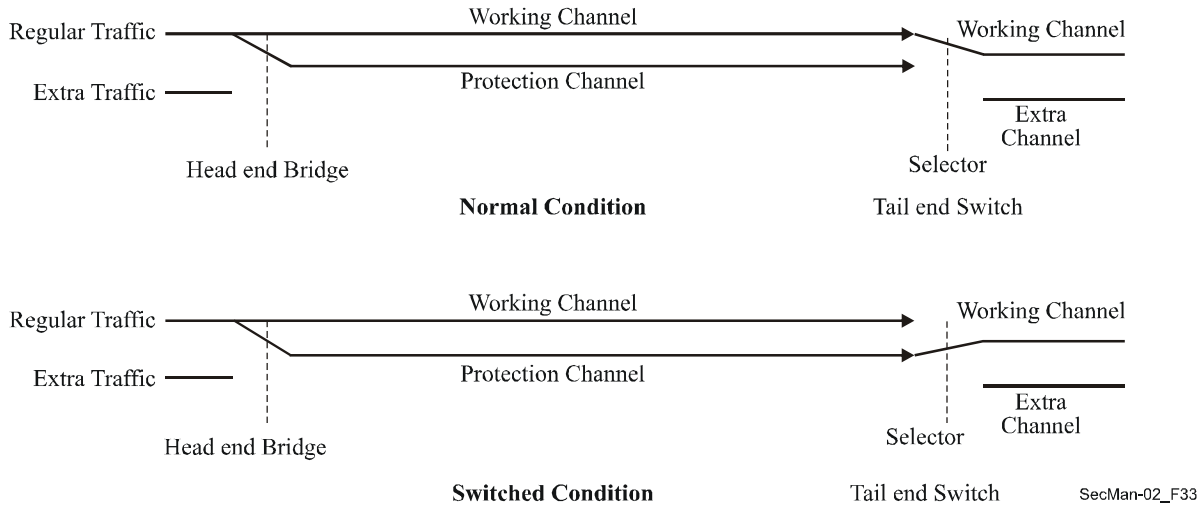


Figure 33 – Multiplex Section 1+1 Linear Protection

The transmit signal is permanently bridged to the protection line. The receiver selects the better signal.

There is no capability for "Extra Traffic" in a 1+1 protection scheme. This performs a Line protection function. Thus it only works on STM-n, whatever rate the line is. It can be seen as a subset of 1:1 protection switching. It does not require a control mechanism (Automatic Protection Switching (APS) bytes K1 and K2 of the Multiplex Section OverHead (MSOH)) to operate. It switches based on the same fault condition as those given in 7.3.1.

There is a version of this protection mechanism called 1+1 bidirectional, where the selectors at both ends switch. This requires control by the means of the K1/K2 bytes to be transmitted.

7.3.3 MS-SPRing Protection Switching

The network diagram is shown in Figure 34.

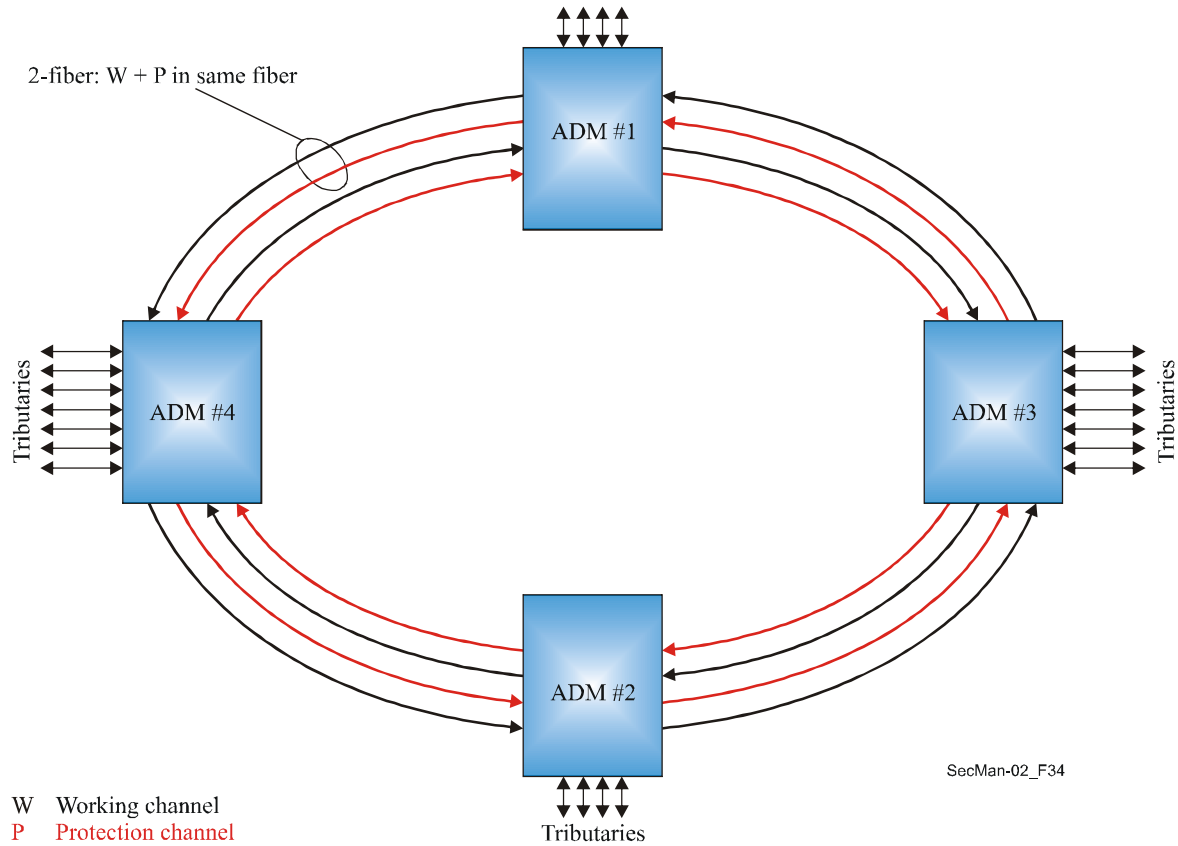


Figure 34 – Network diagram for MS-SPRing Protection Switching

2 Fiber MS-SPRing configuration is dominant in SDH networks. There are 2 fibers for each span of the ring with each carrying half the bandwidth for working and protection channels (e.g., STM-64 line with Administrative Units (AU) AU-4 from 1 to 32 working and AU-4 from 33 to 64 for protection). Normal traffic carried on working channels in one fiber is protected by the protection channels in the opposite direction.

2-fiber MS-SPRing function is shown in Figure 35.

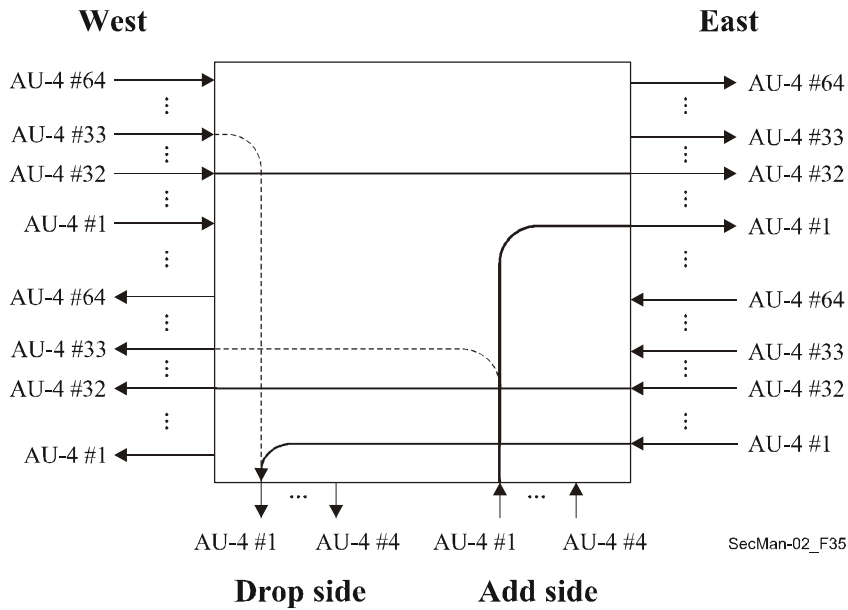


Figure 35 – STM-64 Ring with STM-4 Add-Drop

In Figure 35, the constituent signal "Add AU-4 #1" is transferred to the "East AU-4 #1 Transmit" signal. It is dropped from "East AU-4 #1 Receive" to "Drop AU-4#1". There is also a through connection on AU-4 #32 shown in Figure 35.

If there was a break in the East Fiber, then "Add AU-4 #1" needs to be transmitted out the West Side Protection ("West AU-4 #33 Transmit") and the receive signal dropped from the West Side Protection ("West AU-4 #33 Receive") to "Drop AU-4#1". AU-4 #32 from the West needs to be looped back to AU-4 #64. AU-4 #32 from the East would have been looped back onto the protection channel (AU-4 #64) on the other side of the break, so at this node, the protection ("West AU-4#64 Receive") needs to be looped onto the working channel (AU-4 #32).

Protection switching is done on AU-4 or AU-3 granularity across all the signals in the fiber. Requests and acknowledgements are transmitted by using the Automatic Protection Switching (APS) bytes K1 and K2 of the Multiplex Section OverHead (MSOH). K1 and K2 are transmitted on the line that carries the protection channels. They are transmitted in both directions (East and West), one is the short and the other is the long path.

Squelching is done to avoid delivery of traffic to the wrong client in case of Node isolation or Node failure with add/drop traffic (services from the same time slot but on different spans). For a description of squelching, please refer to Appendix II in Recommendation G.841.

The faults for Signal Fail and Signal Degrade are the same as with Linear Protection Switching (see 7.3.1).

There are three switch configurations to consider:

- Normal (no faults)
- Fault on East side (Need to loopback West and only add/drop from West)
- Fault on West side (Need to loopback East and only add/drop from East)
- Span Switching for 4 Fiber MS-SPRing (Switch to protection, no loopback)

7.3.4 SNCP Protection Switching

The network diagram is shown in Figure 36.

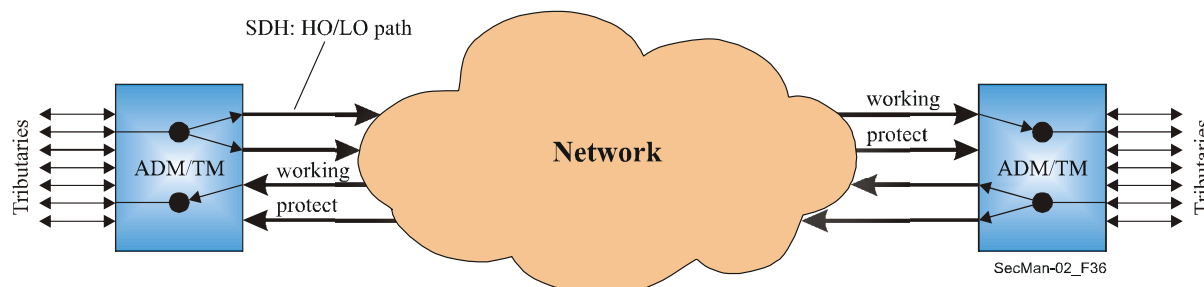


Figure 36 – SNCP Protection Switching

SNCP is path based. Thus only one signal (AU-3, AU-4, etc.) is switched at a time. It can also be thought of as unidirectional 1+1 for individual paths. The protection switching is done on path level:

- SDH: High Order Virtual Container HO – VC-4/3, Lower Order Tributary Unit LO – TU-3/2/11/12

No protocol is used (except for Forced Switch). The switching decision between a working and a protect copy is based on local conditions, where both copies are monitored.

- The protection switching time requirement is less than 50 ms. Thus in case of a fiber cut on a fiber with high bandwidth, e.g., 10 Gbit/s or 40 Gbit/s, and all paths are SNCP protected, usually this target time cannot be met if protection switching is done in software which includes defect processing in a state machine and messaging between board and central controller.

7.4 Restoration

Recommendation G.805 describes transport network availability enhancement techniques. The terms "Protection" (replacement of a failed resource with a pre-assigned standby) and "Restoration" (replacement of a failed resource by re-routing using spare capacity) are used to classify these techniques. In general, protection actions complete in the tens of millisecond range, while restoration actions normally complete in times ranging from hundreds of milliseconds to up to a few seconds.

The ASON (Automatic Switched Optical Network) control plane provides a network operator with the ability to offer a user calls with a selectable class of service (CoS), (e.g., availability, duration of interruptions, Errored Seconds, etc.). Protection and restoration are mechanisms (used by the network) to support the CoS requested by the user. The selection of the survivability mechanism (protection, restoration or none) for a particular connection that supports a call will be based on: the policy of the network operator, the topology of the network and the capability of the equipment deployed. Different survivability mechanisms may be used on the connections that are concatenated to provide a call. If a call transits the network of more than one operator then each network should be responsible for the survivability of the transit connections. Connection requests at the UNI or E-NNI will contain only the requested CoS, not an explicit protection or restoration type.

The protection or restoration of a connection may be invoked or temporarily disabled by a command from the management plane. These commands may be used to allow scheduled maintenance activities to be performed. They may also be used to override the automatic operations under some exceptional failure conditions.

Refer to Recommendation G.8080.

7.5 Outside plant

There are many aspects under the question of security in telecommunication systems. The aspects related to the physical security of the outside plant are also considered by ITU-T. The problems of making the hardware of the system resilient to the threat of fire, natural disaster and intentional or accidental intrusion by people are addressed. The two most important security questions covered involve making the components of systems, cable, closures, cabinets, etc., physically able to resist to damage and also the monitoring of systems to prevent any damage when possible or to respond to problems and restore system functionality in the most expeditious manner.

In general, the most important factors to be considered for these aspects of security are:

- cause of damage/loss of data:
 - network maintenance;
 - accidents and calamities (not intended);
 - vandalism (intended ; random);
 - access by non-qualified personnel (e.g., civilians, technicians of other operators);
 - criminality (e.g., damage of terminal or cross connect for burglary; theft of cables; illegal tapping of a cable); and
 - intended; concentrated force or violence.
- plant environment situations:
 - indoor locations (Central Office, Customer Premises);
 - outdoor aerial (exposition to human/natural actions);
 - outdoor at street level (possibility of damages due to works); and
 - outdoor underground (ducted or direct buried).

In general, the following could be recommended concerning the physical layer as precautions to be taken. Most of these are managed by local practices and rules of the individual operators:

- avoid to use nodes at street level (cabinets, pedestals, wall boxes): sensitive to accidents, vandalism, violent actions, fire and general curiosity, it is safer to use underground nodes and cables;
- street cabinets (or other boxes at street level) should be of a "tamper proof" construction;
- all enclosures should have the option to be locked or sealed, to avoid unwanted access;
- ducted plant cables are less vulnerable than direct buried: e.g., accidental damage due to digging operations;
- Termination or demarcation points may have a (lockable) separation between network and customer side; or between circuits, used by different operator;
- indoor customer terminals are less vulnerable than outdoor (wall-mounted) customer terminations (e.g., in case of burglary);
- it may be recommendable to store cable slack at regular locations of the network, for easy repair of accidental damage (both aerial as underground);
- for fiber optics plant, a proper level of circuit separation plus dynamic optical stability is recommended, to avoid loss of data / disturbance of traffic during network maintenance; and
- for vital lines, redundancy (back up lines) by physically separated cables and networks may be recommended (e.g., rings structures for banks, hospitals).

Other actions that could be implemented are:

- establish safety procedures for outdoor installations;
- install fire detection systems, monitoring and control of outside plant;

- establish criteria to assess the safe coexistence in the same part of the network of more than one operator providing multi-services such as POTS, ISDN, xDSL, etc, without any kind of detrimental interaction;
- use technical solutions that provide for the easy implementation of unbundling whilst maintaining the integrity, reliability and interoperability within network topologies, which are commonly used worldwide;
- install signalling devices along underground cables;
- provide monitoring, maintenance support, and testing systems for the outside plant;
- address cable design which has the primary function of protecting the physical integrity of the transmission medium – the optical fibers; and
- address aspects of cable construction, fibres splicing, organizer and closures, branching units, survey and route planning, characteristics of cable ships, loading and laying activities, repair methods, protections and test methods for maritized terrestrial optical fibre cables.

8 Incident Organization and Security Incident Handling (Guidelines) for Telecommunications Organizations

Security management and awareness include a number of processes. Among them are the definition of structures and procedures for handling and disseminating information on security-related incidents. This is also an area where ITU-T experts reacted to an expressed need and developed Recommendation E.409. The purpose of *Recommendation E.409, Incident organization and security incident handling: Guidelines for telecommunications organizations* is to analyze, structure and suggest a method for establishing an incident management organization within a telecommunications organization involved in the provision of international telecommunications, where the flow and structure of an incident are focused. The flow and the handling are useful in determining whether an event is to be classified as an event, an incident, a security incident or a crisis. The flow also covers the critical first decisions that have to be made.

This Recommendation provides an overview and framework that gives guidance for planning incident organization and security incident handling.

It is generic in nature and does not identify or address requirements for specific networks.

While this Recommendation is intended to facilitate international developments regarding telecommunication network security, such developments could be facilitated if the requirements could be applied also to the national Information and Communication Networks (ICN).

Computer crime follows in the wake of the heavily increased use of computers in international telecommunications. Over the last years computer crime has literally exploded, as confirmed by several international and national surveys. In the majority of countries there are no exact figures on the number of computer break-ins or security incidents, especially those related to international telecommunications.

Most telecommunications organizations or companies don't have any specialized organization for handling Information and Communications Networks (ICN) security incidents (although they may have a general crisis team for handling crises of any type). When an ICN security incident occurs it is handled ad hoc, i.e., the persons who detect an ICN security incident take the responsibility to handle it the best they can. In some organizations they may attempt to forget or cover up ICN security incidents as they may affect production, availability and revenues.

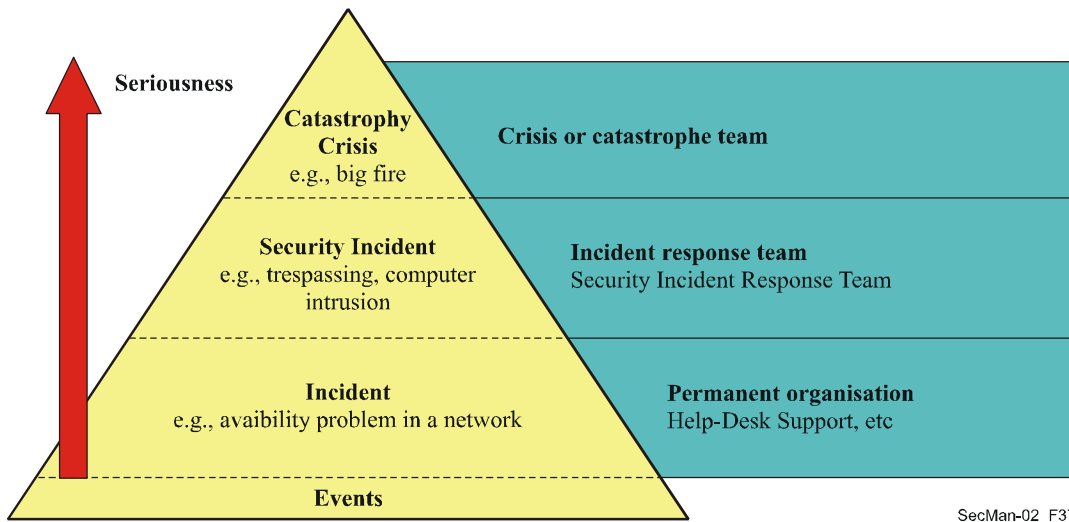
Often when an ICN security incident is detected, the person who detects it doesn't know to whom to report it. This may result in the system or networks administrator deploying a workaround or quick fix just to get rid of the problem. They do not have the delegated authority, time or expertise to correct the system so that the ICN security incident does not recur. These are the main reasons why it is better to have a trained unit or group that can handle security incidents in a prompt and correct manner. Furthermore, many of the issues may be in areas as diverse as media relations, legal, law enforcement, market share, or finance.

When reporting or handling an incident, the use of different taxonomies leads to misunderstanding. This may, in turn, result in an ICN security incident neither getting the proper attention nor the prompt handling that is needed in order to stop, contain and hinder the incident from recurring. This may lead to serious consequences for the affected organization (victim).

To be able to succeed in incident handling and incident reporting one must have an understanding of how incidents are detected, handled and resolved. By establishing a general structure for incidents (i.e., physical, administrative or organizational, and logical incidents) it is possible to obtain a general picture of the structure and flow of an incident. A uniform terminology is the base for a common understanding of words and terms.

8.1 Definitions

The term security incident can be defined as a "security breach, threat, weakness and malfunction that might have an impact on the security of organizational assets". In this Recommendation, it is assumed that an incident is less severe than a security incident and that an information security incident is a particular type of security incident.



SecMan-02_F37

Figure 37 – The pyramid of events in ITU-T Recommendation E.409

The figure above shows the pyramid of events. At the bottom we find the event, followed by incident, security incident and at the top crisis and catastrophe. The closer to the top an event is, the more serious it is. In order to make use of a common and sound vocabulary regarding incident handling within the ICN area, it is recommended that the following definitions are used.

8.1.1 – Event – an event is an observable occurrence, which it is not possible to (completely) predict or control.

8.1.2 – Incident – an event that might have led to an occurrence or an episode which is not serious.

8.1.3 – Security Incident – A security incident is any adverse event whereby some aspect of security could be threatened.

8.1.4 – Information and Communications Networks (ICN) Security Incident – Any real or suspected adverse event in relation to the security of ICN. This includes:

- intrusion into ICN computer systems via the network;
- occurrence of computer viruses;
- probes for vulnerabilities via the network into a range of computer systems;
- PABX call leak-through; and
- any other undesired events arising from unauthorized internal or external actions, including denial of service attacks, disasters and other emergency situations, etc.

8.1.5 – Crisis – A crisis is a state caused by an event - or the knowledge of a forthcoming event - that may cause severe negative consequences. During a crisis one may, in best cases, have the possibility to take measures to prevent the crisis from becoming a catastrophe. When a *catastrophe* occurs one normally has a Business Continuity Plan (BCP) and a crisis management team to handle the situation.

8.2 Rationale

It is recommended that telecommunications organizations creating (computer security) incident response teams (CSIRT), as the first step, declare their use of taxonomy in order to avoid misunderstandings. Collaboration is much easier when using the same "language".

It is recommended that organizations use the term Incident and ICN Security Incident; and define their own subdivisions due to severity of the latter. In essence, an ICN security incident is any undesired, unauthorized event. This means that an ICN security incident includes computer intrusion, denial of service attack or a virus depending on the motivation, experiences and available knowledgeable resources in the organization. In organizations that have created an effective virus fighting team, viruses may not be considered as ICN security incidents but rather as incidents.

An example or template of such a subdivision could be as follows:

- Incidents
 - Violating Internet Netiquette (Spamming, Abusive Content, etc.)
 - Violating security policies
 - Individual viruses
- ICN security incidents
 - Scans and probes
 - Computer intrusions
 - Computer sabotage and damage (availability attacks as bombing, DoS-attacks)
 - Malicious software (viruses, trojans, worms, etc.)
 - Information theft and espionage
 - Impersonation

By using the same granularity and preciseness in terminology it is possible to gain experiences in:

- guidance of the severity and scope;
- indication of the need for promptness (e.g., for restoring the required level of security);
- efforts of likely countermeasures; and
- possible costs involved.

9 Conclusions

ITU-T has for a long time developed a set of foundational Recommendations on security: X.800 is a reference document on security architecture for Open System Interconnection, and the X.810-X.816 Series defines a security framework for open systems covering overview, authentication, access control, non-repudiation, confidentiality, integrity and security and audit alarms, respectively. More recently, ITU-T Recommendation X.805 has been developed to describe the security architecture for systems providing end-to-end communications. The architectural revision that X.805 represents takes into account the increased threats and vulnerabilities that result from the emerging multi-network and multi-service provider environment. Recommendation X.509 on public-key and attribute certificate frameworks is certainly the most referred text from the ITU-T in security applications, either directly or implicitly within other standards built on X.509 principles.

In addition to these framework Recommendations, ITU-T has developed security provisions in several systems and services defined by its Recommendations. In this manual, some are described in Section 6: voice-over-IP using H.323 or IP-Cablecom, secure fax transmission, and network management. An example of application of public key and privilege management infrastructure applications in e-health is also given. *Caveat emptor*, there are many *more* areas where the security needs of telecommunications and information technologies are addressed in ITU-T Recommendations. Those and aspects such as fraud prevention and disaster recovery being developed in several ITU-T Study Groups will be further addressed in future editions. ITU-T's work on security is reinforced by the organization of, or participation in international seminars or workshops on security, the development of a security project, by designating a lead study group for security work in ITU-T and collaboration with other Standard Development Organization (e.g. ISO/IEC JTC 1/SC 27).

References

In addition to the ITU-T Recommendations (which can be found at www.itu.int/ITU-T/publications/recs.html) mentioned in this manual, the following material was also used.

- [ApplCryp] B. Schneier, "Applied Cryptography – Protocols, Algorithms and Source Code in C" 2nd edition, Wiley, 1996; ISBN 0-471-12845-7
 - [Chadwick] D. W. Chadwick; "The Use of X.509 in E-Healthcare", Workshop on Standardization in E-health; Geneva, 23-25 May 2003; PowerPoint at www.itu.int/itudoc/itu-t/workshop/e-health/s5-02.html and audio presentation at www.itu.int/ibs/ITU-T/e-health/Links/B-20030524-1100.ram
 - [Euchner] M. Euchner, P-A. Probst; "Multimedia Security within Study Group 16: Past, Presence and Future", ITU-T Security Workshop; 13-14 May 2002, Seoul, Korea; www.itu.int/itudoc/itu-t/workshop/security/present/s2p3r1.html
 - [FreePresc] Free prescriptions statistics in the UK; www.doh.gov.uk/public/sb0119.htm
 - [Packetizer] "A Primer on the H.323 Series Standard" www.packetizer.com/iptel/h323/papers/primer/
 - [Policy] D. W. Chadwick, D. Mundy; "Policy Based Electronic Transmission of Prescriptions"; IEEE POLICY 2003, 4-6 June, Lake Como, Italy. sec.isi.salford.ac.uk/download/PolicyBasedETP.pdf
 - [SG17] ITU-T Study Group 17; "Lead Study Group on Communication System Security" www.itu.int/ITU-T/studygroups/com17/cssecurity.html (Section 2 on the Catalogue of ITU-T Recommendations related to Communications System Security; Section 3 on Compendium of Security Definitions in ITU-T Recommendations)
 - [Shannon] G. Shannon; "Security Vulnerabilities in Protocols"; ITU-T Security Workshop; 13-14 May 2002, Seoul, Korea; www.itu.int/itudoc/itu-t/workshop/security/present/s1p2.html
 - [Wisekey] S. Mandil, J. Darbellay; "Public Key Infrastructures in e-health"; written contribution to Workshop on Standardization in E-health; Geneva, 23-25 May 2003; www.itu.int/itudoc/itu-t/workshop/e-health/wcon/s5con002_ww9.doc
- ISO/IEC 9796-1:1991 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 1: Mechanisms using redundancy
- ISO/IEC 9979:1999 (2nd edition) Procedure for registering cryptographic algorithms.
 [Note: See www.iso-register.com where all relevant information is available on any standardized algorithm.]

Annex A

Catalogue of ITU-T Recommendations related to security

Compiled by ITU-T Study Group 17, Lead Study Group on Communication Systems Security (CSS)

No.	TITLE	MAIN PURPOSE and SECURITY ASPECTS	Study Group
E.408	Telecommunication networks security requirements	Provides an overview of security requirements and a framework that identifies security threats to telecommunication networks in general (both fixed and mobile; both voice and data) and gives guidance for planning countermeasures that can be taken to mitigate the risks arising from the threats.	SG2
E.409	Incident Organization and Security Incident Handling: Guidelines for Telecommunications Organizations	Analyses, structures and suggests a method for establishing an incident management organization within a telecommunications organization involved in the provision of international telecommunications, where the flow and structure of an incident are focused. The flow and the handling are useful in determining whether an event is to be classified as an event, an incident, a security incident or a crisis. The flow also covers the critical first decisions that have to be made. To be able to succeed in incident handling and incident reporting one must have an understanding of how incidents are detected, handled and resolved. By establishing a general structure for incidents (i.e. physical, administrative or organizational, and logical incidents) it is possible to obtain a general picture of the structure and flow of an incident. A uniform terminology is the base for a common understanding of words and terms.	SG2
F.400	Message Handling System and Service overview	Provides an overview to define the overall system and service of an MHS and serves as a general overview of MHS. This Overview is one of a set of Recommendations, which describe the system model and elements of service of the Message Handling System (MHS) and services. This Recommendation overviews the capabilities of an MHS that are used by Service providers for the provision of public Message Handling (MH) services to enable users to exchange messages on a store-and-forward basis. The message handling system is designed in accordance with the principles of the Reference Model of Open Systems Interconnection (OSI Reference Model) for ITU-T applications (X.200) and uses the presentation layer services and services offered by other, more general, application service elements. An MHS can be constructed using any network fitting in the scope of OSI. The message transfer service provided by the MTS is application independent. Examples of standardized applications are the IPM service (F.420 plus X.420), the EDI Messaging service (F.435 plus X.435) and the Voice Messaging Service (F.440 plus X.440). End systems can use the Message Transfer (MT) service for specific applications that are defined bilaterally. Message handling services provided by Service providers belong to the group of Telematic services. The public services built on MHS, as well as access to and from the MHS for public services are defined in the F.400-series Recommendations. The technical aspects of MHS are defined in the X.400-series Recommendations. The overall system architecture of MHS is defined in ITU-T Rec. X.402. Elements of service are the service features provided through the application processes. The elements of service are considered to be components of the services provided to users and are either elements of a basic service or they are optional user facilities, classified either as essential optional user facilities, or as additional optional user	SG17

		facilities. Security capabilities of MHS are described in §15 of F.400 including MHS-security threats, Security model, elements of service describing the security features (defined in Annex B), Security management, MHS-security dependencies, IPM security.	
F.440	Message Handling Services: The Voice Messaging (VM-) Service.	Specifies the general, operational and quality of service aspects of the public international Voice Messaging (VM-) service, a specific type of Message Handling (MH) service, that is an international telecommunication service offered by Administrations, enabling subscribers to send a message to one or more recipients and to receive messages via telecommunication networks using a combination of store and forward, and store and retrieve techniques. The VM-service enables subscribers to request a variety of features to be performed during the handling and exchange of voice encoded messages. Some features are inherent in the basic VM-service. Other non-basic features may be selected by the subscriber, either on a per-message basis or for an agreed contractual period of time, if they are provided by Administrations. Intercommunication with the Interpersonal Messaging (IPM) service may be provided as an option in the VM-service. Basic features have to be made available internationally by Administrations. Non-basic features, visible to the subscriber, are classified as either essential or additional. Essential optional features must be made available internationally by Administrations. Additional optional features may be made available by some Administrations for national use and internationally on the basis of bilateral agreement. Non-basic features are called optional user facilities. VM-service may be provided using any communications network. VM-service may be offered separately or in combination with various Telematic or data communication services. Technical specifications and protocols, to be used in the VM-service are defined in the X.400-Series Recommendations. Annex G: Secure voice messaging elements of service; Annex H: Voice Messaging security overview	SG17
F.851	Universal Personal Telecommunication (UPT) - Service description (service set 1)	Is intended to provide the service description and operational provisions for Universal Personal Telecommunication (UPT). This Recommendation provides the general service description from the point of view of the individual UPT subscriber or UPT user. UPT also allows the UPT user to participate in a user-defined set of subscribed services, from amongst which the user defines personal requirements, to form a UPT service profile. The UPT user may use the UPT service with minimal risk of violated privacy or erroneous charging due to fraudulent use. In principle, any basic telecommunications service can be used with the UPT service. The services provided to the UPT user are only limited by the networks and terminals used. Among essential user features the first is the "UPT user <i>identity authentication</i> ", and as optional user feature there is the UPT service <i>provider authentication</i> . Section 4.4 details security requirements.	SG2
G.808.1	Generic protection switching – Linear trail and subnetwork protection	Provides an overview of linear protection switching. It covers Optical Transport Networks (OTN), Synchronous Digital Hierarchy (SDH) networks and Asynchronous Transfer Mode (ATM) networks based protection schemes. Overviews of ring protection and dual node sub-network (e.g. ring) interconnect schemes will be provided in other Recommendations.	SG15
G.827	Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths	Defines network performance parameters and objectives for the path elements and end-to-end availability of international constant bit-rate digital paths. These parameters are independent of the type of physical network supporting the end-to-end path, e.g., optical fibre, radio relay or satellite. Guidance is included on methods for improving availability and calculating the end-to-end availability of a combination of network elements.	SG13

G.841	Types and characteristics of SDH network protection architectures	Describes the various protection mechanisms for Synchronous Digital Hierarchy (SDH) networks, their objectives and their applications. Protection schemes are classified as SDH trail protection (at the section or path layer) and as SDH sub-network connection protection (with inherent monitoring, non-intrusive monitoring, and sub-layer monitoring).	SG15
G.842	Interworking of SDH network protection architectures	Describes mechanisms for interworking between network protection architectures. Interworking is described for single and dual node interconnection for exchanging traffic between rings. Each ring may be configured for MS-shared protection or for SNCP protection.	SG15
G.873.1	Optical Transport Network (OTN) – Linear protection	Defines the APS protocol and protection switching operation for the linear protection schemes for the Optical Transport Network at the Optical Channel Data Unit (ODUk) level. Protection schemes considered in this Recommendation are ODUk trail protection; ODUk sub-network connection protection with inherent monitoring; ODUk sub-network connection protection with non-intrusive monitoring; and ODUk sub-network connection protection with sub-layer monitoring.	SG15
G.911	Parameters and calculation methodologies for reliability and availability of fiber optic systems	Identifies a minimum set of parameters necessary to characterize the reliability and availability of fibre optic systems. Different parameters are given for system reliability and maintenance, for active optic device reliability, for passive optical device reliability, and for optical fibre and cable reliability. It also provides guidelines and methods for calculating the predicted reliability of devices, units and systems. Examples are included.	SG15
H.233	Confidentiality system for audiovisual services	A <i>privacy</i> system consists of two parts, the <i>confidentiality mechanism</i> or <i>encryption process</i> for the data, and a <i>key management</i> subsystem. This Recommendation describes the confidentiality part of a privacy system suitable for use in narrow-band audiovisual services. Although an <i>encryption algorithm</i> is required for such a privacy system, the specification of such an algorithm is not included here: the system caters for more than one specific algorithm. The <i>confidentiality system</i> is applicable to point-to-point links between terminals or between a terminal and a Multipoint Control Unit (MCU); it may be extended to multipoint working in which there is no decryption at the MCU.	SG16
H.234	Encryption key management and authentication system for audiovisual services	A <i>privacy system</i> consists of two parts, the <i>confidentiality mechanism</i> or <i>encryption process</i> for the data, and a <i>key management</i> subsystem. This Recommendation describes <i>authentication and key management</i> methods for a privacy system suitable for use in narrow-band audiovisual services. <i>Privacy</i> is achieved by the use of <i>secret keys</i> . The keys are loaded into the <i>confidentiality part</i> of the privacy system and control the way in which the transmitted data is encrypted and decrypted. If a third party gains access to the keys being used, then the privacy system is no longer secure. The maintenance of keys by users is thus an important part of any privacy system. Three alternative practical methods of <i>key management</i> are specified in this Recommendation.	SG16
H.235	Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals	Describes enhancements within the framework of the H.3xx-series Recommendations to incorporate <i>security services</i> such as <i>Authentication and Privacy (data encryption)</i> . The proposed scheme is applicable to both simple point-to-point and multipoint conferences for any terminals using ITU-T H.245 control protocol. For example, H.323 systems operate over packet-based networks not providing guaranteed quality of service. For the same technical reasons that the base network does not provide QOS, the network does not provide a <i>secure service</i> . Secure real-time communication over insecure networks generally involves two major areas of concern – <i>authentication and privacy</i> . It describes the security infrastructure and specific <i>privacy techniques</i> to be employed by the H.3xx-series of	SG16

multimedia terminals. This Rec. will cover areas of concern for interactive conferencing. These areas include, but are not strictly limited to, *authentication and privacy* of all real-time media streams that are exchanged in the conference. It provides the protocol and algorithms needed between the H.323 entities.

This Rec. utilizes the general facilities supported in ITU-T H.245 and as such, any standard operated in conjunction with this control protocol may use this security framework. It is expected that, wherever possible, other H-series terminals may interoperate and directly utilize the methods described in this Recommendation. This Recommendation will not initially provide for complete implementation in all areas, and will specifically highlight *endpoint authentication and media privacy*.

It includes the ability to negotiate services and functionality in a generic manner, and to be selective concerning cryptographic techniques and capabilities utilized. The specific manner in which they are used relates to systems capabilities, application requirements and specific security policy constraints. It supports varied cryptographic algorithms, with varied options appropriate for different purposes; e.g. key lengths. Certain *cryptographic algorithms* may be allocated to specific security services (e.g. one for fast media stream encryption and another for signalling encryption).

It should also be noted that some of the available cryptographic algorithms or mechanisms may be reserved for export or other national issues (e.g. with restricted key lengths). This Rec. supports signalling of well-known algorithms in addition to signalling non-standardized or proprietary cryptographic algorithms. There are no specifically mandated algorithms; however, it is strongly suggested that endpoints support as many of the applicable algorithms as possible in order to achieve interoperability. This parallels the concept that the support of ITU-T H.245 does not guarantee the interoperability between two entities' codecs.

Version 2 of ITU-T H.235 supersedes H.235 version 1 featuring several improvements such as elliptic curve cryptography, security profiles (simple password-based and sophisticated digital signature), new security countermeasures (media anti-spamming), support for the Advanced Encryption Algorithm (AES), support for backend service, object identifiers defined and changes incorporated from the H.323 implementors guide.

Version 3 of H.235 supersedes H.235 version 2 featuring a procedure for encrypted DTMF signals, object identifiers for the AES encryption algorithm for media payload encryption, the enhanced OFB (EOFB) stream-cipher encryption mode for encryption of media streams, an authentication-only option in Annex D for smooth NAT/firewall traversal, a key distribution procedure on the RAS channel, procedures for more secure session key transport and more robust session key distribution and updating, procedures for securing multiple payload streams, better security support for direct-routed calls in a new Annex I, signaling means for more flexible error reporting, clarifications and efficiency improvements for fast start security and for Diffie-Hellman signaling along with longer Diffie-Hellman parameters and changes incorporated from the H.323 implementors guide.

H.235 Annex F: *Hybrid Security Profile*. This annex describes an efficient and scaleable, *PKI-based hybrid security profile* deploying *digital signatures* from H.235 Annex E and deploying the *baseline security profile* from H.235 Annex D. This annex is suggested as an option. H.323 *security entities* (terminals, gatekeepers, gateways, MCUs, etc.) may implement this *hybrid security profile* for improved security or whenever required. The notion of "hybrid" in this text shall mean that security procedures from the signature profile in H.235 Annex E are actually applied in a lightweight sense; the digital signatures still conform to the RSA procedures. However, *digital signatures* are deployed only where absolutely necessary while high efficient *symmetric security*

		<p><i>techniques</i> from the baseline security profile in H.235 Annex D are used otherwise. The hybrid security profile is applicable for scaleable "global" IP telephony. This security profile overcomes the limitations of the simple, baseline security profile of H.235 Annex D when applying it strictly. Furthermore, this security profile overcomes certain drawbacks of H.235 Annex E such as the need for higher bandwidth and increased performance needs for processing when applying it strictly. For example, the hybrid security profile does not depend on the (static) administration of mutual shared secrets of the hops in different domains. Thus, users can choose their VoIP provider much easier. Thus, this security profile supports a certain kind of user mobility as well. It applies asymmetric cryptography with signatures and certificates only where necessary and uses otherwise simpler and more efficient symmetric techniques. It provides tunneling of H.245 messages for H.245 message integrity and also some provisions for non-repudiation of messages. The hybrid security profile mandates the GK-routed model and is based upon the H.245 tunneling techniques; support for non GK-routed models is for further study.</p>	
H.323	Packet-based multimedia communications system	<p>Describes terminals and other entities providing real-time audio, video, data and/or multimedia communications services over Packet Based Networks (PBN), which may not provide a guaranteed Quality of Service. Support for audio is mandatory, data and video are optional, but if supported, the ability to use a common mode of operation is mandatory, so that all terminals supporting that media type can interwork. The packet based network may include Local Area Networks, Enterprise Area Networks, Metropolitan Area Networks, Intra-Networks, and Inter-Networks (including the Internet), point-to-point connections, a single network segment, or an internetwork having multiple segments with complex topologies, therefore entities can use point-to-point, multipoint, or broadcast configurations. Such entities may interwork with terminals on B-ISDN, N-ISDN, Guaranteed Quality of Service LANs, GSTN and/or wireless networks, and entities may be integrated into personal computers or implemented in stand-alone devices such as videotelephones.</p> <p>Annex J: Security for Simple endpoint types</p>	SG16
H.350.2	Directory services architecture for H.235	<p>Describes an LDAP schema to represent H.235 elements. It is an auxiliary class related to H.350 and derives much of its functionality from that architecture. Implementers should review H.350 in detail before proceeding with this Rec. Its attributes include H.235 identity, password and certificate elements. These elements can be downloaded to an endpoint for automatic configuration or accessed by a gatekeeper for call signalling and authentication.</p> <p>The scope of this Rec. does not include normative methods for the use of the LDAP directory itself or the data it contains. The purpose of the schema is not to represent all possible data elements in the H.235 protocol, but rather to represent the minimal set required to accomplish the design goals enumerated in H.350.</p>	SG16
H.530	Security for H.510 in H.323 Multimedia Mobile Environments	<p>Provides security procedures in H.323 mobility environments such as under scope of H.510 that describes mobility for H.323 multimedia systems and services. It provides the details about the security procedures for H.510. So far, the signaling capabilities of H.235 in version 1 and 2 are designed to handle security in mostly static H.323 environments. Those environments and multimedia systems can achieve some limited mobility within gatekeeper zones; H.323 in general and H.235 specifically provide only very little support for secure roaming of mobile users and terminals across different domains with many involved entities in a mobility, distributed environment for example. The H.323 mobility scenarios depicted in H.510 regarding terminal mobility pose a new situation with their flexible and dynamic character also from a security point of view. Roaming H.323 users and mobile terminals have to be authenticated by a foreign, visited domain. Likewise, the</p>	SG16

		mobile user would like to obtain evidence about the true identity of the visited domain. In addition to that, it may be also useful to obtain evidence about the identity of the terminals complementing user authentication. Thus, these requirements demand for mutual authentication of the user and the visited domain and optionally also of the identity of the terminal. Usually initially only the home domain knows the mobile user, where he or she is subscribed and assigned a password; the visited domain does not know the mobile user. As such, the visited domain does not share any established security relationship with the mobile user and the mobile terminal. In order let the visited domain achieve the authentication and authorization assurance for the mobile user and the mobile terminal, the visited domain would relay certain security tasks such as authorization checks or key-management to the home domain through intermediate network and service entities. This requires securing the communication and key management between the visited domain and the home domain too. While in principle, mobility H.323 environments are more open than closed H.323 networks; there is of course also need to secure the key management tasks appropriately. It is also true, that communication within and across the mobility domains deserves protection against malicious tampering.	
J.93	Requirements for conditional access in the secondary delivery of digital television or cable television systems	Defines the data privacy and access requirements protecting MPEG digital television signals passed on cable television networks between the cable head-end and the ultimate subscriber. The exact cryptographic algorithms used in this process are not in J.93 as they are regionally and/or industry determined.	SG9
J.96 Amd. 1	Technical method for ensuring privacy in long-distance international MPEG-2 television transmission conforming to Recommendation J.89	Contains a common standard for a conditional access system for long distance international transmission of digital television conforming to the MPEG-2 Professional Profile (4:2:2). The Basic Interoperable Scrambling System (BISS) based on the DVB-CSA specification using fixed clear keys called Session Words is described. Another backward compatible mode introduces an additional mechanism to insert Encrypted Session Words, while at the same time conserves interoperability.	SG9
J.112	Transmission systems for interactive cable television services	Digital television services have been established in many countries and the benefits of extending these to provide interactive services are widely recognized. Cable television distribution systems are particularly suited for the implementation of bidirectional data services and this Recommendation complements and extends the scope of J.83 "Digital multi-programme systems for television, sound and data services for cable distribution" to make provision for bidirectional data over coaxial and hybrid fibre-coax cables for interactive services. It also contains several annexes in recognition of different existing media environments. It is recommended that for the introduction of fast Internet access and/or interactive cable television services, the systems be used to achieve the benefits of economies of scale and facilitate interoperability. Security requirements are established, the use of SP-DOCSS Data Over Cable Security System (DOCSS) Specification; SP-RSM Removable Security Module Specification and SP-BDS Baseline Data-Over-Cable Security Specification is recommended.	SG9

J.160	Architectural framework for the delivery of time-critical services over cable television networks using cable modems	Provides the architectural framework that will enable cable television operators to provide time-critical services over their networks that have been enhanced to support cable modems. The security services available through IPCom's core service layer are authentication, access control, integrity, confidentiality and non-repudiation. An IPCom protocol interface may employ zero, one or more of these services to address its particular security requirements. IPCom security addresses the security requirements of each constituent protocol interface by: <ul style="list-style-type: none"> • identifying the threat model specific to each constituent protocol interface; • identifying the security services (authentication, authorization, confidentiality, integrity, and non-repudiation) required to address the identified threats; • specifying the particular security mechanism providing the required security services. The security mechanisms include both the security protocol (e.g. IPsec, RTP-layer security, and SNMPv3 security) and the supporting key management protocol (e.g. IKE, PKINIT/Kerberos).	SG9
J.170	IPCom security specification	Defines the Security Architecture, protocols, algorithms, associated functional requirements and any technological requirements that can provide for the security of the system for the IPCom network. <i>Authentication, access control, message and bearer content integrity, confidentiality and non-repudiation security services</i> must be provided as defined herein for each of the network element interfaces.	SG9
J.191	IP feature package to enhance cable modems	Provides a set of IP-based features that may be added to a cable modem that will enable cable operators to provide an additional set of enhanced services to their customers including support for IPCom Quality of Service (QoS), enhanced security, additional management and provisioning features, and improved addressing and packet handling. These IP-based features reside in the logical element Portal Service (PS or just Portal). A Cable Modem that contains these enhanced features is an IP-enhanced Cable Modem (IPCM), and is an implementation of a J.190 HA device class. As described in Rec. J.190, the HA device class includes both Cable Modem functionality as well as Portal Services functionality. Chapter 11 security: defines the security interfaces, protocols and functional requirements needed to reliably deliver cable-based IP services in a secure environment to the PS. The purpose of any security technology is to protect value, whether a revenue stream, or a purchasable information asset of some type. Threats to this revenue stream exist when a user of the network perceives the value, expends effort and money, and invents a technique to get around making the necessary payments. Annex C: Security threats and preventative measures.	SG9
M.3010	Principles for a telecommunications management network	Defines concepts of Telecommunications Management Network (TMN) architectures (TMN functional architecture, TMN information architecture, and TMN physical architectures) and their fundamental elements and describes the relationship among the three architectures and provides a framework to derive the requirements for the specification of TMN physical architectures from the TMN functional and information architectures. A logical reference model for partitioning of management functionality, the Logical Layered Architecture (LLA), is provided. This Rec. also defines how to demonstrate TMN conformance and compliance for the purpose of achieving interoperability. The requirements of the TMN involve the ability to ensure secure access to management information by authorized management information users. TMN includes functional blocks for which security functionality is performed by security techniques to protect the TMN environment in order to assure the safety of the information exchanged over the interfaces and residing in the management application. Security principles and mechanisms are also related to the control of access rights of the TMN users to information associated with TMN applications.	SG4

M.3016	Overview of TMN Security (M.3sec)	Provides an overview and framework that identifies security threats to a TMN and outlines how available security services can be applied within the context of the TMN functional architecture, as described in Recommendation M.3010. This Rec. is generic in nature and does not identify or address the requirements for a specific TMN interface.	SG4
M.3210.1	TMN management services for IMT-2000 security management (M.IMTSEC)	Is one of the series of TMN Management Service Recommendations that provide description of management services, goals and context for management aspects of IMT-2000 networks. This Rec. describes a subset of Security Management services to provide Requirements and Analysis of the Security management and a profile for <i>fraud management</i> in an IMT-2000 mobile network. The emphasis is on the X interface between two service providers and the management services needed between the two to detect and prevent fraud by operating the Fraud Information Gathering System (FIGS) as means to monitor a defined set of subscriber activities to limit their financial exposure to large unpaid bills produced on subscriber accounts whilst the subscriber is roaming. It builds on the function sets identified in ITU T M.3400 by defining new function sets, functions and parameters and adding additional semantics and restrictions.	SG4
M.3320	Management requirements framework for the TMN X interface	Is part of a series dealing with the transfer of information for the management of telecommunication networks and services, and only some parts address security aspects. The purpose of this Rec. is to define a requirements framework for all functional, service and network-level requirements for the TMN exchange of information between Administrations. It also provides for the general framework of using the TMN X-interface for the exchange of information between Administrations, Recognized Operating Agencies, other Network Operators, Service Providers, Customers and other entities. It includes specifications of the security requirements of the TMN X interface.	SG4
M.3400	TMN management functions	Is one of a series of Recommendations of the Telecommunications Management Network (TMN), providing specifications of TMN management functions and TMN management function sets. The content is developed in support of Task Information Base B (Roles, resources and functions), associated with Task 2 (Describe TMN management context) in the TMN interface specification methodology specified in ITU-T M.3020. When performing the analysis of TMN management context, it is desirable to consider maximal use of the TMN management function sets available in this Recommendation. It includes descriptions of the security management function supported by the TMN.	SG4
Q.293	Intervals at which security measures are to be invoked	This is an extract from the Blue Book and contains only sections 8.5 (Intervals at which security measures are to be invoked) to 8.9 (Load sharing method) of Q.293	SG4
Q.813	Security transformations application service element for remote operations service element (STASE-ROSE)	Provides specifications to support security transformations, such as <i>encryption, hashing, sealing and signing</i> , focusing on whole Remote Operations Service Element (ROSE) Protocol Data Units (PDUs). Security transformations are used to provide various security services such as <i>authentication, confidentiality, integrity and non-repudiation</i> . This Recommendation describes an approach to the provisioning of security transformations that is implemented in the application layer and requires no security-specific functionality in any of the underlying OSI stack layers. This Recommendation enhances TMN security by supporting security transformations for ROSE PDUs and exchange of related security information.	SG4

Q.815	Specification of a security module for whole message protection	Specifies an optional security module to be used with Rec. Q.814, Specification of an Electronic Data Interchange Interactive Agent that provides security services for whole Protocol Data Units (PDUs). In particular, the security module supports <i>non-repudiation of origin and of receipt</i> , as well as whole <i>message integrity</i> .	SG4
Q.817	TMN PKI – Digital certificates and certificate revocation lists profiles	Explains how Digital Certificates and Certificate Revocation Lists can be used in the TMN and provides requirements on the use of Certificate and Certificate Revocation List extensions. Is intended to promote interoperability among TMN elements that use Public Key Infrastructure (PKI) to support security-related functions. The purpose is to provide interoperable, scalable mechanism for <i>key distribution and management</i> within a TMN, across all interfaces, as well as in support of <i>non-repudiation service</i> over the X interface. It applies to all TMN interfaces and applications. It is independent of which communications protocol stack or which network management protocol is being used. PKI facilities can be used for a broad range of security functions, such as, <i>authentication, integrity, non-repudiation, and key exchange</i> (M.3016). However, it does not specify how such functions should be implemented, with or without PKI.	SG4
Q.1531	UPT security requirements for service Set 1	Specifies UPT security requirements for both user-to-network and internetwork communication applicable to UPT Service Set 1 as defined within Rec. F.851. This Rec. covers all aspects of security for UPT using DTMF accesses and out-band DSS 1 based user accesses.	SG15
Q.1741.1	IMT-2000 references to release 1999 of GSM evolved UMTS core network with UTRAN access network	Includes references to the 3GPP security specifications i.e. to <i>TS 21.133: Security Threats and Requirements, TS 33.102: Security Architecture, TS 33.103: Security Integration Guidelines, TS 33.105: Cryptographic Algorithm requirements, TS 33.106: Lawful interception requirements, TS 33.107: Lawful interception Architecture and Functions, TS 33.120: Security Objectives and Principles</i>	SSG
Q.1741.2	IMT-2000 references to release 4 of GSM evolved UMTS core network with UTRAN access network	Includes references to the 3GPP security specifications as <i>TS 21.133: Security Threats and Requirements, TS 22.048: Security Mechanisms for the (U) SIM application toolkit, TS 22.101: Service aspects; Service principles, TS 33.102: Security Architecture, TS 33.103: Security Integration Guidelines, TS 33.105: Cryptographic Algorithm requirements, TS 33.106: Lawful interception requirements, TS 33.107: Lawful interception Architecture and Functions, TS 33.120: Security Objectives and Principles, TS 33.200: Network Domain Security – MAP, TS 35.205, .206, .207, and .208: Specification of the MILENAGE Algorithm Set</i>	SSG
Q.1741.3	IMT-2000 references to release 5 of GSM evolved UMTS core network with UTRAN access network	Includes references to the 3GPP security specifications as <i>TS 22.101: Service aspects; Service principles, TS 33.102: Security Architecture, TS 33.106: Lawful interception requirements, TS 33.107: Lawful interception Architecture and Functions, TS 33.108: Handover interface for Lawful Interception (LI), TS 33.200: Network Domain Security – MAP, TS 33.203: Access security for IP-based services, TS 33.210: Security; Network Domain Security (NDS); IP network layer security, TS 35.205, .206, .207, .208 and .909: Specification of the MILENAGE Algorithm Set</i>	SSG
T.30	Procedures for document facsimile transmission in the general switched telephone network	Annex G provides procedures for secure G3 document facsimile transmission using the HKM and HFX system, Annex H provides for security in facsimile G3 based on the <i>RSA algorithm</i>	SG16
T.36	Security capabilities for use with Group 3 facsimile terminals	Defines the two independent technical solutions, which may be used in the context of secure facsimile transmission. The two technical solutions are based upon the HKM/HFX40 algorithms and the <i>RSA algorithm</i> .	SG16

T.123 Annex B	Extended Transport Connections	This annex to revised T.123 features a <i>connection negotiation protocol (CNP)</i> that offers security capability negotiation. The security mechanism applied includes various means for network and transport security on a node-to-node basis and covers means such as TLS/SSL, IPSEC w/o IKE or manual <i>key management</i> , X.274/ ISO TLSP and GSS-API.	SG16
T.503	A document application profile for the interchange of Group 4 facsimile documents	Defines a document application profile that may be used by any Telematic service. Its purpose is to specify an interchange format suitable for the interchange of Group 4 facsimile documents that contain only raster graphics. Documents are interchanged in a formatted form, which enables the recipient to display or print the document as intended by the originator.	SG16
T.563	Terminal Characteristics for Group 4 facsimile apparatus	Defines the general aspects of Group 4 facsimile apparatus and the interface to the physical network.	SG16
T.611	Programming Communication Interface (PCI) APPLI/COM for Facsimile Group 3, Facsimile Group 4, Teletex, Telex, E-mail and file transfer services	Defines a Programming Communication Interface called "APPLI/COM", which provides unified access to different communications services, such as telefax group 3 or other Telematic services. This Rec. describes the structure and contents of messages and the way to exchange them between a Local Application (LA) and a Communication Application (CA). Any communication is preceded by a login process and terminated by a logout process, where both the processes facilitate the implementation of security schemes especially important on multi-user systems, and provide means to implement security mechanisms between the LA and the CA. This Rec. forms a high level API (Application Programming Interface), which gives powerful control and monitoring on the telecommunication activity to the application designers.	SG16
X.217	Information technology - Open Systems Interconnection - Service definition for the association control service element -	Defines Association Control Service Element (ACSE) services for application-association control in an open systems interconnection environment. ACSE supports connection-oriented and connectionless modes of communication. Three functional units are defined in the ACSE. The mandatory <i>Kernel functional unit</i> is used to establish and release application-associations. The ACSE includes two optional functional units, one of them is the optional <i>Authentication</i> functional unit, which provides additional facilities for exchanging information in support of authentication during association establishment without adding new services. The ACSE <i>authentication facilities</i> may be used to support a limited class of <i>authentication methods</i> . Amendment 1 provides support of authentication mechanisms for the connectionless mode.	SG17

X.227	Information technology – Open Systems Interconnection – Connection-oriented protocol for the Association Control Service Element: Protocol specification.	This Protocol Specification defines procedures that are applicable to instances of communication between systems, which wish to interconnect in an Open Systems Interconnection environment in a connection-oriented mode, i.e. a connection-oriented mode protocol for the application-service-element for application-association control, the Association Control Service Element (ACSE). The Protocol Specification includes the <i>Kernel functional</i> unit that is used to establish and release application-associations. The <i>Authentication functional</i> unit provides additional facilities for exchanging information in support of <i>authentication</i> during association establishment without adding new services. The ACSE <i>authentication facilities</i> can be used to support a limited class of <i>authentication methods</i> . The Application Context Negotiation functional unit provides additional facility for the selection of the application context during association establishment. This Protocol Specification includes an annex that describes a protocol machine, referred to as the Association Control Protocol Machine (ACPM), in terms of a state table. This Protocol Specification includes an annex that describes a simple authentication-mechanism that uses a password with an AE title, and is intended for general use, and includes also an example of an <i>authentication-mechanism specification</i> . To this authentication-mechanism the following name (of ASN.1 datatype OBJECT IDENTIFIER) is assigned: {joint-iso-itu-t(2) association-control(2) authentication-mechanism(3) password-1(1)}. For this authentication-mechanism, the password is the authentication-value. The data type of authentication-value shall be "GraphicString".	SG17
X.237	Information technology - Open Systems Interconnection - Connectionless protocol for the Association Control Service Element: Protocol specification	Amendment 1 to this Recommendation includes the ASN.1 extensibility marker in the module describing the protocol. It also enhances the connectionless ACSE protocol specification to provide support for conveyance of authentication parameters in the A-UNIT-DATA APDU.	SG17
X.257	Information technology - Open Systems Interconnection - Connectionless protocol for the Association Control Service Element: Protocol Implementation Conformance Statement (PICS) proforma	Provides the protocol implementation conformance statement (PICS) proforma for the OSI connectionless protocol for the Association Control Service Element (ACSE), which is specified in Recommendation X.237. The PICS proforma represents, in tabular form, the mandatory and optional elements of the connectionless ACSE protocol. The PICS proforma is used to indicate the features and choices of a particular implementation of the connectionless ACSE protocol.	SG17

X.272	Data compression and privacy over frame relay networks	Defines Data Compression Service and Privacy Service for Frame Relay networks including negotiation and encapsulation of Data Compression, <i>Secure data compression, authentication and encryption</i> over frame relay. The presence of a data <i>compression service</i> in a network will increase the effective throughput of the network. The demand for transmitting sensitive data across public networks requires facilities for ensuring the <i>privacy</i> of the data. In order to achieve optimum compression ratios, it is essential to compress the data before <i>encrypting</i> it. Hence, it is desirable to provide facilities in the <i>data compression service</i> to negotiate <i>data encryption protocols</i> as well. Since the task of compressing and then encrypting the data is computational intensive, efficiency is achieved through providing simultaneous <i>data compression and encryption (secure data compression)</i> . Data Compression protocols are based on PPP Link Control Protocol (IETF RFC 1661) and PPP Encryption Control Protocol (IETF RFC 1968 and 1969). This Recommendation applies to Unnumbered Information (UI) frames encapsulated using Q.933 Annex E. It addresses data compression and privacy on both permanent virtual connections (PVC) and switched virtual connections (SVC).	SG17
X.273	Information technology - Open Systems Interconnection - Network layer security protocol	Specifies the protocol to support the <i>integrity, confidentiality, authentication and access control services</i> identified in the OSI security model as applicable to connection-mode and connectionless-mode network layer protocols. The protocol supports these services through the use of <i>cryptographic mechanisms, security labeling</i> and assigned <i>security attributes</i> , such as <i>cryptographic keys</i> .	SG17
X.274	Information technology - Telecommunications and information exchange between systems - Transport layer security protocol	Specifies the protocol, which can support the <i>integrity, confidentiality, authentication and access control services</i> identified in the OSI security model as relevant to the transport layer. The protocol supports these services through the use of <i>cryptographic mechanisms, security labeling</i> and assigned <i>attributes</i> , such as <i>cryptographic keys</i> .	SG17
X.400/ F.400	Message handling system and service overview	Defines Message Handling System (MHS) elements of service for User Agent (UA)-to-UA, Message Transfer Agent (MTA)-to-MTA, UA-to-MTA, and UA-to-Message Store (MS) security services of <i>confidentiality, integrity, authentication, non-repudiation</i> and <i>access control</i> identified as relevant to the Application Layer. (See F.400)	SG17
X.402	Information technology - Message Handling Systems (MHS): Overall architecture	This Recommendation specifies security procedures and Object Identifiers for use in MHS protocols to realize the services of <i>confidentiality, integrity, authentication, non-repudiation</i> and <i>access controls</i> identified as relevant to the Application Layer.	SG17
X.411	Information technology - Message Handling Systems (MHS) - Message transfer system: Abstract service definition and procedures	Specifies mechanisms and procedures supporting <i>confidentiality, integrity, authentication and non-repudiation services</i> identified as relevant to the Application Layer. The protocol supports these services through the use of <i>cryptographic mechanisms, security labeling, and digital signatures</i> as identified in Recommendation X.509. Although this Recommendation specifies protocol that uses <i>asymmetric cryptographic techniques, symmetric cryptographic techniques</i> are also supported.	SG17
X.413	Information technology - Message Handling Systems (MHS): Message Store: Abstract service definition	Specifies mechanisms, protocol and procedures supporting <i>integrity, access control, authentication and non-repudiation services</i> identified as relevant to the Application Layer. The protocol supports these services on behalf of the Message Store direct user.	SG17

X.419	Information technology - Message Handling Systems (MHS): Protocol specifications	Specifies procedures and application contexts to identify secure access for MHS entities and remote users by providing <i>authentication and access control</i> services identified as relevant to the Application Layer.	SG17
X.420	Information technology - Message Handling Systems (MHS) - Interpersonal messaging system	Specifies mechanisms, protocol and procedures for the exchange of objects between Interpersonal Messaging Users or User Agents on behalf of its direct user identified relevant to the Application Layer. The security services supported are <i>integrity, confidentiality, authentication and access control</i> identified as relevant to the Application Layer.	SG17
X.435	Information technology - Message Handling Systems: Electronic data interchange messaging system	Specifies mechanisms, protocol and procedures for the exchange of objects between Electronic Data Interchange (EDI) User Agents on behalf of its direct user. The security services supported are <i>integrity, confidentiality, authentication and access control</i> identified as relevant to the Application Layer.	SG17
X.440	Information technology - Message Handling Systems: Voice messaging system	Specifies mechanisms, protocol and procedures for the exchange of objects between Voice User Agents on behalf of its direct user. The security services supported are <i>integrity, confidentiality, authentication and access control</i> identified as relevant to the Application Layer.	SG17
X.500	Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services	Together with other Recommendations, has been produced to facilitate the interconnection of information processing systems to provide directory services. A set of such systems, together with the directory information that they hold, can be viewed as an integrated whole, called the Directory. The information held by the Directory, collectively known as the Directory Information Base (DIB), is typically used to facilitate communication between, with or about objects such as application entities, people, terminals and distribution lists. The Directory plays a significant role in Open Systems Interconnection, whose aim is to allow, with a minimum of technical agreement outside of the interconnection standards themselves, the interconnection of information processing systems. This Rec. introduces and models the concepts of the Directory and of the DIB and overviews the services and capabilities, which they provide. Other Recommendations make use of these models in defining the abstract service provided by the Directory, and in specifying the protocols through which this service can be obtained or propagated. This Rec. specifies the Directory and its security features.	SG17
X.501	Information technology – Open Systems Interconnection – The Directory: Models	Provides a number of different models for the Directory as a framework for the other ITU-T Recommendations in the X.500 series. The models are the overall (functional) model, the administrative authority model, generic Directory Information models providing Directory User and Administrative User view on Directory information, generic Directory System Agent (DSA) and DSA information models and operational framework and a security model. It specifies the Directory use of its X.509 Public-key and attribute certificate frameworks.	SG17

X.509	Information technology - Open Systems Interconnection - The Directory: Authentication framework (1993 edition – <i>the second edition/version</i>) Authentication framework (1997 edition – <i>the third edition/version</i>) Public-key and attribute certificate frameworks (2000 edition – <i>the fourth edition/version</i>)	Defines a framework for public-key certificates and attribute certificates, and defines a framework for the provision of authentication services by Directory to its users. It describes two levels of authentication: <i>simple authentication</i> , using a password as a verification of claimed identity; and <i>strong authentication</i> , involving credentials formed using cryptographic techniques. While simple authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services. The frameworks defined may be used to profile application to <i>Public Key Infrastructures</i> (PKI) and <i>Privilege Management Infrastructures</i> (PMI). The framework for public-key certificates includes specification of data objects used to represent the certificates themselves as well as revocation notices for issued certificates that should no longer be trusted. While it defines some critical components of a PKI, it does not define a PKI in its entirety. However, it provides the foundation upon which full PKIs and their specifications would be built. The framework for attribute certificates includes specification of <i>data objects</i> used to represent the certificates themselves as well as <i>revocation notices</i> for issued certificates that should no longer be trusted. While it defines some critical components of a PMI, it does not define a PMI in its entirety. However, it provides the foundation upon which full PMIs and their specifications would be built. <i>Information objects</i> for holding PKI and PMI objects in the Directory and for comparing presented values with stored values are also defined.	SG17
X.519	Information technology - Open Systems Interconnection - The Directory: Protocol specification	Specifies procedures and application contexts to identify secure access during binding of Directory entities.	SG17

X.680	Information technology – OSI networking and system aspects – Abstract Syntax Notation One (ASN.1): Specification of basic notation	Provides a standard notation called Abstract Syntax Notation One (ASN.1) for defining the syntax of information data. It defines a number of simple data types and specifies a notation for referencing these types and for specifying values of these types. The ASN.1 notations can be applied whenever it is necessary to define the abstract syntax of information without constraining in any way how the information is encoded for transmission. ASN.1 is used for the definition of data types, values, and constraints on data types i.e. defines a number of simple types, with their tags, and specifies a notation for referencing these types and for specifying values of these types; defines mechanisms for constructing new types from more basic types, and specifies a notation for defining such types and assigning them tags, and for specifying values of these types; defines character sets (by reference to other Recs.) for use within ASN.1. 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 Rec. defines several basic types and their corresponding values, and rules for combining them into more complex types and values. In some protocol architectures, each message is specified as the binary value of a sequence of octets. However, standards-writers need to define quite complex data types to carry their messages, without concern for their binary representation. In order to specify these data types, they require a notation that does not necessarily determine the representation of each value. ASN.1 is such a notation. This notation is supplemented by the specification of one or more algorithms called encoding rules that determine the value of the octets that carry the application semantics (called the transfer syntax). NOTE: The ASN.1 series of Recs. (and in particular the ASN.1 distinguished and canonical encoding rules) have been used extensively in many security-related standards and Recommendations. In particular, H.323, and the X.400 and X.500 series are heavily dependent on ASN.1. These Recs. have formed, and continue to form important building blocks for security-related work.	SG17
X.681	Information technology – OSI networking and system aspects – Abstract Syntax Notation One (ASN.1): Information object specification	Provides the ASN.1 notation which allows information object classes as well as individual information objects and sets thereof to be defined and given reference names, i.e. provides notation for specifying information object classes, information objects and information object sets. An information object class defines the form of a conceptual table (an information object set) with one column for each field in the information object class, and with each complete row defining an information object. An application designer frequently needs to design a protocol which will work with any of a number of instances of some class of information objects, where instances of the class may be defined by a variety of other bodies, and may be added to over time. Examples of such information object classes are the "operations" of Remote Operations Service (ROS) and the "attributes" of the OSI Directory. This Rec. provides notation which allows information object classes as well as individual information objects and information object sets thereof to be defined and given reference names. See NOTE above (X.680).	SG17
X.682	Information technology – OSI networking and system aspects – Abstract Syntax Notation One (ASN.1): Constraint specification	Is part of Abstract Syntax Notation One (ASN.1) and provides notation for specifying user-defined constraints, table constraints, and contents constraints. Provides the ASN.1 notation for the general case of constraint and exception specification by which the data values of a structured data type can be limited. The notation also provides for signalling if and when a constraint is violated. Application designers require a notation to define a structured data type to convey their semantics and notation is also required to further constrain the values that can appear. Examples of such constraints are restricting the range of some component(s), or using a specified information object set to constrain an "ObjectClassFieldType" component, or using the "AtNotation" to specify a relation between components. See NOTE above (X.680).	SG17

X.683	Information technology – OSI networking and system aspects – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications	Is part of Abstract Syntax Notation One (ASN.1) and defines notation for parameterization of ASN.1 specifications, i.e. defines the provisions for parameterized reference names and parameterized assignments for data types which are useful for the designer when writing specifications where some aspects are left undefined at certain stages of the development to be filled in at a later stage to produce a complete definition of an abstract syntax. Application designers need to write specifications in which certain aspects are left undefined. Those aspects will later be defined by one or more other groups (each in its own way), to produce a fully defined specification for use in the definition of an abstract syntax (one for each group). In some cases, aspects of the specification (for example, bounds) may be left undefined even at the time of abstract syntax definition, being completed by the specification of International Standardized Profiles or functional profiles from some other body. See NOTE above (X.680).	SG17
X.690	Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)	Specifies a set of Basic Encoding Rules (BER) that may be applied to values of types defined using the ASN.1 notation, i.e. used to derive the specification of a transfer syntax for values of types defined using the notation specified in of X.680 series of ITU-T Recs. referred to as Abstract Syntax Notation One or ASN.1. Application of these encoding rules produces a transfer syntax for such values. It is implicit in the specification of these encoding rules that they are also used for decoding, i.e. these basic encoding rules are also to be applied for decoding such a transfer syntax in order to identify the data values being transferred. It also specifies a set of canonical and distinguished encoding rules that restrict the encoding of values to just one of the alternatives provided by the basic encoding rules, i.e. it 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. See NOTE above (X.680).	SG17
X.691	Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)	X.680 series of Recs. describe Abstract Syntax Notation One (ASN.1), a notation for the definition of messages to be exchanged between peer applications. This Recommendation describes a set of encoding rules that can be applied to values of all ASN.1 types to achieve a much more compact representation than that achieved by the Basic Encoding Rules and its derivatives (described in X.690), i.e. it specifies a set of Packed Encoding Rules that may be used to derive a transfer syntax for values of types defined in Rec. X.680. The Packed Encoding Rules are also to be applied for decoding such a transfer syntax in order to identify the data values being transferred. There are more than one set of encoding rules that can be applied to values of ASN.1 types. This Packed Encoding Rules (PER) are so called because they achieve a much more compact representation than that achieved by the Basic Encoding Rules (BER) and its derivatives described in Rec. X.690. See NOTE above (X.680).	SG17

X.692	Information technology – ASN.1 encoding rules: Specification of Encoding Control Notation (ECN) + Annex E: Support for Huffman encodings	Defines the Encoding Control Notation (ECN) used to specify encodings of ASN.1 types or of parts of types that differ from those provided by standardized encoding rules such as the Basic Encoding Rules (BER) and the Packed Encoding Rules (PER). It provides several mechanisms for such specification. It also provides the means to link the specification of encodings to the type definitions to which they are to be applied. ECN can be used to encode all types of an ASN.1 specification, but can also be used with standardized encoding rules such as BER or PER to specify only the encoding of types that have special requirements. An ASN.1 type specifies a set of abstract values. Encoding rules specify the representation of these abstract values as a series of bits. See NOTE above (X.680).	SG17
X.693	Information technology – ASN.1 encoding rules: XML encoding rules	The publication of Abstract Syntax Notation One (ASN.1) became the generally used notation for the definition of messages to be exchanged between peer applications. This Recommendation specifies encoding rules that may be applied to encode values of ASN.1 types using the Extensible Markup Language (XML), i.e. specifies a set of Basic XML Encoding Rules (XER) that may be used to derive a transfer syntax for values of types defined in X.680 series of Recs. This Recommendation also specifies a set of Canonical XML Encoding Rules which provide constraints on the Basic XML Encoding Rules and produce a unique encoding for any given ASN.1 value. It is implicit in the specification of these encoding rules that they are also used for decoding. Application of these encoding rules produces a transfer syntax for such values. It is implicit in the specification of these encoding rules that they are also to be used for decoding. There is more than one set of encoding rules that can be applied to values of ASN.1 types. This Rec. defines two sets of encoding rules that use the Extensible Markup Language (XML). These are called the XML Encoding Rules (XER) for ASN.1, and both produce an XML document compliant to W3C XML 1.0. The first set is called the Basic XML Encoding Rules. The second set is called the Canonical XML Encoding Rules because there is only one way of encoding an ASN.1 value using these encoding rules. (Canonical encoding rules are generally used for applications using security-related features such as digital signatures.)	SG17
X.733	Information technology – Open Systems Interconnection – Systems Management: Alarm reporting function	Defines a Systems Management Function which may be used by an application process in a centralized or decentralized management environment to interact for the purpose of systems management. This Recommendation defines a function which consists of generic definitions, services and functional units, is positioned in the application layer. The alarm notifications defined by this function provides information that a manager may need to act upon pertaining to a system's operational condition and quality of service.	SG4
X.735	Information technology – Open Systems Interconnection – Systems Management: Log control function	Defines a Systems Management Function which may be used by an application process in a centralized or decentralized management environment to interact for the purpose of systems management. This Recommendation defines the Log Control function and consists of services and two functional units. This function is positioned in the application layer.	SG4
X.736	Information technology – Open Systems Interconnection – Systems Management: Security alarm reporting function	Defines the security alarm reporting function, a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information for the purpose of systems management. This Recommendation is positioned in the application layer. The security alarm notifications defined by this systems management function provide information regarding operational condition and quality of service, pertaining to security.	SG4

X.740	Information technology – Open Systems Interconnection – Systems Management: Security audit trail function	Defines the security audit trail function. The security audit trail function is a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information and commands for the purpose of systems management. This function is positioned in the application layer.	SG4
X.741	Information technology – Open Systems Interconnection – Systems Management: Objects and attributes for access control	Defines specifications applicable to the provision of access control for applications that use OSI management services and protocols. The access control information identified by this Recommendation may be used in support of access control schemes based on access control lists, capabilities, security labels, and contextual constraints.	SG4
X.790	Trouble management function for ITU-T applications	Is concerned with the management of malfunction in systems and communications networks from the perspective of a provider of service and user of that service. Malfunction, referred to as "trouble" is a problem that has an adverse effect on the quality of service perceived by network users. When a trouble is detected, possibly as a result of an alarm report, a trouble report may be entered by a user or the system may raise a report automatically. Management of that trouble report is necessary to ensure that it receives attention and that the trouble is cleared to restore the service to its previous level of capability. A report format is defined to allow a user to report a trouble, which will then be progressed to resolution by a provider. During the resolution by the service provider, the service user may determine the current state of resolution by issuing a request for this information. When cleared the provider may notify the user. Particular types of troubles are included; however, the use of this Recommendation by a particular application may require trouble types specific to that application to be used – this is catered for. At the time of a trouble, a network may have been interworking with another network to provide a service, and the problem or malfunction may be due to the other network. Therefore it may be necessary to exchange trouble management information between management systems across interfaces which may be client to service provider or service provider to service provider interfaces and may represent inter-jurisdictional as well as intra-jurisdictional boundaries. In addition to exchanging information on trouble that has already been detected, advance information on service inaccessibility may also need to be exchanged. Thus, a service provider may need to inform a customer of future service inaccessibility (because of planned maintenance, for example). The scope includes all of the above processes for exchange of management information.	SG4
X.800	Security architecture for Open Systems Interconnection for CCITT applications	Defines the general security-related architectural elements which can be applied appropriately in the circumstances for which protection of communication between open systems is required. It establishes, within the framework of the Reference Model, guidelines and constraints to improve existing Recommendations or to develop new Recommendations in the context of OSI in order to allow secure communications and thus provide a consistent approach to security in OSI. This Recommendation extends the Reference Model to cover security aspects which are general architectural elements of communications protocols, but not discussed in the Reference Model. This Recommendation provides a general description of security services and related mechanisms, which may be provided by the Reference Model; and defines the positions within the Reference Model where the services and mechanisms may be provided.	SG17

X.802	Information technology – Lower layers security model	Describes the cross layer aspects of the revision of security services in the lower layers of the OSI Reference Model (Transport, Network, Data Link, Physical). It describes the architectural concepts common to these layers, the basis for interactions relating to security between layers and the placement of security protocols in the lower layers.	SG17
X.803	Information technology - Open Systems Interconnection - Upper layers security model	Describes the selection, placement and use of security services and mechanisms in the upper layers (applications, presentation and session layers) of the OSI Reference Model.	SG17
X.805	Security architecture for systems providing end-to-end communications	Defines the general security-related architectural elements that when appropriately applied, in particular in a multi-vendor environment, can ensure that a network is properly protected against malicious and inadvertent attacks, and operates with provision for performance parameters such as a high availability, appropriate response time, integrity, scalability, and accurate billing function.	SG17
X.810	Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview	Defines the framework within which security services for open systems are specified. This part of the Security Frameworks describes the organization of the <i>security framework</i> , defines <i>security concepts</i> , which are required in more than one part of the security framework, and describes the interrelationship of the services and mechanisms identified in other parts of the framework. This framework describes all aspects of <i>authentication</i> as these apply to Open Systems, the relationship of authentication with other security functions such as <i>access control</i> and the management requirements for authentication.	SG17
X.811	Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework	Defines a general framework for the provision of authentication. The primary goal of authentication is <i>to counter the threats of masquerade and replay</i> .	SG17
X.812	Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework	Defines a general framework for the provision of access control. The primary goal of access control is <i>to counter the threat of unauthorized operations</i> involving a computer or communications system; these threats are frequently subdivided into classes known as <i>unauthorized use, disclosure, modification, destruction and denial of service</i> .	SG17
X.813	Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework	Defines a general framework for the provision of non-repudiation services. The goal of the non-repudiation service is <i>to collect, maintain, make available, and validate irrefutable evidence regarding identification of originators and recipients involved in data transfers</i> .	SG17

X.814	Information technology - Open Systems Interconnection - Security frameworks for open systems: Confidentiality framework	Defines a general framework for the provision of confidentiality services. Confidentiality is the property that <i>information is not made available or disclosed</i> to unauthorized individuals, entities or processes.	SG17
X.815	Information technology - Open Systems Interconnection - Security frameworks for open systems: Integrity framework	Defines a general framework for the provision of integrity services. The property that <i>data has not been altered or destroyed</i> in an unauthorized manner is called integrity.	SG17
X.816	Information technology - Open Systems Interconnection - Security frameworks for open systems: Security audit and alarms framework	Describes a basic model for handling security alarms and for conducting a security audit for open systems. A security audit is <i>an independent review and examination of system records and activities</i> . The security audit service provides an audit authority with the ability to specify, select and manage the events, which need to be recorded within a security audit trail.	SG17
X.830	Information technology - Open Systems Interconnection - Generic upper layers security: Overview, models and notation	Belongs to a series of Recommendations, which provide a set of facilities to aid the construction of OSI Upper Layer protocols, which support the provision of security services. It defines the following: a) general <i>models of security exchange protocol functions and security transformations</i> ; b) a set of <i>notational tools</i> to support the specification of selective field protection requirements in an abstract syntax specification, and to support the specification of security exchanges and security transformations; c) a set of <i>informative guidelines</i> as to the application of the generic upper layer security facilities covered by this series of Recommendations.	SG17
X.831	Information technology - Open Systems Interconnection - Generic upper layers security: Security Exchange Service Element (SESE) service definition	Belongs to a series of Recommendations, which provide a set of facilities to aid the construction of OSI Upper Layer protocols, which support the provision of security services. This Recommendation <i>defines the service</i> provided by the Security Exchange Service Element (SESE). The SESE is an application-service-element (ASE), which facilitates the communication of <i>security information</i> to support the provision of <i>security services</i> within the Application Layer of OSI.	SG17
X.832	Information technology - Open Systems Interconnection - Generic upper layers security: Security Exchange Service Element (SESE) protocol specification	Belongs to a series of Recommendations, which provide a set of facilities to aid the construction of OSI Upper Layer protocols, which support the provision of security services. This Recommendation <i>specifies the protocol</i> provided by the Security Exchange Service Element (SESE). The SESE is an application-service-element (ASE), which facilitates the communication of <i>security information</i> to support the provision of <i>security services</i> within the Application Layer of OSI.	SG17

X.833	Information technology - Open Systems Interconnection - Generic upper layers security: Protecting transfer syntax specification	Belongs to a series of Recommendations, which provide a set of facilities to aid the construction of OSI Upper Layer protocols, which support the provision of security services. This Recommendation defines the protecting transfer syntax, associated with Presentation Layer support for <i>security services</i> in the Application Layer.	SG17
X.834	Information technology - Open Systems Interconnection - Generic upper layers security: Security Exchange Service Element (SESE) Protocol Implementation Conformance Statement (PICS) proforma	Belongs to a series of Recommendations on Generic Upper Layers Security (GULS). It is the Protocol Implementation Conformance Statement (PICS) proforma for the Security Exchange Service Element Protocol specified in ITU-T Rec. X.832 and the Security Exchange described in ITU-T Rec. X.830. Annex C. provides a description of the standardized capabilities and options in a form that supports conformance evaluation of a particular implementation.	SG17
X.835	Information technology – Open Systems Interconnection – Generic upper layers security: Protecting transfer syntax PICS proforma	Belongs to a series of Recommendations on Generic Upper Layers Security (GULS). It is the Protocol Implementation Conformance Statement (PICS) proforma for the Protecting transfer syntax Protocol specified in ITU-T Rec. X.833. This Recommendation provides a description of the standardized capabilities and options in a form that supports conformance evaluation of a particular implementation.	SG17
X.841	Information technology – Security techniques – Security Information Objects for access control	Provides object definitions that are commonly needed in <i>security standards</i> to avoid multiple and different definitions of the same functionality. Precision in these definitions is achieved by use of the Abstract Syntax Notation One (ASN.1). This Rec. covers only static aspects of Security Information Objects (SIOs).	SG17
X.842	Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services	Provides guidance for the use and management of Trusted Third Party (TTP) services, a clear definition of the basic duties and services provided, their description and their purpose, and the roles and liabilities of TTPs and entities using their services. This Rec. identifies different major categories of TTP services including <i>time stamping, non-repudiation, key management, certificate management, and electronic notary public</i> .	SG17
X.843	Information technology – Security techniques – Specification of TTP services to support the application of digital signatures	Defines the services required to support the application of digital signatures for <i>non-repudiation</i> of creation of a document. Since this implies <i>integrity</i> of the document and <i>authenticity</i> of the creator, the services described can also be combined to implement <i>integrity and authenticity services</i> .	SG17

X.901	Information technology – Open distributed processing – Reference Model: Overview	The rapid growth of distributed processing has led to a need for a coordinating framework for the standardization of Open Distributed Processing (ODP). This Reference Model provides such a framework and creates an architecture to support distribution, interworking and integrated portability. This Rec. contains a motivational overview of ODP giving scoping, justification and explanation of key concepts, and an outline of the ODP architecture. It contains explanatory material on how this Reference Model is to be interpreted and applied by its users, standards writers and architects of ODP systems. It also contains a categorization of required areas of standardization expressed in terms of the reference points for conformance identified in Rec. X.903. ODP systems have to be secure, i.e. must be built and maintained in a manner which ensures that system facilities and data are <i>protected against unauthorized access, unlawful use and any other threats or attacks</i> . Security requirements are difficult to meet by remoteness of interactions, and mobility of the system and of the system users. The security rules for ODP systems may define: the <i>detection of security threats; the protection against security threats; the limiting any damage caused by any security breaches</i> .	SG17
X.902	Information technology – Open distributed processing – Reference Model: Foundations	Contains the definition of the concepts and analytical framework for normalized description of (arbitrary) distributed processing systems. It introduces the principles of conformance to ODP standards and the way in which they are applied. This is only to a level of detail sufficient to <i>establish requirements for new specification techniques</i> .	SG17
X.903	Information technology – Open distributed processing – Reference Model: Architecture	Contains the specification of the required characteristics that qualify distributed processing as open. These are the constraints to which ODP standards must conform. It uses the descriptive techniques from Recommendation X.902	SG17
X.904	Information technology – Open distributed processing – Reference Model: Architectural semantics.	Contains a normalization of the ODP modelling concepts defined in Rec. X.902, clauses 8 and 9. The normalization is achieved by interpreting each concept in terms of the constructs of the different standardized formal description techniques.	SG17
X.1081	The telebiometric multimodal model – A framework for the specification of security and safety Aspects of telebiometrics	Defines a Telebiometric Multimodal Model that provides a common framework for the specification of four inter-connected security issues: Privacy, Authentication, Safety and Security. This Telebiometric Multimodal Model covers all the possibilities for safe and secure multimodal man-machine interactions, and is derived in part from ISO 31 and IEC 60027-1 standards. The cognitive, perceptual and behavioral modalities of a human being are also relevant in the field of telecommunication, and are likely to be used by a biometric sensor or effector in the future, for authentication purposes. These are also covered by the Telebiometric Multimodal Model. Taxonomy is presented of the interactions that occur at the multimodal layer where the human body interacts electronic, photonic, chemical or material devices capturing biometric parameters or impacting that body. Authentication of a human being, with preservation of his privacy and safety, can be specified in terms of interactions between devices and the Personal Privacy Sphere, which models and encapsulates the interactions of a human being with its environment, making discussion of such interactions explicit and engineerable. This Recommendation includes specification of the Personal Privacy Sphere, categorization of modalities of interaction across that sphere, base and derived units for measuring and specifying (in a quantitative manner) such interactions, and a scale hierarchy for relative propinquity.	SG17

X.1121	Framework of secure technologies for mobile end-to-end data communication	Describes security threats on mobile end-to-end data communication and security requirements for mobile user and application service provider (ASP) in the upper layer of the OSI Reference Model for mobile end-to-end data communications between a mobile terminal in mobile network and an application server in an open network. In addition, it shows where the security technologies realizing certain security function appear in the mobile end-to-end data communication model. It provides a framework of security technologies for mobile end-to-end data communications.	SG17
X.1122	Guideline for implementing secure mobile systems based on PKI	PKI technology is a security technology that is applied to the relation between mobile terminal and application sever in general model of mobile end-to-end data communication between mobile user and ASP or to the relation between mobile terminal and mobile security gateway and between mobile security gateway and server in gateway model of mobile end-to-end data communication between mobile user and ASP. Although PKI technology is a very useful technology for protecting mobile end-to-end data communications, there are characteristics specific to mobile data communications that require the PKI technology to be adapted when constructing secure mobile systems (encipherment, digital signature, data integrity, and so on). As methods to construct and manage secure mobile systems based on PKI technology has not been established this recommendation shows a guideline to construct secure mobile systems based on PKI technology.	SG17

Annex B

Security Terminology

The following ITU-T security-related definitions and abbreviations have been extracted from relevant ITU-T Recommendations.

The ITU-T online SANCHO (*Sector Abbreviations and defiNitions for a teleCommunications tHesaurus Oriented*) database provides access to English, French and Spanish "terms and definitions" or "abbreviations and acronyms" defined within ITU-T publications. This is a free online resource that can be accessed at www.itu.int/sancho. A CD-ROM version is also published regularly. All the terms and definitions above can be found in SANCHO with a list of Recommendations where the term or definition is used.

ITU-T SG 17 has developed a compendium of Security Definitions used in ITU-T Recommendations, which can be found at www.itu.int/ITU-T/studygroups/com17/cssecurity.html.

B.1 List of security-related terms and definitions

The following list comprises the more commonly used security terms that are defined in current ITU-T Recommendations. A more complete list of security definitions is in the compendium maintained by Study Group 17 (see link above).

Term	Definition	Reference
access control	<ol style="list-style-type: none"> 1. The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner 2. Limiting the flow of information from the resources of a system only to authorized persons, programs, processes or other system resources on a network. 	X.800 J.170
access control list	A list of entities, together with their access rights, which are authorized to have access to a resource.	X.800
access control policy	The set of rules that define the conditions under which an access may take place.	X.812
access control service	The access control service provides means to ensure that resources are accessed by subjects only in an authorized manner. Resources concerned may be the physical system, the system software, applications and data. The access control service can be defined and implemented at different levels of granularity in the TMN: at agent level, object level or attribute level. The limitations of access are laid out in access control information: the means to determine which entities are authorized to have access; what kind of access is allowed (reading, writing, modifying, creating, deleting).	M.3016
accidental threats	Threats that exist with no premeditated intent. Examples of realized accidental threats include system malfunctions, operational blunders and software bugs.	X.800
accountability	The property that ensures that the actions of an entity may be traced uniquely to the entity.	X.800
active threat	The threat of a deliberate unauthorized alteration of information contained in the system, or change to the state of the system. <i>Note</i> - Examples of security-relevant active threats may be: modification of messages, replay of messages, insertion of spurious messages, masquerading as an authorized entity, denial of service, malicious change to the routing tables of a system by an unauthorized user.	X.800
adjudicator	Entity who arbitrates disputes that may arise as a result of repudiated events or actions i.e. who evaluates the evidence and determines whether or not the disputed action or event occurred. <i>Adjudication</i> can only be provided effectively if the parties to the dispute accept the <i>authority</i> of the adjudicator	X.813
algorithm	A mathematical process which can be used for the scrambling and descrambling of a data stream.	J.93
asymmetric authentication method	A method of authentication, in which not all authentication information is shared by both entities.	X.811
asymmetric cryptographic algorithm	An algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ. <i>Note</i> - With some asymmetric cryptographic algorithms, decipherment of ciphertext or the generation of a digital signature requires the use of more than one private key.	X.810
attack	The activities undertaken to bypass or exploit deficiencies in a system's security mechanisms. By a direct attack on a system they exploit deficiencies in the underlying algorithms, principles, or properties of a security mechanism. Indirect attacks are performed when they bypass the mechanism, or when they make the system use the mechanism incorrectly.	H.235

Term	Definition	Reference
attribute	In the context of message handling, an information item, a component of an attribute list, that describes a user or distribution list and that can also locate it in relation to the physical or organizational structure of message handling system (or the network underlying it).	X.400
Attribute Authority	1. An authority which assigns privileges by issuing attribute certificates. 2. An entity trusted by one or more entities to create and sign attribute certificates. <i>Note</i> - a CA may also be an AA	X.509 X.842
attribute certificate	A data structure, digitally signed by an Attribute Authority, that binds some attribute values with identification information about its holder.	X.509
attribute type	An identifier that denotes a class of information (e.g. personal names). It is a part of an attribute.	X.400
attribute value	An instance of the class of information an attribute type denotes (e.g. a particular personal name). It is a part of an attribute.	X.400
audit	See security audit	X.800
audit trail	See security audit trail.	X.800
authenticated identity	A distinguishing identifier of a principal that has been assured through authentication.	X.811
authentication	1. The process of corroborating an identity. <i>Note</i> -- See principal and verifier and the two distinguished form of authentication (data origin auth. + entity auth.). Authentication can be unilateral or mutual. <i>Unilateral</i> authentication provides assurance of the identity of only one principal. <i>Mutual</i> authentication provides assurance of the identities of both principals. 2. The provision of assurance of the claimed identity of an entity. 3. See data origin authentication, and peer entity authentication. The term "authentication" is not used in connection with data integrity; the term "data integrity" is used instead. 4. The corroboration of the identity of objects relevant to the establishment of an association. For example, these can include the AEs, APs, and the human users of applications. NOTE – This term has been defined to make it clear that a wider scope of authentication is being addressed than is covered by peer-entity authentication in CCITT Rec. X.800. 5. The process of verifying the claimed identity of an entity to another entity. 6. The process intended to allow the system to check with certainty the identification of a party.	X.811 X.811 X.800 X.217 J.170 J.93
authentication certificate	A security certificate that is guaranteed by an authentication authority and that may be used to assure the identity of an entity.	X.811
authentication exchange	1. A mechanism intended to ensure the identity of an entity by means of information exchange. 2. A sequence of one or more transfers of exchange authentication information for the purposes of performing an authentication	X.800 X.811
authentication service	The authentication service delivers proof that the identity of an object or subject has indeed the identity it claims to have. Depending on the type of actor and on the purpose of identification, the following kinds of authentication may be required: user authentication, peer entity authentication, data origin authentication. Examples of mechanisms used to implement the authentication service are passwords and Personal Identification Numbers (PINs) (simple authentication) and cryptographic-based methods (strong authentication).	M.3016
authentication token (token)	Information conveyed during a strong authentication exchange, which can be used to authenticate its sender.	X.509

Term	Definition	Reference
authenticity	<ol style="list-style-type: none"> 1. The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity who claims to have given the information. 2. The property that the claimed data source can be verified to the satisfaction of the recipient. 	J.170 T.411
authority	An entity, responsible for the issuance of certificates. Two types are defined; certification authority which issues public-key certificates and attribute authority which issues attribute certificates.	X.509
authority certificate	A certificate issued to an authority (e.g. either to a certification authority or to an attribute authority).	X.509
authorization	<ol style="list-style-type: none"> 1. The granting of rights, which includes the granting of access based on access rights. <i>Note:</i> this definition implies the rights to perform some activity (such as to access data); and that they have been granted to some process, entity, or human agent. 2. The granting of permission on the basis of authenticated identification. 3. The act of giving access to a service or device if one has the permission to have the access. 	X.800 H.235 J.170
availability	The property of being accessible and useable upon demand by an authorized entity.	X.800
cable security portal (CSP)	A functional element that provides security management and translation functions between the HFC and the Home.	J.191
call management server (CMS)	IPCablecom. Controls the audio connections. Also called a Call Agent in MGCP/SGCP terminology.	J.191
capability	A token used as an identifier for a resource such that possession of the token confers access rights for the resource.	X.800
certificate	A set of security-relevant data issued by a security authority or trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data (<i>security certificate</i> -- X.810). The term refers to " <i>public key</i> " certificates which are values that represent an owners public key (and other optional information) as verified and signed by a trusted authority in an unforgeable format.	H.235
certificate policy	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.	X.509
Certificate Revocation List (CRL)	<ol style="list-style-type: none"> 1. A signed list indicating a set of certificates that are no longer considered valid by the certificate issuer. In addition to the generic term CRL, some specific CRL types are defined for CRLs that cover particular scopes. 2. A CRL includes the serial numbers of certificates that have been revoked (for example, because the key has been compromised or because the subject is no longer with the company) and whose validity period has not yet expired. 	X.509 Q.817
Certification Authority (CA)	<ol style="list-style-type: none"> 1. An authority trusted by one or more users to create and assign public-key certificates. Optionally the certification authority may create the users' keys. 2. An entity that is trusted (in the context of a security policy) to create security certificates containing one or more classes of security-relevant data. 	X.509 X.810
certification path	An ordered sequence of certificates of objects in the Directory Information Tree which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.	X.509
challenge	A time variant parameter generated by a verifier.	X.811
cipher	<ol style="list-style-type: none"> 1. A cryptographic algorithm, a mathematical transform. 2. An algorithm that transforms data between plaintext and ciphertext. 	H.235 J.170

Term	Definition	Reference
ciphertext	Data produced through the use of encipherment. The semantic content of the resulting data is not available. <i>Note</i> - Ciphertext may itself be input to encipherment, such that super-enciphered output is produced.	X.800
claimant	An entity which is or represents a <i>principal</i> for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.	X.811
cleartext	Intelligible data, the semantic content of which is available.	X.800
compromised evidence	Evidence that was, at one time, satisfactory but which no longer has the confidence of the Trusted Third Party or adjudicator.	X.813
confidentiality	1. The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.	X.800
confidentiality service	The confidentiality service provides protection against unauthorized disclosure of exchanged data. The following kinds of confidentiality services are distinguished: selective field confidentiality; connection confidentiality; data flow confidentiality.	M.3016
content integrity	1. Enables the recipient to verify that the original content of a message has not been modified. 2. This element of service allows the originator of the message to provide to the recipient of the message a means by which the recipient can verify that the content of the message has not been modified. Content Integrity is on a per-recipient basis, and can use either an asymmetric or a symmetric encryption technique.	X.400 X.400
counter-signature	Digital signature appended to a data unit which has already been signed by a different entity (e.g., a TTP).	X.813
credentials	Data that is transferred to establish the claimed identity of an entity	X.800
cryptanalysis	1. analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext. 2. The process of recovering the plaintext of a message or the encryption key without access to the key. 3. The science of recovering the plaintext of a message without access to the key (to the electronic key in electronic cryptographic systems).	X.800 J.170 J.93
cryptographic algorithm	Mathematical function that computes a result from one or several input values.	H.235
cryptographic chaining	A mode of use of a cryptographic algorithm in which the transformation performed by the algorithm depends on the values of previous inputs or outputs.	X.810
cryptographic checkvalue	Information which is derived by performing a cryptographic transformation (see cryptography) on the data unit. <i>Note</i> - The derivation of the checkvalue may be performed in one or more steps and is a result of a mathematical function of the key and a data unit. It is usually used to check the integrity of a data unit.	X.800
cryptographic system, cryptosystem	1. A collection of transformations from plain text into ciphertext and vice versa, the particular transformation(s) to be used being selected by keys. The transformations are normally defined by a mathematical algorithm. 2. A cryptosystem is simply an algorithm that can convert input data into something unrecognizable (encryption), and convert the unrecognizable data back to its original form (decryption). RSA encryption techniques are described in X.509.	X.509 Q.815
cryptography	The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. <i>Note</i> – Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or method is cryptanalysis.	X.800

Term	Definition	Reference
data confidentiality	This service can be used to provide for protection of data from unauthorized disclosure. The data confidentiality service is supported by the authentication framework. It can be used to protect against data interception.	X.509
data integrity	The property that data has not been altered or destroyed in an unauthorized manner.	X.800
data origin authentication	<ol style="list-style-type: none"> 1. The corroboration that the source of data received is as claimed. 2. The corroboration of the identity of the principal that is responsible for a specific data unit. 	X.800 X.811
decipherment	The reversal of a corresponding reversible encipherment.	X.800
decryption	See decipherment.	X.800
delegation	Conveyance of privilege from one entity that holds such privilege, to another entity.	X.509
denial of service	The prevention of authorized access to resources or the delaying of time-critical operations.	X.800
descrambling	<ol style="list-style-type: none"> 1. The restoration of the characteristics of a vision/sound/data signal in order to allow reception in a clear form. This restoration is a specified process under the control of the conditional access system (receiving end). 2. The process of reversing the scrambling function (see "scrambling") to yield usable pictures, sound, and data services 	J.96 J.93
digital fingerprint	A characteristic of a data item, such as a cryptographic checkvalue or the result of performing a one-way hash function on the data, that is sufficiently peculiar to the data item that it is computationally infeasible to find another data item that will possess the same characteristics.	X.810
digital signature	<ol style="list-style-type: none"> 1. Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. 2. A cryptographic transformation of a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties, and the sender against forgery by the recipient. 	X.800 X.843
direct attack	An attack on a system based on deficiencies in the underlying algorithms, principles, or properties of a security mechanism.	X.814
directory service	A service to search and retrieve information from a catalogue of well defined objects, which may contain information about certificates, telephone numbers, access conditions, addresses etc. An example is provided by a directory service conforming to the X.500.	X.843
double enveloping technique	Additional protection may be provided to a complete message, including the envelope parameters, by the ability to specify that the content of a message is itself a complete message, i.e., a double enveloping technique is available though the use of the Content Type argument which makes it possible to specify that the content of a message is an inner envelope.	X.402
eavesdropping	A breach of confidentiality by monitoring communication.	M.3016
electronic key	The term for data signals which are used to control the descrambling process in subscriber decoders. NOTE – There are at least three types of electronic keys: those used for television signal streams, those used for protecting control system operations, and those used for the distribution of electronic keys on the cable system.	J.93
encipherment	<ol style="list-style-type: none"> 1. The cryptographic transformation of data (see cryptography) to produce ciphertext. <i>Note</i> - Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed. 2. Encipherment (encryption) is the process of making data unreadable to unauthorized entities by applying a cryptographic algorithm (an encryption algorithm). Decipherment (decryption) is the reverse operation by which the ciphertext is transformed to the plaintext. 	X.800 H.235

Term	Definition	Reference
encryption	1. A method used to translate information in plaintext into ciphertext. 2. The process of scrambling signals to avoid unauthorized access. (See also encipherment)	J.170 J.93
end entity	A certificate subject that uses its private key for purposes other than signing certificates or an entity that is a relying party.	X.509
end-to-end encipherment	Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system. (See also link-by-link encipherment.)	X.800
entity	1. A human being, an organization, a hardware component or a piece of software. 2. Any concrete or abstract thing of interest. While in general the word entity can be used to refer to anything, in the context of modelling it is reserved to refer to things in the universe of discourse being modelled.	X.842 X.902
entity authentication	Corroboration of the identity of a principal, within the context of a communication relationship. <i>Note</i> -- The principal's authenticated identity is assured only when this service is invoked. Assurance of continuity of authentication can be obtained by methods described in §.5.2.7/ X.811	X.811
event discriminator	A function which provides initial analysis of a security-related event and, if appropriate, generates a security audit and/or an alarm.	X.816
evidence	Information that, either by itself or when used in conjunction with other information, may be used to resolve a dispute. <i>Note</i> - Particular forms of evidence are digital signatures, secure envelopes and security tokens. Digital signatures are used with <i>public</i> key techniques while secure envelopes and security tokens are used with <i>secret</i> key techniques.	X.813
evidence generator	An entity that produces non-repudiation evidence. <i>Note</i> - This entity may be the non-repudiation service requester, the originator, the recipient or multiple parties working in conjunction (e.g. a signer and co-signer).	X.813
forgery	An entity fabricates information and claims that such information was received from another entity or sent to another entity	M.3016
hash function	A (mathematical) function that maps values from a (possibly very) large set of values into a smaller range of values	X.810
hide	An operation that applies confidentiality protection to unprotected data or additional confidentiality protection to already protected data.	X.814
identity-based security policy	A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed.	X.800
indirect attack	An attack on a system which is not based on the deficiencies of a particular security mechanism (e.g. attacks which bypass the mechanism, or attacks which depend on the system using the mechanism incorrectly).	X.814
integrity	1. The property that data has not been altered in an unauthorized manner. (See also data integrity)	H.235
integrity service	The integrity service provides means to ensure the correctness of exchanged data, protecting against modification, deletion, creation (insertion) and replay of exchanged data. The following kinds of integrity services are distinguished: selective field integrity; connection integrity without recovery; connection integrity with recovery.	M.3016
integrity-protected channel	A communications channel to which an integrity service has been applied. (See connection integrity and connectionless integrity.)	X.815
integrity-protected data	Data and all relevant attributes within an integrity-protected environment.	X.815

Term	Definition	Reference
integrity-protected environment	An environment in which unauthorized data alterations (including creation and deletion) are prevented or detectable.	X.815
intentional threats	Threats that may range from casual examination using easily available monitoring tools to sophisticated attacks using special system knowledge. An intentional threat, if realized, may be considered to be an "attack".	X.800
intrusion resistance	The ability of a hardware object to deny physical, electrical, or irradiation-based access to internal functionality by unauthorized parties.	J.93
IPCablecom	An ITU-T project that includes an architecture and a series of Recommendations that enable the delivery of real-time services over the cable television networks using cable modems.	J.160
Kerberos	A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.	J.170
key	<ol style="list-style-type: none"> 1. A sequence of symbols that controls the operations of encipherment and decipherment. 2. A mathematical value input into the selected cryptographic algorithm. 	X.800 J.170
key distribution service	The service of distributing keys securely to authorized entities performed by a key distribution center and described in ISO/IEC 11770-1.	X.843
key exchange	The swapping of public keys between entities to be used to encrypt communication between the entities.	J.170
key management	The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.	X.800
leakage of information	When information was acquired by an unauthorized party by monitoring transmissions, by unauthorized access to information stored in any MHS entity, or by masquerade, that might result from impersonation and misuse of the MTS or through causing an MTA to operate incorrectly. Leakage of information threats include the following: loss of confidentiality; loss of anonymity; misappropriation of messages; traffic analysis.	X.402
link-by-link encipherment	The individual application of encipherment to data on each link of a communications system. (See also end-to-end encipherment.) <i>Note</i> - The implication of link-by-link encipherment is that data will be in cleartext form in relay entities.	X.800
loss or corruption of information	The integrity of data transferred is compromised by unauthorized deletion, insertion, modification, re-ordering, replay or delay	M.3016
manipulation detection	A mechanism which is used to detect whether a data unit has been modified (either accidentally or intentionally).	X.800
masquerade	The pretence by an entity to be a different entity.	X.800
message authentication code (MAC)	A cryptographic checkvalue that is used to provide data origin authentication and data integrity.	X.813
message origin authentication	Enables the recipient, or any MTA through which the message passes, to authenticate the identity of the originator of a message.	X.400
message sequence integrity	<ol style="list-style-type: none"> 1. Allows the originator to provide to a recipient proof that the sequence of messages has been preserved. 2. This element of service allows the originator of the message to provide to a recipient of the message a means by which the recipient can verify that the sequence of messages from the originator to the recipient has been preserved (without message loss, re-ordering, or replay). Message Sequence Integrity is on a per-recipient basis, and can use either an asymmetric or a symmetric encryption technique. 	X.400

Term	Definition	Reference
message sequencing	When part or all of a message is repeated, time-shifted, or reordered, e.g. to exploit the authentication information in a valid message and resequence or time-shift valid messages. Although it is impossible to prevent replay with the MHS security services, it can be detected and the effects of the threat eliminated. Message sequencing include: replay of messages; reordering of messages; pre-play of messages; delay of messages.	X.402
monitoring role	The role, in which a TTP monitors the action or the event and is trusted to provide evidence about what was monitored.	X.813
mutual authentication	The assurance of the identities of both principals.	X.811
non-repudiation	<ol style="list-style-type: none"> 1. The ability to prevent a sender from denying later that he or she sent a message or performed an action. 2. Protection from denial by one of the entities involved in a communication of having participated in all or part of the communication. 3. A process by which the sender of a message (e.g. a request on a pay-per-view) cannot deny having sent the message 	J.170 H.235 J.93
notarization	The registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery.	X.800
notary	A Trusted Third Party with whom data is registered so that later assurance of the accuracy of the characteristics of the data can be provided.	X.813
passive threat	The threat of unauthorized disclosure of information without changing the state of the system.	X.800
password	<ol style="list-style-type: none"> 1. Confidential authentication information, usually composed of a string of characters. 2. Referring to a user-entered password string: is understood to be the assigned security key, which the mobile user shares with his home domain. This user password and derived user shared secret shall be applied for the purpose of user authentication. 	X.800 H.530
peer-entity authentication	<ol style="list-style-type: none"> 1. The corroboration that a peer entity in an association is the one claimed. 2. Establishing the proof of the identity of the peer entity during a communication relationship. 	X.800 M.3016
personal security environment (PSE)	Secure local storage for an entity's private key, the directly trusted CA key and possibly other data. Depending on the security policy of the entity or the system requirements this may be e.g.; a cryptographically protected file or a tamper resistant hardware token.	X.843
physical security	The measures used to provide physical protection of resources against deliberate and accidental threats.	X.800
principal	<ol style="list-style-type: none"> 1. An entity whose identity can be authenticated. 	X.811
privacy	<ol style="list-style-type: none"> 1. The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. <i>Note</i> - Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security. 2. A mode of communication in which only the explicitly enabled parties can interpret the communication. This is typically achieved by encryption and shared key(s) for the cipher. 	X.800 H.235
private key; secret key (deprecated)	<ol style="list-style-type: none"> 1. (In a public key cryptosystem) that key of a user's key pair which is known only by that user. 2. A key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity). 3. The key used in public key cryptography that belongs to an individual entity and must be kept secret. 	X.509 X.810 J.170
privilege	An attribute or property assigned to an entity by an authority.	X.509

Term	Definition	Reference
Privilege Management Infrastructure (PMI)	The infrastructure able to support the management of privileges in support of a comprehensive authorization service and in relationship with a Public Key Infrastructure.	X.509
public key	<ol style="list-style-type: none"> 1. (In a public key cryptosystem) that key of a user's key pair which is publicly known. 2. A key that is used with an asymmetric cryptographic algorithm and that can be made publicly available. 3. The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key. 	X.509 X.810 J.170
public key certificate	<ol style="list-style-type: none"> 1. The public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it. 2. values that represent an owners public key (and other optional information) as verified and signed by a trusted authority in an unforgeable format. 3. A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate. 	X.509 H.235 J.170
Public Key Cryptography	A cryptographic technique based upon a two-key algorithm, private and public, wherein a message is encrypted with the public key but can only be decrypted with the private key. Also known as a Private-Public Key (PPK) system. NOTE – Knowing the public key does not reveal the private key. Example: Party A would devise such a private and public key, and send the public key openly to all who might wish to communicate with Party A, but retain the private key in secret. Then, while any who have the public key can encrypt a message for Party A, only Party A with the private key can decrypt the messages.	J.93
Public Key Infrastructure (PKI)	The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.	X.509
Registration Authority (RA)	<ol style="list-style-type: none"> 1. An entity who is responsible for identification and authentication of subjects of certificates, but is not a CA or an AA, and hence does not sign or issue certificates. <i>Note</i> - an RA may assist in the certificate application process, revocation process, or both. 2. Authority entitled and trusted to perform the registration service. 	X.842 X.843
relay attack	An attack on authentication in which exchange AI is intercepted and then immediately forwarded.	X.811
relying party	A user or agent that relies on the data in a certificate in making decisions.	X.509
replay	A message, or part of a message, is repeated to produce unauthorized effect. For example, a valid message containing authentication information may be replayed by another entity in order to authenticate itself (as something that it is not).	X.800
repudiation	<ol style="list-style-type: none"> 1. Denial by one of the entities involved in a communication of having participated in all or part of the communication. 2. An entity involved in a communication exchange subsequently denies the fact. 3. (In an MHS the case) when an MTS-user or the MTS may later deny submitting, receiving, or originating a message, and include: denial of origin, denial of submission, denial of delivery. 	X.800 M.3016 X.402
reveal	An operation that removes some or all of previously applied confidentiality protection.	X.814
revocation certificate	A security certificate issued by a security authority to indicate that a particular security certificate has been revoked.	X.810
revocation list certificate	A security certificate that identifies a list of security certificates that have been revoked.	X.810
routing control	The application of rules during the process of routing so as to chose or avoid specific networks, links or relays.	X.800

Term	Definition	Reference
rule-based security policy	A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.	X.800
seal	A cryptographic checkvalue that supports integrity but does not protect against forgery by the recipient (i.e., it does not provide non-repudiation). When a seal is associated with a data element, that data element is said to be <i>sealed</i> . <i>Note</i> - Although a seal does not by itself provide non-repudiation, some non-repudiation mechanisms make use of the integrity service provided by seals, e.g. to protect communications with trusted third parties.	X.810
secret key	A key that is used with a symmetric cryptographic algorithm. Possession of a secret key is restricted (usually to two entities).	X.810
security	The term " <i>security</i> " is used in the sense of minimizing the vulnerabilities of assets and resources. An <i>asset</i> is anything of value. A <i>vulnerability</i> is any weakness that could be exploited to violate a system or the information it contains. A <i>threat</i> is a potential violation of security.	X.800
security administrator	A person who is responsible for the definition or enforcement of one or more parts of a security policy.	X.810
security alarm	A message generated when a security-related event that is defined by security policy as being an alarm condition has been detected. A security alarm is intended to come to the attention of appropriate entities in a timely manner.	X.816
security association	A relationship between two or more entities for which there exist attributes (state information and rules) to govern the provision of security services involving those entities. The relationship between lower layer communicating entities for which there exists corresponding security association attributes.	X.803 X.802
security audit	An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.	X.800
security audit trail	Data collected and potentially used to facilitate a security audit.	X.800
security auditor	An individual or a process allowed to have access to the security audit trail and to build audit reports.	X.816
security authority	1. An entity that is responsible for the definition, implementation or enforcement of security policy. 2. The entity accountable for the administration of a security policy within a security domain. 3. The administrator responsible for the implementation of a security policy.	X.810 X.841 X.903
security certificate	A set of security-relevant data issued by a security authority or trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data. <i>Note</i> - All certificates are deemed to be security certificates. The term security certificate in the X.800 series is adopted in order to avoid terminology conflicts with X.509.	X.810
security domain	1. A collection of users and systems subject to a common security policy. 2. The set of resources subject to a single security policy.	X.841 X.411
security exchange	A transfer or sequence of transfers of application-protocol-control-information between open systems as part of the operation of one or more security mechanisms.	X.803
security information (SI)	Information needed to implement security services.	X.810

Term	Definition	Reference
security label	The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.	X.800
security management	Security management comprises all activities to establish, maintain and terminate the security aspects of a system. Topics covered are: management of security services; installation of security mechanisms; key management (management part); establishment of identities, keys, access control information, etc.; management of security audit trail and security alarms.	M.3016
security model	a framework for describing the security services that counter potential threats to the MTS and the security elements that support those services.	X.402
security policy	1. The set of rules laid down by the security authority governing the use and provision of security services and facilities. 2. The set of criteria for the provision of security services. <i>Note</i> - See identity-based and rule-based security policy. A complete security policy will necessarily address many concerns which are outside of the scope of OSI.	X.509 X.800
security rules	Local information which, given the security services selected specify the underlying security mechanisms to be employed, including all parameters needed for the operation of the mechanism. <i>Note</i> - Security rules are a form of secure interaction rules as defined in the Upper Layers Security Model	X.802
security service	A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.	X.800
security state	State information that is held in an open system and that is required for the provision of security services.	X.803
security token	A set of data protected by one or more security services, together with security information used in the provision of those security services, that is transferred between communicating entities.	X.810
security transformation	A set of functions (system security functions and security communication functions) which, in combination, operate upon user data items to protect those data items in a particular way during communication or storage.	X.803
selective field protection	The protection of specific fields within a message which is to be transmitted.	X.800
sensitivity	Characteristic of a resource that implies its value or importance.	X.509
shared secret	Refers to the security key for the cryptographic algorithms; it may be derived from a password.	H.530
shield	The conversion of data into integrity-protected data.	X.815
signature	See digital signature.	X.800
simple authentication	Authentication by means of simple password arrangements.	X.509
Source of Authority (SOA)	An Attribute Authority that a privilege verifier for a particular resource trusts as the ultimate authority to assign a set of privileges.	X.509
spamming	A denial-of-service attack when sending unauthorized data in excess to a system. A special case is media spamming when sending RTP packets on UDP ports. Usually the system is flooded with packets; the processing consumes precious system resources.	H.235
strong authentication	Authentication by means of cryptographically derived credentials.	X.509
symmetric authentication method	A method of authentication in which both entities share common authentication information.	X.811
symmetric cryptographic algorithm	An algorithm for performing encipherment or the corresponding algorithm for performing decipherment in which the same key is required for both encipherment and decipherment.	X.810

Term	Definition	Reference
threat	A potential violation of security.	X.800
time stamping service	A service which attests the existence of electronic data at a precise instant of time. <i>Note</i> -Time stamping services are useful and probably indispensable to support long term validation of signatures.	X.842
traffic analysis	The inference of information from observation of traffic flows (presence, absence, amount, direction and frequency).	X.800
traffic flow confidentiality	A confidentiality service to protect against traffic analysis, i.e. a security service to provide the protection of the information which might be derived from observation of traffic flows.	X.800
traffic padding	The generation of spurious instances of communication, spurious data units and/or spurious data within data units.	X.800
trapdoor	The result of an action, in which an entity of a system is altered to allow an attacker to produce an unauthorized effect on command or at a predetermined event or sequence of events. For example, a password validation could be modified so that, in addition to its normal effect, it also validates an attacker's password.	X.800
Trojan horse	When introduced to the system, the Trojan horse has an unauthorized function in addition to its authorized function. A relay that also copies messages to an unauthorized channel is a Trojan Horse.	X.800
trust	Entity X is said to <i>trust</i> entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.	X.810
trusted entity	An entity that can violate a security policy, either by performing actions which it is not supposed to do, or by failing to perform actions which it is supposed to do.	X.810
trusted functionality	Functionality perceived to be correct with respect to some criteria, e.g., as established by a security policy.	X.800
trusted third party (TTP)	A security authority or its agent that is trusted (by other entities) with respect to some security-relevant activities (in the context of a security policy).	X.810
unauthorized access	An entity attempts to access data in violation of the security policy in force	M.3016
unshield	The conversion of integrity protected data into the data originally shielded.	X.815
user authentication	Establishing proof of the identity of the human user or application process.	M.3016
validate	The checking of integrity-protected data to detect loss of integrity.	X.815
verifier	An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.	X.811
vulnerability	Any weakness that could be exploited to violate a system or the information it contains.	X.800
X.509 certificate	A public key certificate specification developed as part of the ITU-T X.500 standards directory.	J.170

B.2 Security-related Acronyms

Acronym	Definition
AA	[X.509] Attribute Authority
ACI	[SANCHO] Access Control Information
AE	[M.3010] Application entity
AES	[H.235] [J.170] Advanced Encryption Standard Algorithm
APS	[SANCHO] Automatic Protection Switching
ASN.1	[H.680] Abstract Syntax Notation One
ASON	[SANCHO] Automatically Switched Optical Network
ASP	[X.805] [X.1121] Application Service Provider
CA	[H.234] [H.235] [J.170] [X.509] Certification Authority. A trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates. [J.170] Call Agent. The part of the CMS that maintains the communication state, and controls the line side of the communication.
CME	[X.790] Conformant Management Entity
CMIP	[M.3010] Common management information protocol
CMS	[J.170] Cryptographic Message Syntax. [J.170] Call Management Server, that controls the audio connections. Also called a Call Agent in MGCP/SGCP terminology (this is one example of an Application Server).
CORBA	[SANCHO] Common Object Request Broker Architecture
COS	[SANCHO] Class of service
CP	Certificate Policy
CPS	[SANCHO: X.842] Certification Practice Statement [SANCHO: Q.817] Certification Policy Statement
CRL	[H.235] [X.509] Certificate Revocation List
DCN	[SANCHO] Data Communication Network
DES	[SANCHO] Data Encryption Standard, Digital Encryption Standard
DHCP	[SANCHO] Dynamic Host Configuration Protocol
DOCSIS	[SANCHO] Data-Over-Cable Service Interface Specification
DSA	[X.509] Directory System Agent [SANCHO] Digital Signature Algorithm
DSL	[SANCHO] Digital Subscriber Loop
DSP	[SANCHO] Digital Signal Processor [SANCHO] Directory Service Protocol
FDS	[SANCHO] Fraud Detection System
FEAL	[T.36] The Fast Data Encipherment Algorithm is a family of algorithms that maps 64 plaintext to 64-bit ciphertext blocks under a 64-bit secret key. It is similar to DES but with a far simpler f-function. It was designed for speed and simplicity, making it suitable for less complex microprocessors (e.g. smartcards). (in A. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997)
FIGS	[M.3210.1] Fraud Information Gathering System
GK	[H.235] [H.510] [H.530] Gatekeeper
GW	[H.235] Gateway
HFC	[SANCHO] Hybrid Fiber-Coaxial Cable
HFX	[T.30] [T.36] Hawthorne Facsimile Cipher
HKM	[T.30] [T.36] Hawthorne Key Management algorithm

Acronym	Definition
ICN	Information and Communication Network
ICT	Information and Communication Technology
ID	[H.235] Identifier
IDEA	[T.36] The International Data Encryption Algorithm is an encryption algorithm created by Xuejia Lai and James Massey in 1992 that uses a block cipher with a 128-bit key (64-bit blocks with a 128 bit key), and is generally considered to be very secure. It is considered among the best publicly known algorithms. In the several years that it has been in use, no practical attacks on it have been published despite of a number of attempts to find some (http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci213675,00.html).
IKE	[J.170] Internet Key Exchange is a key management mechanism used to negotiate and derive keys for SAs in IPsec.
IKE-	[J.170] A notation defined to refer to the use of IKE with pre-shared keys for authentication
IKE+	[J.170] A notation defined to refer to IKE requiring public-key certificates
IMT-2000	[M.3210.1] International Mobile Telecommunications 2000
IP	[X.805] Internet Protocol
IPsec	[H.235] [H.530] [J.170] [X.805] Internet Protocol Security.
IVR	[J.170] Interactive Voice Response System
LAN	[M.3010] Local Area Network
LDAP	[H.235] Lightweight Directory Access Protocol
LLA	[M.3010] Logical Layered Architecture
MAC	[H.235] [J.170] Message Authentication Code. A fixed-length data item that is sent together with a message to ensure integrity, also known as a MIC. [J.170] Media Access Control. It is a sub-layer of the Data Link Layer. It normally runs directly over the physical layer
MCU	[H.235] Multicast Unit. [H.323] Multipoint Control Unit
MD5	[H.235] [J.170] Message Digest No. 5
MG	[J.170] Media Gateway
MGC	[J.170] Media Gateway Controller
MGCP	[J.170] Media Gateway Control Protocol
MIB	[J.170] [M.3010] Management Information Base
MIS	[M.3010] Management Information System
MS	[M.3210.1] Management system Message Store Multiplex Section
MSP	[SANCHO] Multiplex Section Protection
MS-SPRing	Multiplex Section Shared Protection Ring
MTA	[J.170] Media Terminal Adapter Multimedia Terminal Adapter Message Transfer Agent
NAT	[H.235] Network Address Translation
OAM&P	[SANCHO] Operations, Administration, Maintenance & Provisioning
OS	[M.3010] [X.790] Operations System
OSF	[M.3010] Operations Systems Function
OSI	[SANCHO] Open Systems Interconnection
OSS	[J.170] Operational Support System. The back-office software used for configuration, performance, fault, accounting, and security management.
PDA	Personnal Data Assistant

Acronym	Definition
PKI	[H.235] [H.530] [X.509] [J.170] Public Key Infrastructure. A process for issuing public key certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing certification processes.
PKINIT	[J.160] Public Key Cryptography Initial Authentication [J.191] Public-Key Cryptography for Initial Authentication
PMI	[X.509] Privilege Management Infrastructure
QoS	[SANCHO] Quality of Service
RA	Registration Authority
RADIUS	[J.170] Remote Authentication Dial-In User Service
RAS	[SANCHO] Registration, Admission and Status [SANCHO] Registration, Admission and Status Protocol
RBAC	[X.509] Role-Based Access Control
RKS	[J.170] Record Keeping Server. The device which collects and correlates the various Event Messages.
RSA	[H.235] [T.30] [T.36] Rivest, Shamir and Adleman (public key algorithm)
RTP	[H.225.0] [H.235] [J.170] Real time protocol
SHA1	[H.235] Secure Hash Algorithm No.1
SG	Signalling Gateway
SIP	[J.170] [X.805] Session Initiation Protocol. An application-layer control (signalling) protocol for creating, modifying, and terminating sessions with one or more participants.
SNC	[SANCHO] Sub-Network Connection
SNMP	[J.170] [X.805] Simple Network Management Protocol
SoA	[X.509] Source of Authority
SRTP	[H.235] Secure Real-Time Transport Protocol
SS7	[J.170] [X.805] The Signalling System number 7 is an architecture and set of protocols for performing out-of-band call signalling with a telephone network.
SSL	[H.235] [X.805] Secure Socket Layer
TFTP	[SANCHO] Trivial File Transfer Protocol
TGS	[J.160] Ticket Granting Server
TLS	[H.235] Transport Level Security
TMN	[M.3010] [M.3210.1] [X.790] Telecommunications management network
TTP	[X.810] Trusted Third Party
UDP	[J.170] User Datagram Protocol.
VA	Validation Authority
VoIP	[X.805] Voice over IP
VPN	[X.805] Virtual Private Network

Annex C

List of Study Groups and Security-related Questions

The standardization work of ITU-T is carried out by Study Groups (SGs) in which representatives of the ITU-T membership develop Recommendations (standards) for the various fields of international telecommunications. The SGs drive their work in the form of study Questions. Each of these addresses technical studies in a particular area of telecommunication standardization. Below are ITU-T Study Groups for the 2001-2004 study period, their title and mandates, and the study Questions that address security work.

SG 2	Operational aspects of service provision, networks and performance <i>Lead Study Group on Service definition, Numbering, Routing and Global Mobility</i>
<p>Study Group 2 is responsible for studies relating to principles of service provision, definition and operational requirements of service emulation; numbering, naming, addressing requirements and resource assignment including criteria and procedures for reservation and assignment; routing and interworking requirements; human factors; operational aspects of networks and associated performance requirements including network traffic management, quality of service (traffic engineering, operational performance and service measurements); operational aspects of interworking between traditional telecommunication networks and evolving networks; evaluation of feedback from operators, manufacturing companies and users on different aspects of network operation.</p>	
<p>Main security-related Questions: - Q.5/2 – Service quality of networks</p>	
SG 3	Tariff and accounting principles including related telecommunications economic and policy issues
<p>Study Group 3 is responsible for studies relating to tariff and accounting principles for international telecommunication services and study of related telecommunication economic and policy issues. To this end, Study Group 3 shall in particular foster collaboration among its Members with a view to the establishment of rates at levels as low as possible consistent with an efficient service and taking into account the necessity for maintaining independent financial administration of telecommunication on a sound basis.</p>	
<p>Main security-related Questions: <i>None</i></p>	
SG 4	Telecommunication management, including TMN <i>Lead Study Group on TMN.</i>
<p>As the lead study group for management activities, Study Group 4 work on security addresses the following areas:</p> <ol style="list-style-type: none"> a) Architectural considerations and requirements for the management interfaces, b) Detailed requirements for securing the management network (also referred to as the management plane), specifically as the networks are becoming converged, c) Protocol and models to support securing management information and management of security parameters. 	
<p>Management of Telecommunications network is defined at different levels of abstractions, from managing network element level information to management services offered to the customer. The security requirements for the information exchanged between management systems and between management systems and network elements depend on whether the management networks are within one administration or between administrations. Based on the architectural principles, explicit requirements, mechanisms and protocol support have been defined in existing Recommendations and additional ones are under development.</p> <p>Q.18/4 along with Q7/4 is working on revising Recommendation M.3016 into a multipart series to provide detailed security requirements, services, and mechanisms. Other groups will define profiles using these Recommendations suited to the specific applications such as 3GPP and ETSI TISPAN.</p>	
<p>Main security-related Questions: - Q.18/4 – Protocols for Management Interfaces</p>	

SG 5	Protection against electromagnetic environment effects
<p>Study Group 5 is responsible for studies relating to protection of telecommunication networks and equipment from interference and lightning as well as for studies related to electromagnetic compatibility (EMC). In fulfilling its mission, SG 5 has worked on several Questions and developed a number of Recommendations and Handbooks that contribute to the security of the network against electromagnetic threats. Electromagnetic threats involve malicious man-made high power transient phenomena such as High-Altitude Electromagnetic Pulse (HEMP) and High-Power Microwave (HPM). Also, electromagnetic security could involve of information leaks from telecommunication networks by unexpected radio emission from equipment.</p> <p>The nature of the malicious threats and the corresponding mitigation techniques are similar to those that apply to natural or unintentional electromagnetic disturbances. Thus, the traditional activities of Study Group 5 related to protection against lightning and controlling Electromagnetic Interference (EMI) contribute to the security of the network against malicious man-made threats. There are presently six Questions allocated to Study Group 5 that have bearing on electromagnetic security of the telecommunication network. While there are many similarities between malicious man-made electromagnetic threats and the inadvertent or natural electromagnetic environment, there are certain significant differences. In fulfilling its mission, Study Group 5 has worked on several Questions and developed a number of Recommendations and Handbooks that contribute to the security of the network against electromagnetic threats.</p> <p>The two principal area of electromagnetic security are:</p> <ol style="list-style-type: none"> a) Resistibility and immunity of telecommunication networks and equipment against malicious man-made high power transient phenomena. Such threats include <ul style="list-style-type: none"> – Electromagnetic fields produced by nuclear detonations at high altitude — High-Altitude Electromagnetic Pulse (HEMP). – High-Power Electromagnetic (HPE) generators including High-Power Microwave (HPM) and Ultra-Wideband (UWB) sources. b) Possibility of information leaks from telecommunication networks by unexpected radio emission from equipment. 	
<p>The nature of the malicious electromagnetic threats and the corresponding mitigation techniques are similar to those that apply to natural or unintentional electromagnetic disturbances. For example, there are similarities between HEMP and the electromagnetic pulse created by lightning. Shielding and filtering techniques that reduce the emission of unwanted radio energy from equipment also minimize the possibility of unintentional energy leakage. Thus, the traditional activities of Study Group 5 related to protection against lightning and controlling Electromagnetic Interference (EMI) contribute to the security of the network against malicious man-made threats. The following Table describes the Questioned allocated to Study Group 5 for the 2001-2004 Study Period that have bearing on the security of the network.</p>	
<p>Main security-related Questions:</p> <ul style="list-style-type: none"> - Q.2/5 – EMC related to broadband access systems (<i>Control of unwanted emissions from broadband access systems contributes to reducing the possibility of information leaks</i>). - Q.4/5 – Resistibility of new types of communication equipment and access networks (<i>Resistibility of equipment to lightning improves resistibility of equipment to HEMP-induced surges</i>). - Q.5/5 – Lightning protection of fixed, mobile and wireless systems (<i>Techniques used for lightning protection also provide a degree of hardening of the facility against HEMP and HPE</i>). - Q.6/5 – Bonding configurations and earthing of telecommunication systems in the global environment (<i>Appropriate bonding and earthing measures also help hardening of the facility against HEMP and HPE</i>). - Q.12/5 – Maintenance and enhancement of existing EMC Recommendations (<i>EMC of telecommunication equipment improves the immunity of equipment against the conducted and radiated HEMP environment as well as radiated HPE environment. Also, EMC of telecommunication equipment reduces the possibility of information leaks</i>). - Q.13/5 – Maintenance and enhancement of existing resistibility recommendations (<i>Resistibility of equipment to lightning improves resistibility of equipment to HEMP-induced surges</i>). 	

SG 6	Outside plant
<p>Study Group 6 is responsible for studies relating to outside plant such as the construction, installation, jointing, terminating, protection from corrosion and others forms of damage from environment impact, except electromagnetic processes, of all types of cable for public telecommunications and associated structures.</p>	
<p>Main security-related Questions:</p> <ul style="list-style-type: none"> - Q.1/6 – Environmental issues of telecommunication plant - Q.2/6 – Fire safety - Q.5/6 – Optical fibre cable network maintenance 	

SG 9	Integrated broadband cable networks and television and sound transmission <i>Lead Study Group on integrated broadband cable and television networks.</i>
<p>The ITU Study Group on "Integrated broadband cable networks and television and sound transmission" (Study Group 9) is the lead study group on integrated broadband cable and television networks. The Study Group prepares and maintains recommendations on:</p> <ol style="list-style-type: none"> a) Use of cable and hybrid networks, primarily designed for television and sound programme delivery to the home, as integrated broadband networks to also carry voice or other time critical services, video on demand, interactive services, etc. b) Use of telecommunication systems for contribution, primary distribution and secondary distribution of television, sound programmes and similar data services. <p>In this role, Study Group 9 evaluates threats and vulnerabilities to broadband networks and services, documents security objectives, evaluates countermeasures, and defines security architectures. The main security areas addressed are secure broadband services, secure VoIP services, secure home networking services, and secure application environments for interactive television services.</p>	
<p>Security related activities have focused on the following areas:</p> <ol style="list-style-type: none"> a) <i>Secure broadband services</i>: provide security services for broadband access networks. Namely, authentication of the cable modem, cryptographic key management, privacy and integrity of transmitted data, and secure download of cable modem software. b) <i>Secure VoIP services</i>: IPCablecom is a special project on time-critical interactive services over cable television network using IP-protocol, in particular Voice and Video over IP. Security services provided in IPCablecom include authentication of the Multimedia Terminal Adapter (MTA) to the service provider, authentication of the service provider to the MTA, secure device provisioning and configuration, secure device management, secure signalling, and secure media. c) <i>Secure home networking services</i>: Enhanced Cable Modems can provide home networking services such as firewalls and Network Address Translation. Security services provided for enhanced Cable Modems include authentication of the Multimedia Terminal Adapter (MTA) to the service provider, authentication of the service provider to the MTA, secure device provisioning and configuration, secure device management, packet-filtering/firewall functionality, secure firewall management, and secure download of enhanced cable modem software. d) <i>Secure application environments for interactive television services</i>: Interactive television services rely on the security services defined in Java and the Multimedia Home Platform (MHP) specification. 	
<p>Main security-related Questions:</p> <ul style="list-style-type: none"> - Q.6/9 – Methods and practices for conditional access and copy protection for digital cable television distribution to the home - Q.13/9 – Voice and video IP applications over cable television networks - Q.14/9 – The extension of cable-based services over broadband in Home Networks 	

SG 11	<p>Signalling requirements and protocols <i>Lead Study Group on intelligent networks.</i></p>
<p>Study Group 11 is responsible for studies relating to signalling requirements and protocols for Internet Protocol (IP) related functions, some mobility related functions, multimedia functions and enhancements to existing Recommendations on access and inter-network signalling protocols of ATM, N-ISDN and PSTN.</p>	
<p>Main security-related Questions:</p> <ul style="list-style-type: none"> - Q.1/11 – Signalling requirements for signalling support for new, value added, IP based and IN based services. - Q.6/11 – Signalling requirements for signalling support for service interworking of dialup Internet access and Voice, Data and Multimedia Communications over IP-based networks. - Q.12/11 – Access and network signalling for advanced narrow-band and broadband services. 	
SG 12	<p>End-to-end transmission performance of networks and terminals <i>Lead Study Group on Quality of Service and performance.</i></p>
<p>Study Group 12 is responsible for guidance on the end-to-end transmission performance of networks, terminals and their interactions, in relation to the perceived quality and acceptance by users of text, speech, and image applications. This work includes the related transmission implications of all networks (e.g., those based on PDH, SDH, ATM and IP) and all telecommunications terminals (e.g., handset, hands-free, headset, mobile, audiovisual, and interactive voice response).</p>	
<p>Main security-related Questions:</p> <ul style="list-style-type: none"> Q.12/12 – Transmission performance considerations for voiceband services carried on networks that use Internet Protocol (IP) Q.13/12 – Multimedia QoS/performance requirements 	

SG 13	<p>Multi-protocol and IP-based networks and their internetworking <i>Lead Study Group for IP related matters, B-ISDN, Global Information Infrastructure and satellite matters.</i></p>
<p>Due to the nature of the responsibility of Study Group 13 and the studies related to</p> <ul style="list-style-type: none"> a) Internetworking of heterogeneous networks encompassing multiple domains, b) Multiple protocols and innovative technologies with a goal to deliver high-quality, reliable networking. c) Specific aspects are architecture, interworking and adaptation, end-to-end considerations, routing and requirements for transport. <p>As the lead study group for IP related matters, B-ISDN, Global Information Infrastructure and satellite matters and the new NGN-Project a lot of security issues will be affected in a very broad sense. Traditionally Study Group 13 has implicitly handled security aspects when dealing with architecture and network structure issues, knowing that it was absolutely necessary to cover such issues (from an architecture and implementation point of view) in order to ensure a functional and reliable network. The difficulties with security aspects increase when the new –more or less open- digital packet switched technologies and the liberalized environment described, e.g. in the GII concept, are implemented. This is especially true when, in the concept of the "value added chain" according to the GII approach (or the subset of it NGN), third parties are involved. In this environment security with all its facets will become an even more important issue and must be addressed in an explicit manner. Therefore Study Group 13 had decided to incorporate in every new or eventually revised Recommendation a security section for references to those sections of the Recommendation in which security aspects are addressed. Even if there are no security aspects dealt with in a Recommendation, this fact should be recorded in this particular security section. This decision was already acknowledged by Study Group 17 and proposed to offer it to all ITU-T study groups. Further it was decided in Study Group 13 that Recommendations having security-related specifications should be reported to Study Group 17 in order to allow timely updating of the "Catalogue of the approved security Recommendations" and "Compendium of ITU-T Approved Security Definitions." Also the new NGN project addresses security aspects in several sections with a special attention in section 6.6.</p>	
<p>Main security-related Questions:</p> <ul style="list-style-type: none"> Q.1/13 – Principles, Requirements, Frameworks and Architectures for an Overall Heterogeneous Network Environment Q.3/13 – OAM and Network Management in IP-Based and Other Networks Q.4/13 – Broadband and IP Related Resource Management Q.6/13 – Performance of IP-Based Networks and The Emerging Global Information Infrastructure Q.7/13 – B-ISDN/ATM Cell Transfer and Availability Performance Q.8/13 – Transmission Error and Availability Performance Q.10/13 – Core Network Architecture and Interworking Principles Q.11/13 – Mechanisms to Allow IP-Based Services to Operate in Public Networks 	

SG 15	<p>Optical and other transport networks <i>Lead Study Group on Access Network Transport and on Optical Technology.</i></p>
<p>Question 14 in Study Group 15 (Q.14/15) is responsible for specifying the management and control requirements and supporting information models for transport equipment. Q.14/15 has been following the ITU-T established TMN concept and framework for the definition of these requirements and models. Security management is one of the five key TMN management functional categories. Security management has been within the scope of and under study by Q.14/15.</p> <ol style="list-style-type: none"> a) Requirements for transport equipment management: G.7710/Y.1701, G.784, and G.874 address the Equipment Management Functions (EMFs) inside a transport Network Element that are common to multiple technologies, specific to SDH NE, and specific to OTN NE, respectively. Applications are described for Date & Time, Fault Management, Configuration Management, Account Management, Performance Management and Security Management. These applications result in the specification of EMF functions and their requirements. Security management requirements in these Recommendations are currently under study. b) Data Communication Network Architecture and Requirements: G.7712/Y.1703 defines the architecture requirements for a Data Communications Network (DCN) which may support distributed management communications related to the Telecommunications Management Network (TMN), distributed signalling communications related to the Automatically Switched Transport Network (ASTN), and other distributed communications (e.g., Orderwire or Voice Communications, Software Download). Various applications (e.g., TMN, ASTN, etc.) require a packet based communications network to transport information between various components. For example, the TMN requires a communications network, which is referred to as the Management Communications Network (MCN) to transport management messages between TMN components (e.g., NEF component and OSF component). ASTN requires a communications network, which is referred to as the Signalling Communications Network (SCN) to transport signalling messages between ASTN components (e.g., CC components). G.7712/Y.1703 references M.3016 for MCN security requirements. SCN security requirements are defined in G.7712/Y.1703. c) Distributed Call and Connection Management: G.7713/Y.1704 provides the requirements for the distributed call and connection management for both the User Network Interface (UNI) and the Network Node Interface (NNI). The requirements in this Recommendation specify the communications across interfaces to effect automated call operations and connection operations. Security attributes are specified, along with others, to allow verification of call and connection operations (e.g., this may include information to allow authentication of the call request, and possibly integrity checking of call request). d) Architecture and requirements for routing in the automatically switched optical networks: G.7715/Y.1706 specifies the requirements and architecture for the routing functions used for the establishment of switched connections (SC) and soft permanent connections (SPC) within the framework of the Automatically Switched Optical Network (ASON). The main areas covered in this Recommendation include the ASON routing architecture, functional components including path selection, routing attributes, abstract messages and state diagrams. This Recommendation references ITU-T Rec. M.3016 and X.800 for security considerations. In particular, it states that, depending on the context of usage of a routing protocol, the overall security objectives defined in ITU-T Rec. M.3016 of confidentiality, data integrity, accountability and availability may take on varying levels of importance. A threat analysis of a proposed routing protocol should address the following items based on ITU-T Rec. X.800; i.e. masquerade, eavesdropping, unauthorized access, loss or corruption of information (includes replay attacks), repudiation, forgery and denial of service. e) Framework of ASON Management: G.7716 addresses the management aspects of the ASON control plane and the interactions between the management plane and the ASON control plane. Fault management, configuration management, accounting management, performance management, and security management requirements for the Control plane components will be included. 	
<p>Main security-related Questions: - Q.14/15 – Network Management for transport systems and equipment</p>	

SG 16	<p>Multimedia services, systems and terminals <i>Lead Study Group on multimedia services, systems and terminals, e-business and e-commerce.</i></p>
<p>Study Group 16 is the lead study group on multimedia services, systems and terminals, and lead on e-business and e-commerce. Question G (of WP 2/16) covers "Security of Multimedia Systems and Services" and addresses the following security issues.</p> <p>Advanced multimedia (MM) applications like telephony over packet-based networks, Voice-over-IP, interactive conferencing and collaboration; MM messaging, Audio/Video streaming and others are subject to a variety of crucial security threats in heterogeneous environments. Misuse, malicious tampering, eavesdropping, and denial-of-service attacks are just a few of the potential risks; especially on IP-based networks.</p> <p>It is recognized that those applications have common security needs that could be satisfied by generic security measures; e.g. by network security. Yet, MM applications typically are subject to application-specific security needs that could best be fulfilled by security measures at the application layer. Question G focuses on the application-security issues of MM applications and takes complementary network security means into account as appropriate.</p>	
<p>Main security-related Questions: - Q.G/16 – Security of Multimedia Systems and Services</p>	

SG 17	<p>Data Networks and Telecommunication Software <i>Lead Study Group on frame relay, communication system security, languages and description techniques.</i></p>
<p>Study Group 17 is responsible for studies relating to data communication networks, for studies relating to the application of open system communications including networking, directory and security, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems.</p> <p>ITU-T Study Group 17 is the lead study group for security issues. The ITU-T security standardization effort is coordinated via a new ITU-T Project on Security managed under Question G/17. As part of this effort, a catalogue of ITU Recommendations related to security and a compendium of security definitions extracted from approved ITU-T Recommendations have been developed and kept up-to-date. A workshop on Security was held May 2002 in Seoul, Korea and a second Workshop is currently targeted for early next study period. Current information is available on the Study Group 17 page of the ITU web site (see http://www.itu.int/ITU-T/studygroups/com17/cssecurity.html).</p> <p>Under the responsibility of Question E/17, the well-known Recommendation X.509, <i>Public-key and attribute certificate frameworks</i> is the foundation for Public Key Infrastructures (PKI) and Privilege Management Infrastructures (PMI). X.509 continues to be enhanced to meet evolving needs. Under Questions F/17 and H/17, a substantial number of core security architecture, framework, and protocol Recommendations are in place, especially in the X.800-series.</p> <p>A fresh look at security was undertaken this study period that culminated in new Recommendations. A new flagship Recommendation, X.805, was prepared that defines a security architecture for providing end-to-end network security. This architecture can be applied to various kinds of networks independently of the network's underlying technology. It can be used as a tool to ensure the completeness of security considerations in developing Recommendations and for conducting security assessments of networks. Another fundamental Recommendation is X.1051 that presents the requirements for an information security management system (ISMS) in the context of telecommunications. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the telecommunication organization's overall business risks. X.1081 is a framework Recommendation establishing the foundation for future telebiometric specifications. X.1121 and X.1122 focus on mobile end-to-end data communications. X.1121 analyses the security threats in a mobile environment and the means for protection from the point of view of the mobile user and the application service provider. X.1122 provides guidance when constructing secure mobile systems based on Public Key Infrastructure (PKI) technology.</p> <p>Security-related Questions: Q.E/17 – Directory Services, Directory Systems, and Public-key/Attribute Certificates Q.F/17 – Open Systems Interconnection (OSI) Q.G/17 – Communications Systems Security Project Q.H/17 – Security Architecture and Framework Q.I/17 – Cyber Security Q.J/17 – Security Management Q.K/17 – Telebiometrics Q.L/17 – Secure Communication Services Q.M/17 – Abstract Syntax Notation One (ASN.1) and other Data Languages</p>	

SSG	<p>Special Study Group "IMT-2000 and Beyond" <i>Lead Study Group on IMT-2000 and beyond and for mobility.</i></p>
<p>The ITU-T Special Study Group on "IMT-2000 and Beyond" has included security as a key aspect of its referencing Recommendations for IMT-2000 (3G) Family Members identified in its Q.1741.x (3GPP) and Q.1742.x (3GPP2) series Recommendations. These include an evaluation of perceived threats and a list of security requirements to address these threats, security objectives and principles, a defined security architecture (i.e., security features and mechanisms), cryptographic algorithm requirements, lawful interception requirements, and lawful interception architecture and functions. These studies are dealt with in Question 3, 6 and 7/SSG. The prime objective of the Lawful Interception studies are to identify useful interception and monitoring related information that need to be provided by service providers to national law enforcement agencies. The interception related information and the content of communication may be technology independent or dependent on 3G or evolved 3G mobile networks.</p>	
<p>Main security-related Questions:</p> <ul style="list-style-type: none"> - 3/SSG – Identification of existing and evolving IMT-2000 systems - 6/SSG – Harmonization of evolving IMT-2000 systems - 7/SSG – Convergence of fixed and existing IMT-2000 systems 	

ITU-T security building blocks

Security Architecture Framework

- X.800 – Security architecture
- X.802 – Lower layers security model
- X.803 – Upper layers security model
- X.810 – Security frameworks for open systems: Overview
- X.811 – Security frameworks for open systems: Authentication framework
- X.812 – Security frameworks for open systems: Access control framework
- X.813 – Security frameworks for open systems: Non-repudiation framework
- X.814 – Security frameworks for open systems: Confidentiality framework
- X.815 – Security frameworks for open systems: Integrity framework
- X.816 – Security frameworks for open systems: Security audit and alarms framework

Network Management Security

- M.3010 – Principles for a telecommunications management network
- M.3016 – TMN Security Overview
- M.3210.1 – TMN management services for IMT-2000 security management
- M.3320 – Management requirements framework for the TMN X-Interface
- M.3400 – TMN management functions

Systems Management

- X.733 – Alarm reporting function
- X.735 – Log control function
- X.736 – Security alarm reporting function
- X.740 – Security audit trail function
- X.741 – Objects and attributes for access control

Telecommunication Security

- X.805 – Security architecture for systems providing end-to-end communications
- X.1051 – Information security management system – Requirements for telecommunications (ISMS-T)
- X.1081 – A framework for specification of security and safety aspects of telediometrics
- X.1121 – Framework of security technologies for mobile end-to-end communications
- X.1122 – Guideline for implementing secure mobile systems based on PKI

Televisions and Cable Systems

- J.91 – Technical methods for ensuring privacy in long-distance international television transmission
- J.93 – Requirements for conditional access in the secondary distribution of digital television on cable television systems
- J.170 – IP-Cablecom security specification

Multimedia Communications

- H.233 – Confidentiality system for audiovisual services
- H.234 – Encryption key management and authentication system for audiovisual services
- H.235 – Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals
- H.323 Annex J – Packet-based multimedia communications systems – Security for H.323 Annex F (Security for simple endpoint types)
- H.350.2 – Directory services architecture for H.235
- H.530 – Symmetric security procedures for H.323 mobility in H.510

Protocols

- X.273 – Network layer security protocol
- X.274 – Transport layer security protocol

Security in Frame Relay

- X.272 – Data compression and privacy over frame relay networks

Security Techniques

- X.841 – Security information objects for access control
- X.842 – Guidelines for the use and management of trusted third party services
- X.843 – Specification of TTP services to support the application of digital signatures

Facsimile

- T.30 Annex G – Procedures for secure Group 3 document facsimile transmission using the HKM and HFX system
- T.30 Annex H – Security in facsimile Group 3 based on the RSA algorithm
- T.36 – Security capabilities for use with Group 3 facsimile terminals
- T.503 – Document application profile for the interchange of Group 4 facsimile documents
- T.563 – Terminal characteristics for Group 4 facsimile apparatus

Directory Services and Authentication

- X.500 – Overview of concepts, models and services
- X.501 – Models
- X.509 – Public-key and attribute certificate frameworks
- X.519 – Protocol specifications

Message Handling Systems (MHS)

- X.400/ – Message handling system and service overview
- F.400
- X.402 – Overall architecture
- X.411 – Message transfer system: Abstract service definition and procedures
- X.413 – Message store: Abstract service definition
- X.419 – Protocol specifications
- X.420 – Interpersonal messaging system
- X.435 – Electronic data interchange messaging system
- X.440 – Voice messaging system

ITU-T Recommendations are available from the ITU website <http://www.itu.int/publications/bookshop/how-to-buy.html> (this site includes information on limited free access to ITU-T Recommendations)

Current important security work in ITU-T includes

Telediometrics, Security management, Mobility security, Emergency telecommunications

For further information on ITU-T and its Study Groups: <http://www.itu.int/ITU-T>