ITU

Security in Telecommunications and Information Technology

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

December 2003

ITU-T

Telecommunication
Standardization
Sector of ITU

ITU

International
Telecommunication
Union

Security
in Telecommunications and
Information Technology

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

Contents

Acknowledgements

Preface

Restricted in the past to niche areas such as banking, aerospace or military applications, digital security is slowly but surely becoming everyone's business.

The increased profile of digital security may be attributed to headline news such as viruses spread by e-mail, or hackers stealing credit-card details. But this is only part of the story. As computing and networking become as much a part of daily life as water and electricity, digital security is being talked about not only by experts but also more and more in governments, companies, and by consumers. And, if so many aspects of our business and private life rely on computers and networks, it is imperative that these systems operate securely.

It is also imperative that security be a well-thought process from system inception and design via system implementation to policies and practices for system deployment, operation and use. In the development of standards, security must always be an element of initial work, and not an afterthought – as it is in this stage that vulnerabilities are born. The role of standards committees is to listen to the market and document known issues, to provide workarounds if possible, and to issue specifications or guidelines that assist implementers and users in the task of making communication systems and services sufficiently robust.

ITU-T has been active in security in telecommunications and information technology for many years. However, it may not have always been easy to find out what has been covered, and where it can be found. This manual is a first attempt at aggregating all of the available information. I would like to express my appreciation to the engineers of the ITU Telecommunication Standardization Bureau who, in conjunction with various experts from the ITU membership, have done most of this hard 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.

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

Houlin Zhao

Director, Telecommunication Standardization Bureau

ITU

Geneva, December 2003

Executive Summary

The communications industry, meeting the needs of an increasingly global commerce environment, has contributed to better productivity and bridged communities globally in almost every industrial segment. That this communications infrastructure is so efficient, is in no small part due to standards developed by organizations such as ITU-T. The standards that keep current networks efficient 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 actors, the sheer diversity of applications and platforms, and implementations not always tested enough have increased opportunities for malicious use of networks. In recent years, a surge in security violations (such as viruses and breach of confidentiality of stored data) has been observed throughout global networks, and 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. The answer lies in efforts by standards groups to combat security threats at all areas of the communications infrastructure. These provisions range from details in protocol specifications and in applications to the management of networks. The purpose of this security manual is to highlight and offer a bird's eye view of the numerous Recommendations developed by ITU-T – sometimes in collaboration with other Standard Development Organizations – to secure the communication infrastructure and 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 summarizes the architectural elements defined in ITU-T Recommendation X.805 along with the eight security dimensions that have been defined to address end-to-end security in networked applications – privacy, data confidentiality, authentication, integrity, non-repudiation, access control, communication security, and availability. These general principles are used to guide and understand the details discussed in other sections. Major elements include security layers, security planes and the dimensions applied to the combination of any layer and plane.

Section 3 introduces three key terms used when discussing security: vulnerability, threat and risk. The distinguishing characteristics of the three terms are described and some examples are given. A key point from this section is to note how a security risk is a result of combining vulnerability and threat.

Section 4 builds on information in previous sections to define meta-requirements for establishing a security framework. Key elements for achieving security to combat threats are to define mechanisms and algorithms associated with security measures such as authentication, access control, and data encryption. Section 5 defines these mechanisms with the concept of public key and privilege management infrastructures. These mechanisms and infrastructures can be applied to many different end-user applications.

In addition to this framework, architecture and mechanisms, ITU-T has developed security provisions in several systems and services defined in its Recommendations. Thus a significant focus of this manual is on applications, as seen in Section 6. A sample set of applications is included in this first edition. 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.

In addition, this version of the manual contains 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 Compendia on Communication System Security developed by ITU-T Study Group 17). This is provided in Annex A. This manual also provides the current version of the ITU-T Catalogue of Recommendations with Security Aspects – the list in Annex B is extensive and further demonstrates the breadth of ITU-T work on security. In Annex C we summarize the security-related work that each of the ITU-T Study Groups do. 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 first edition, the manual does not cover all aspects of security, in particular not 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. 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 is engineers and product managers, students and academia, as well as regulators who want to better understand security issues in practical applications.

2 Basic Security Architecture and Dimensions

Recommendation X.805 defines the framework for the architecture and dimensions in achieving end-to-end security of distributed applications. 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.

The security architecture is defined in terms of two major concepts, layers and planes. 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 counter measures 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 of the framework addresses the security of activities performed in a network. The security framework 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 & 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 axis (3 security planes and 3 security layers), the framework also defines eight dimensions that are designed to address network security. These dimensions are defined in the sections 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 counter measures 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.
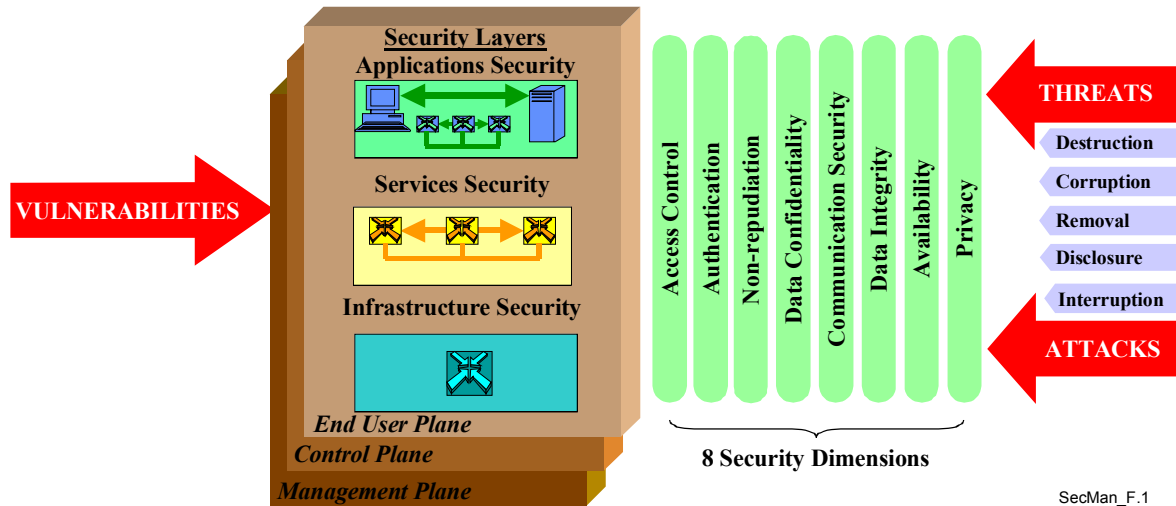
Figure 1
Security Architectural Elements in ITU-T X.805

2.1 Privacy and Data Confidentiality

The concept of privacy is a fundamental motivator for security. Privacy is commonly understood as 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. By extension, privacy is also associated with certain technical means (e.g. cryptography) to ensure that this information is not disclosed to any one other than the intended parties, so that only the explicitly authorized parties can interpret the content exchanged among them.

Most commonly, privacy and confidentiality are used as the same term, but it should be noted that ITU-T X.805 differentiates privacy and data confidentiality, the former relating to the protection of the association of the identity of users and the activities performed by them (such as online purchase habits, Internet sites visited, etc), and the latter relating to the protection against unauthorized access to data contents. Encryption, access control lists, and file permissions are methods often used to provide data confidentiality.

The term Privacy is referenced in several ITU-T Recommendations, including F.115, H.235, J.160, Q.1531, X.800, and X.805.

2.2 Authentication

Authentication is the provision of proof that the claimed identity of an entity is true. Entities here include not only human users but also devices, services and applications. Authentication also provides for assurance that an entity is not attempting a masquerade or an unauthorized replay of a previous communication. There are two kinds of authentication: data origin authentication (i.e. authentication requested in a connection-oriented association) and peer entity authentication (i.e. authentication in a connectionless association). The network should ensure that a data exchange is established with the addressed peer entity (and not with an entity attempting a masquerade or a replay of a previous establishment) and that the data origin is the one claimed. Authentication generally follows identification. Information used for identification, authentication and authorization should be protected by the network.

The term Authentication is referenced in several ITU-T Recommendations, including F.500, F.851, F.852, H.235, J.160, J.93, J.95, M.60, X.217, X.217-Bis, X.509, X.800, X.805, and X.811.

2.3   Integrity

Data integrity is the property that data have not been altered in an unauthorized manner. By extension, data integrity also ensures that information is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities.

The term Integrity is referenced in several ITU-T Recommendations, including H.235, J.160, J.93, J.95, Q.1290, Q.1531, X.800, and X.815.

2.4   Non-repudiation

Non-repudiation is the ability to prevent users from denying later that they performed an action. These actions include content creation, origination, receipt, and delivery, such as sending or receiving messages, establishing or receiving calls, participating in audio and video conferences, etc.

Non-repudiation requirements provide unforgeable proof of shipment and/or receipt of data to prevent the sender from disavowing a legitimate message or the recipient from denying receipt. The network may provide either or both of the following two forms: the recipient of data is provided with proof of origin of data that will protect against any attempt by the sender to falsely deny sending the data or its contents; or the sender is provided with proof of delivery of data such that the recipient cannot later deny receiving the data or its contents.

The term Non-repudiation is referenced in several ITU-T Recommendations, including F.400, F.435, F.440, J.160, J.93, J.95, M.60, T.411, X.400, X.805, X.813, and X.843.

2.5   Other dimensions defined in X.805

In addition to Privacy and Data Confidentiality, Authentication, Integrity and Non-repudiation, ITU-T X.805 defines the three other security dimensions: Access Control, Communication, and Availability.

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. Access Control is defined in ITU-T X.810 section 6.3 and X.812. It is related but beyond the scope of Authentication.

The *Communication* security dimension is a new dimension defined in X.805 that ensures that information flows only between authorized end points. This dimension deals with measures to control network traffic flows for prevention of traffic diversion and interception.

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 network interruption. Network restoration and disaster recovery solutions are included in this category.

3   Vulnerabilities, threats and risks

With such a huge focus on implementing the most advantageous IT solution or determining which of the latest and greatest web applications, servers and databases best suits the objectives of an organization, protecting the information held by those assets has often been handled as second priority. Many enterprises may be fooled into thinking that because they have not been hit, there is no threat.

Standards bodies have a unique ability and responsibility to address security vulnerabilities in protocols. There are immediate and relatively simple actions standards bodies can take to improve the security of all protocols currently being standardized.

A *security vulnerability* is a flaw or weakness in a system's design, implementation or operation that could be exploited to violate the system's security (RFC 2828). A security vulnerability is not a risk, a threat, or an attack.

Vulnerabilities can be of four types. *Threat Model* vulnerabilities originate from the difficulty to foresee future threats (e.g. Signalling System No.7). *Design & Specification* vulnerabilities come from errors or oversights in the design of the protocol that make it inherently vulnerable (e.g. WEP in IEEE 802.11b a.k.a. WiFi). *Implementation* vulnerabilities are vulnerabilities that are introduced by errors in a protocol implementation. Finally, *Operation and Configuration* vulnerabilities originate from improper usage of options in implementations or weak deployment policies (e.g. not enforcing use of encryption in a WiFi network, or selection of a weak stream cipher by the network administrator).

According to X.800, a *security threat* is a potential violation of security, which can be active (when the state of a system can be changed), or passive (unauthorized disclosure of information without changing the state of the system). Masquerading as an authorized entity and denial of service are examples of active threats and eavesdropping to steal a clear password is an example of a passive threat. Agents of threats can be hackers, terrorists, vandals, organized crime, or state sponsored, but in a significant number of cases threats come from insiders of an organization.

A *security risk* originates when a security vulnerability is combined with a security threat. For example, an overflow bug in an operating system application (i.e. a vulnerability) associated with a hacker's knowledge, appropriate tools and access (i.e. a threat) can develop the risk of a web server attack. Consequences of security risks are data loss, data corruption, privacy loss, fraud, downtime, and loss of public confidence.

While threats change, security vulnerabilities exist throughout the life of a protocol. 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.

4   Security Framework Requirements

The requirement for a generic network security framework 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 terrorist actions).

- Public authorities demand security by directives and legislation, in order to ensure availability of services, fair competition and privacy protection.

- Network operators and service providers themselves need security to safeguard their operation and business interests, and to meet their obligations to the customers and the public.

Security requirements for telecommunication networks and services should preferably be based upon internationally agreed security standards, as it increases interoperability as well as avoids duplication of efforts and reinventing the wheel. The provisioning and usage of security services and mechanisms can be quite expensive relatively to the value of the transactions being protected. There is a balance to consider between the cost of security measures and the potential financial effects of security breaches. 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 customisation. 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 a 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.

The security services and mechanisms that can be provided to telecommunication networks or service providers are related to protection 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, measures to prevent service outages due to natural events (weather, etc.) as well as management of security-related information. Provisions must be made to allow lawful interception as requested by duly authorized legal authorities.

5 PKI and privilege management with X.509

X.509 Public Key Infrastructure (PKI) provides a standard for strong authentication, based on public key certificates and certification authorities. PKI provides a scalable way of authenticating the messages of communicating parties. The fundamental technology of a PKI is public key cryptography, and so this will be described first. In addition to PKI, X.509 also provides for Privilege Management Infrastructure (PMI), which defines a standard for strong authorization, based on attribute certificates and attribute authorities. PMI is used to ascertain rights and privileges of users. The components for PKI and PMI are illustrated in Figure 2.

5.1 Secret & Public Key Cryptography

Symmetric (or *secret key*) cryptography refers to a cryptographic system where the enciphering and deciphering keys are the same, 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. One is made public, whereas the other is kept secret. The public key is different from the private key, and although mathematically related, no feasible way is known for deriving the private key from the public key. Public keys are distributed widely; however, the private key is always kept secret (e.g., on a smart card or on a token, in the future also on a PDA or mobile phone). In general, to send encrypted confidential data to someone, a person encrypts the data with the recipient's public key, and the people receiving the encrypted data decrypts it with their corresponding private key. To send authenticated data to someone, the sender encrypts the data with his/her private key, and the recipient authenticates the data with the corresponding public key of the sender. However, asymmetric encryption used in this fashion has a couple of disadvantages. Firstly public key encryption is costly in terms of computing time, therefore it is not efficient to encrypt entire messages using asymmetric encryption. Secondly, 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 who is the recipient. Thus in practice asymmetric encryption is only used to encrypt small parts of messages. When confidentiality is required, the message is encrypted using conventional symmetric encryption, and the symmetric key is asymmetrically encrypted using the public key of the recipient. When authentication 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 (which is sent in the clear) prior to transfer. This appended cryptographic checksum is called a digital signature – an important feature for electronic commerce.

Public key cryptography depends upon people being in possession of the correct public keys of their respective private key holders. If Bob wrongly believes that he is in possession of the public key of Alice, when in fact the public key belongs to the private key held by Jane, then Bob will believe that messages digitally signed by Jane actually came from Alice (which allows Jane to masquerade as Alice). Furthermore, if Bob wished to send a confidential message to Alice, Jane would be able to intercept it and decipher the message, whilst Alice would not be able to read it. Thus it is crucial that people have a way of validating the rightful owner of a public key.
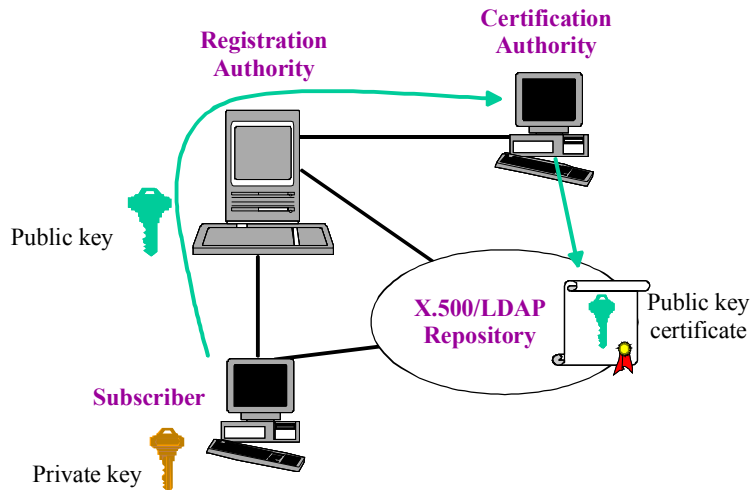
(a) Components of a public key infrastructure
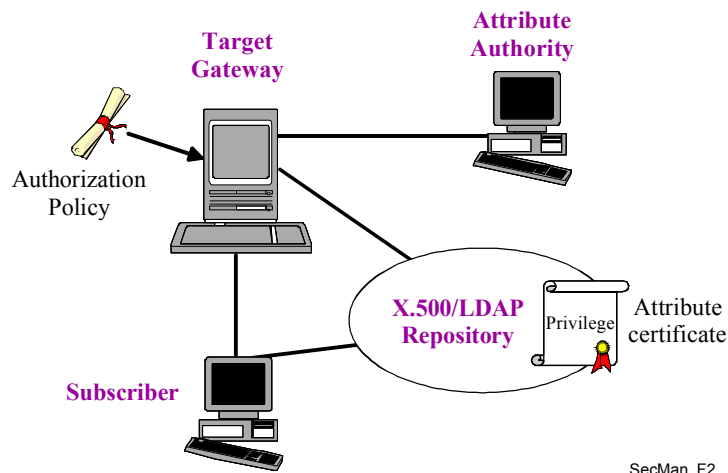
(b) Components of a privilege management infrastructure

Figure 2
Components of PKI and PMI

```
            Plain text                      Plain text
                |                                ↑
                ↓                                |
      encrypt message with          decrypt message with
          secret key                  same secret key
                |                                ↑
                └──────→ cipher text ────────────┘
```

– Both parties share a <u>single, secret key</u>
– Problem: exchanging keys in complete secrecy is difficult
– Best-known example: DES (Data Encryption Standard)
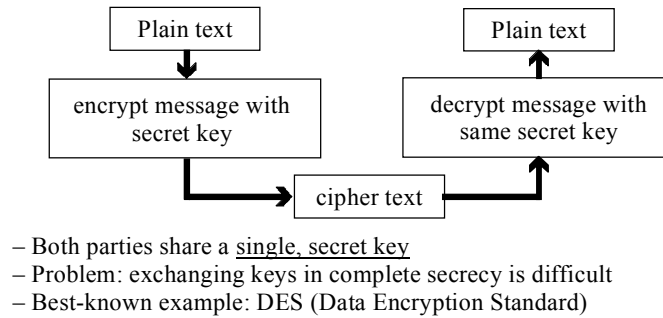
(a) (Symmetric) Secret Key Encryption

```
            Plain text                      Plain text
                |                                ↑
                ↓                                |
      encrypt message with          decrypt message with
      *public* key of receiver       *public* key of receiver
                |                                ↑
                └──────→ cipher text ────────────┘
```

– <u>Each</u> participant has
    - A <u>private</u> key that is shared with no one else, plus
    - A <u>public</u> key known to everyone
– Problem: slower than Secret Key Encryption
– Best-known example: RSA
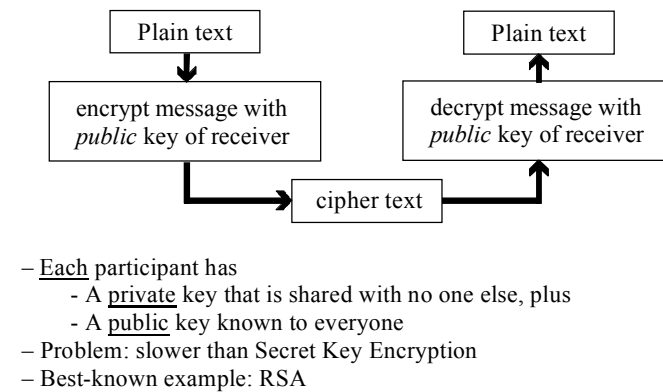
(b) (Asymmetric) Public Key Encryption   SecMan_F3

Figure 3
Illustration of the symmetric (or private) 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 recognised standard format for public key certificates is defined in the X.509 standard. 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 time 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. The X.509 certificate can now be widely published, for example on a web site, in an LDAP directory, or in the Vcard attached to email messages, and the CA's signature ensures that its contents cannot be unknowingly tampered with.

It is obvious that in order to be able to validate a user's public key certificate, a person needs to have access to the valid public key of the CA that issued the user's certificate, so as to be able to check the signature on the user's certificate. A CA may have its public key certified by another (superior) CA, so that validating public keys becomes recursive, as we move along the chain of certificates. Eventually this chain must end somewhere, which is typically when we encounter the self-signed 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 pubic 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 the X.509 standard provides mechanisms for distributing (part 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 quality 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-organisational 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

ITU-T Recommendation X.509 has specified in its first versions the basic elements for Public Key Infrastructures (PKI). This included the definition of Public Key Certificates. The revision approved in 2000 contains a significant enhancement on Attribute Certificates and a framework for Privilege Management Infrastructure. The mechanisms defined allow for setting user access privileges in a multi-vendor and multi-application environment.

There are similar concepts between PMI and PKI, but the first deals with authorization while the second 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 asserter, the privilege verifier, the object method[1], 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 asserter, in accordance with the privilege policy.
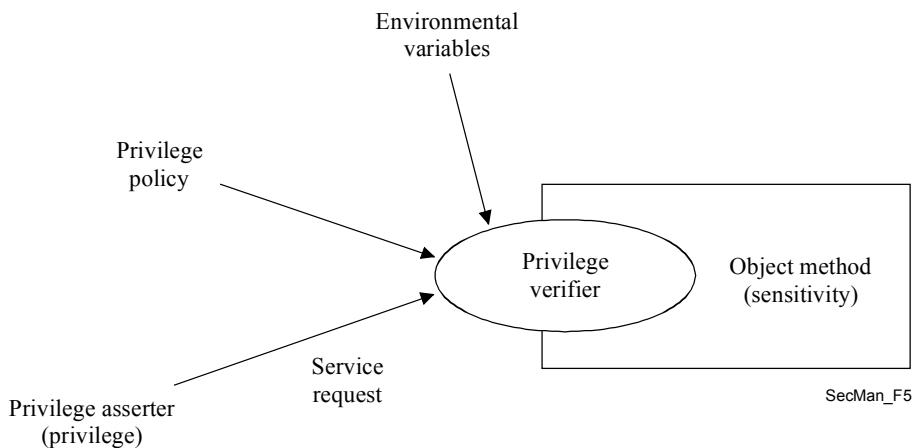
Figure 5
ITU-T X.509 PMI Control Model

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 SoA, other AAs and the privilege asserter (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).
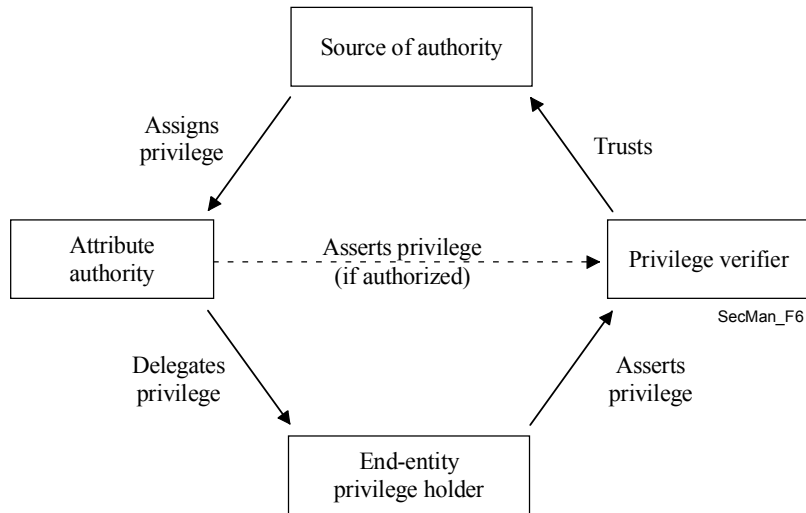
Figure 6
ITU-T X.509 PMI Delegation Model

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 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

Voice-over-IP (VoIP), also known as IP telephony, is the provision of services traditionally offered via the circuit-switched PSTN 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 wait, 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:

- 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 the H.323 specification 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. 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 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 (i.e. H.225.0 to H.221) and between communications procedures (i.e. 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.
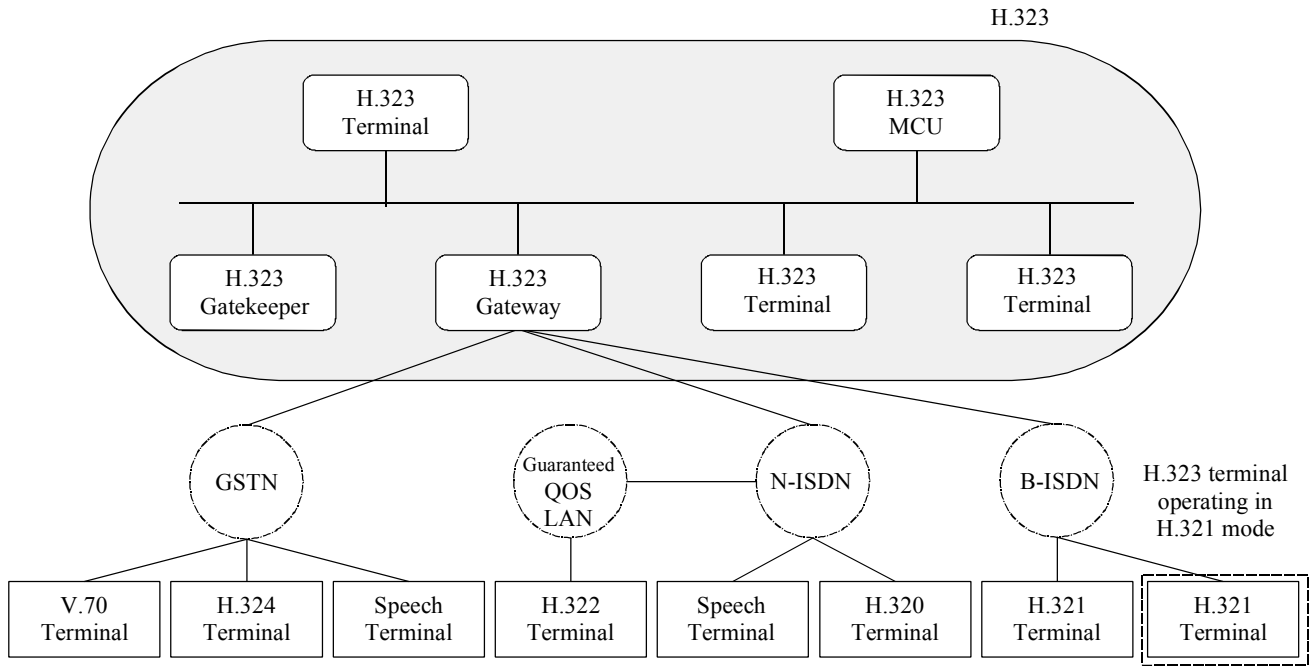
(a) H.323 system and its components [Packetizer]
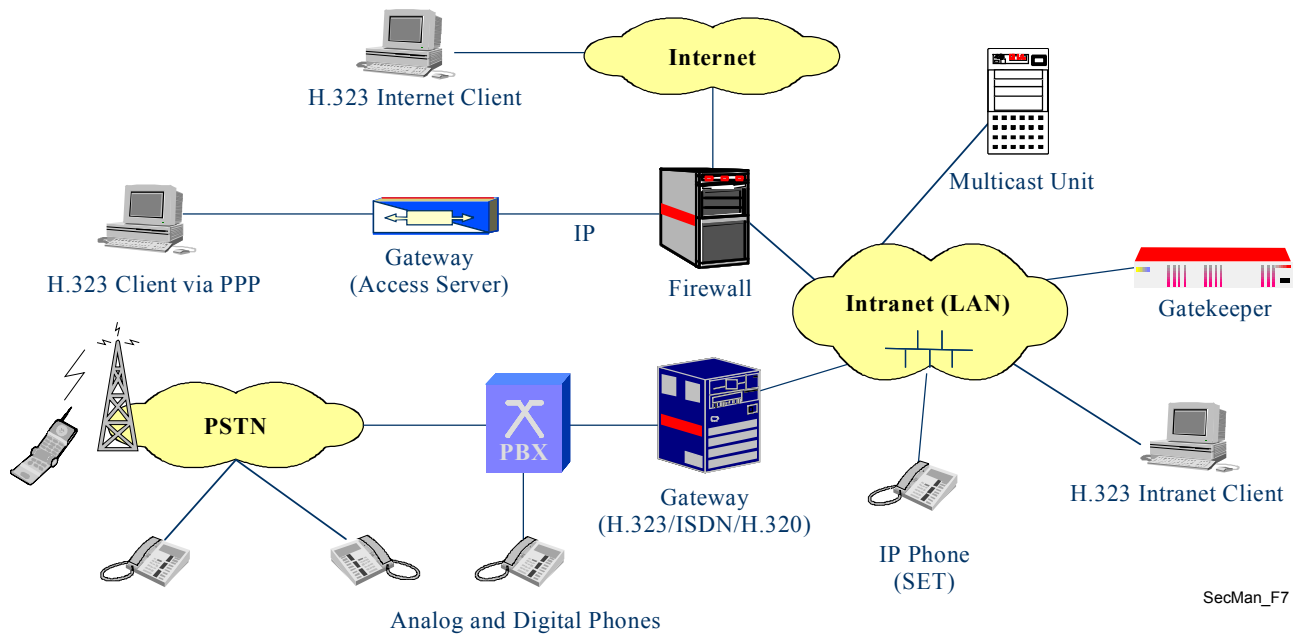
(b) H.323 deployment scenarios [Euchner]

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 Voice-over IP 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.
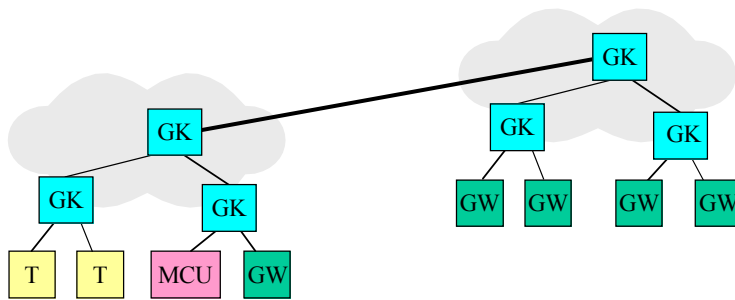
(a) Topology with RAS[1]
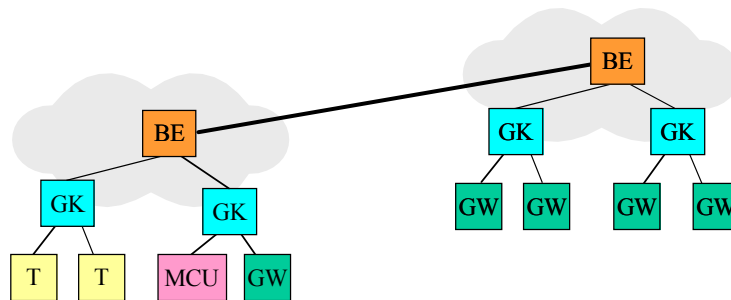
(b) Topology with Annex G/H.225.0
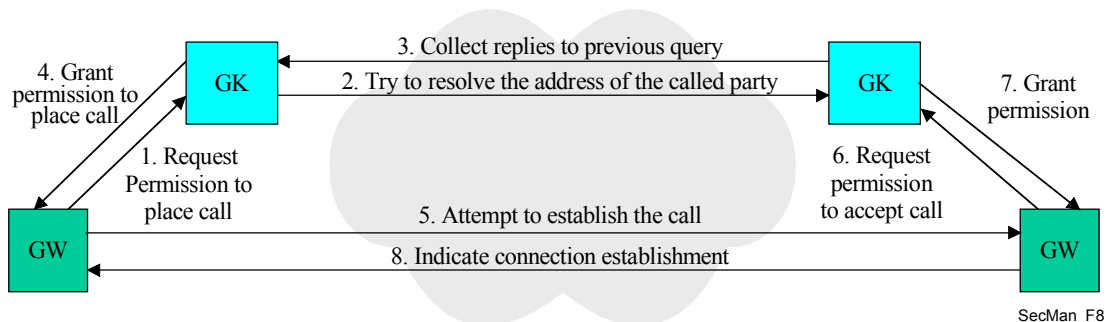
(c) High Level Call Flow

Legend: BE: Border Element; GK: Gatekeeper; GW: Gateway; MCU: Multipoint Control Unit; T: Terminal

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
- 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.
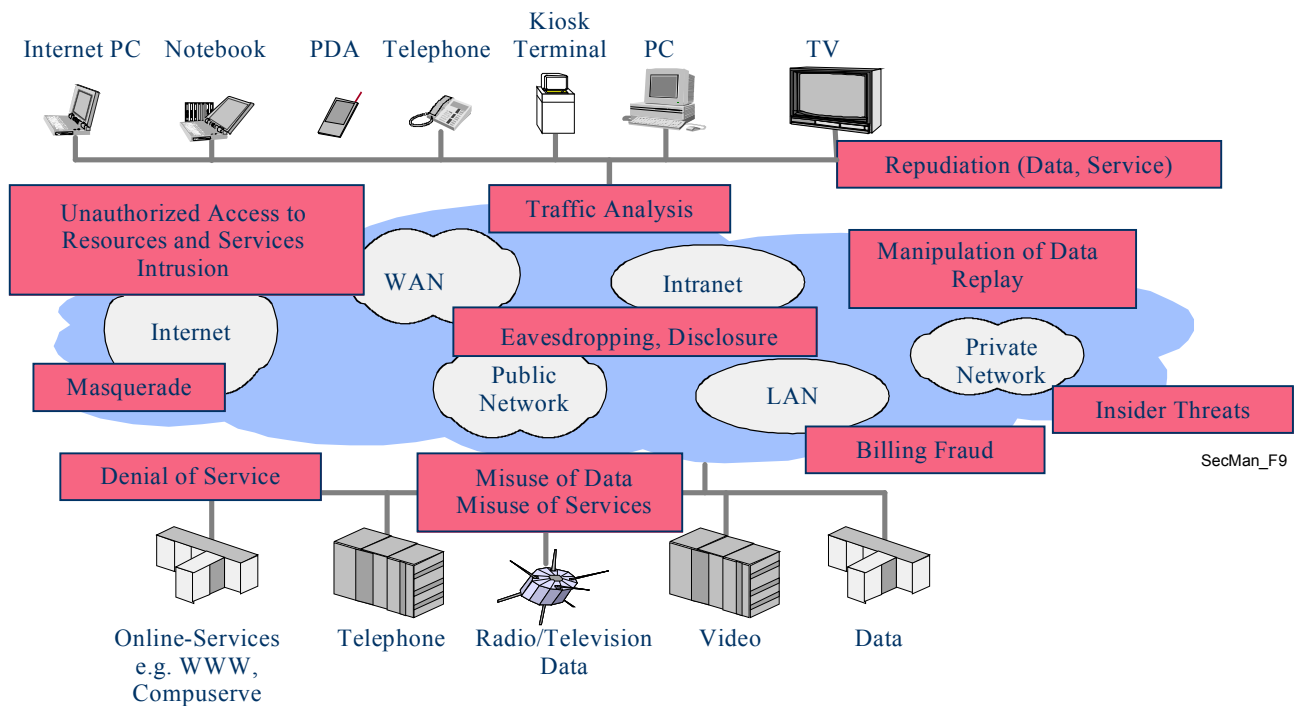
Figure 9
Security threats in Multimedia communications

The main security issues in multimedia communications and IP telephony in general are [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 along.

- 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. Version 3 of H.235 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, 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 optimised 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.
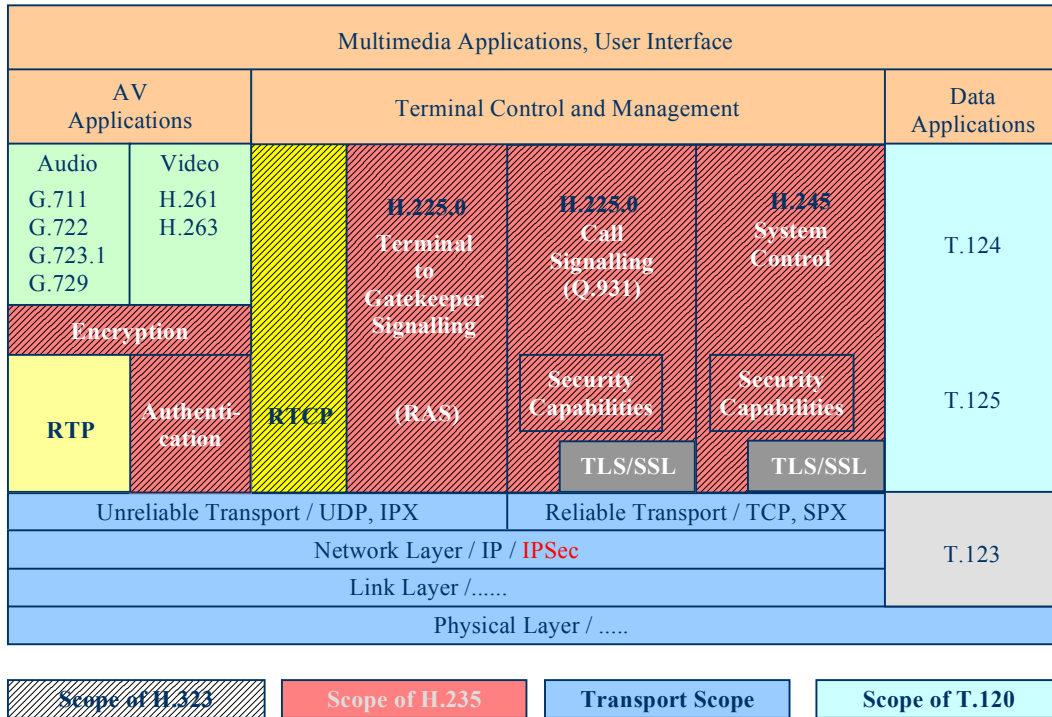
Figure 10
Security in H.323 as provided by H.235 [Euchner]

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.

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 11 illustrates the reference architecture for IPCablecom.
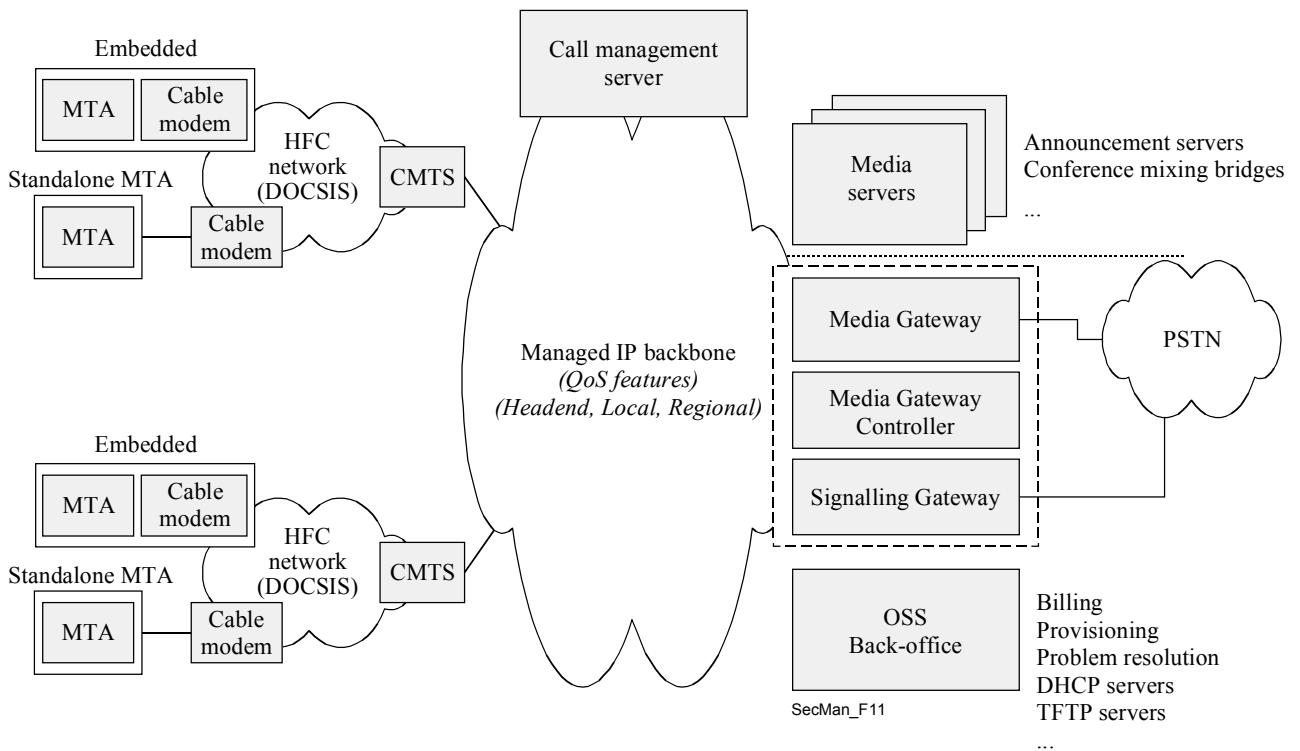
Figure 11
IPCablecom reference architecture [J.165]

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 IPCablecom 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 IPCablecom network. The CMS is a trusted network element that resides on the managed IP portion of the IPCablecom 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 IPCablecom network. For IPCablecom, 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 IPCablecom 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 IPCablecom 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 IPCablecom 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. IPCablecom 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 12 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 12.

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 optional 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 12
IPCablecom security interfaces
(labelled as <label>: <protocol> { <security protocol> / <key management protocol> })

IKE –   IKE with pre-shared keys
IKE+   IKE requires public key certificates
CMS-based KM   Keys randomly generated and distributed by CMS

6.3   Secure Fax Transmission

Facsimile is a very popular application. Initially defined for transmission over the PSTN (ITU-T T.4), then for ISDN (ITU-T 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 T.37 and for real-time (using RTP) using ITU-T 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 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
• Message integrity • Confirmation of message receipt		X		X
• 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 carrier cipher defined in Annex D/T.36. The carrier 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 to exchange the public keys and store them 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 bits 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 13. The management network defines interfaces that determine the exchanges required to perform the OAM&P functions at different levels.
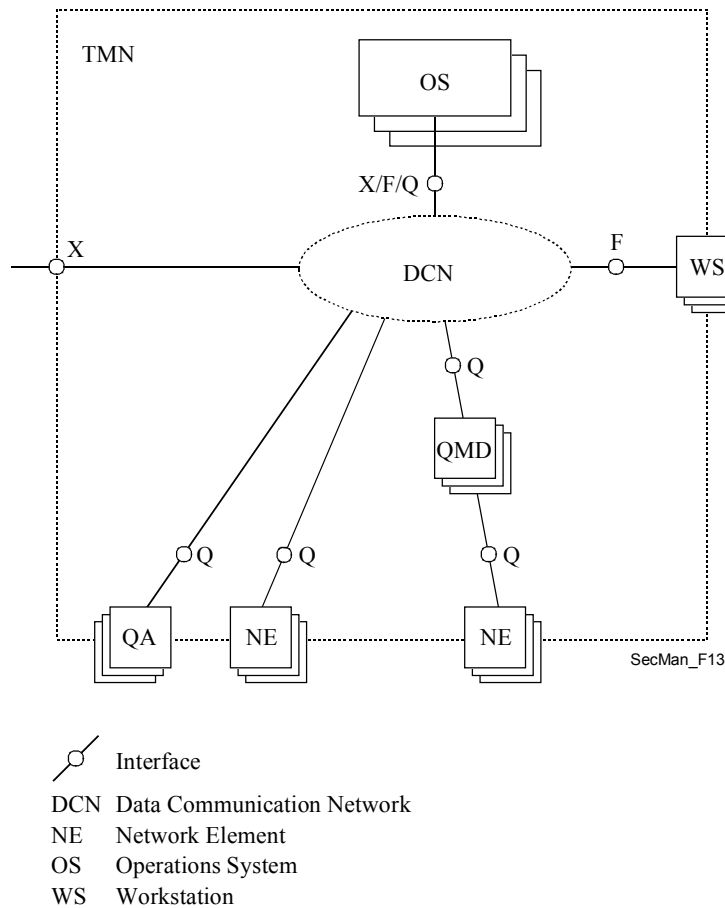
Figure 13
Example of Physical Architecture in M.3010

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 counter measures 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 M.3016, with aspects specific to the X interface being detailed in ITU-T M.3320. The protocol aspects for the different communication layers are specified in ITU-T 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 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. 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 13. It is applied between the Element Management System and the Network Management Systems. The former is used to manage individual network elements and thus 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 14 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 & 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 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 2.5. 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 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 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 15 show initiation of the monitoring management activity either by the home network or by the visited network.
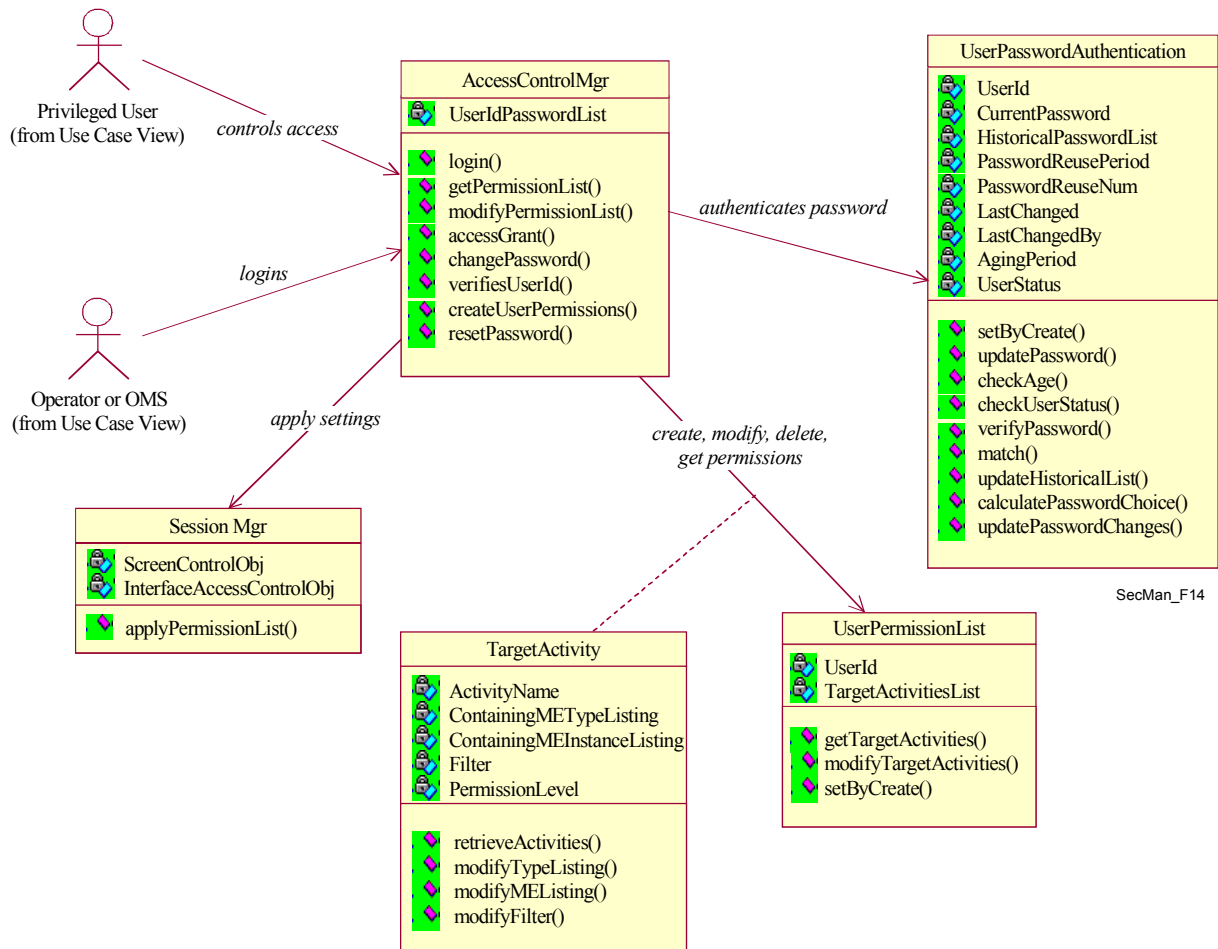
Figure 14
Administering User Privileges in Q.834.3
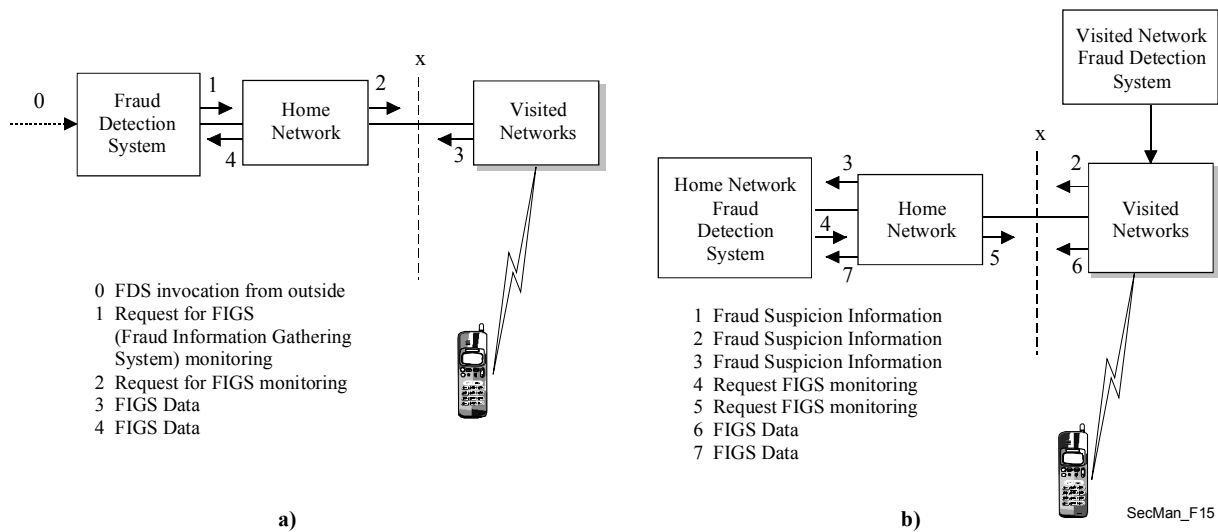
Figure 15
Fraud Management for Wireless Services from Recommendation M.3210.1

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 retrieving the status of the reported troubles. Figure 16 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.
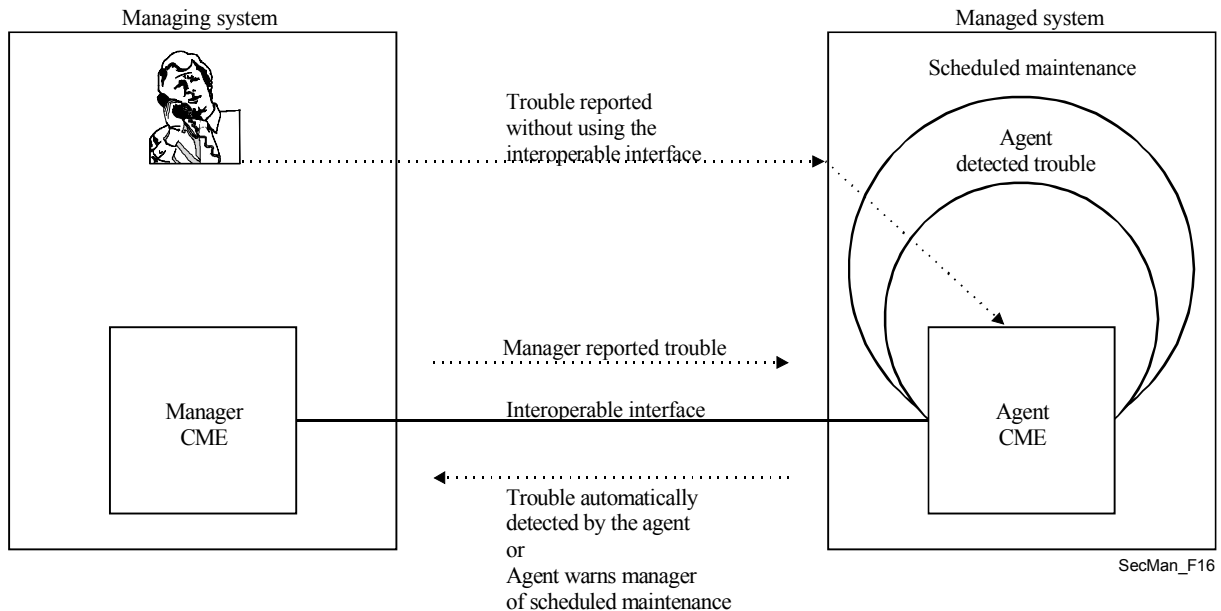
Figure 16
Trouble Management Report Creation defined in ITU-T X.790

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. Even types such as physical security violation are defined in X.736 and alarms resulting from these event types are reported to management systems. This is a management plane activity that can be used to report security violation when unauthorized user gains access for performing provisioning activities in a network element or subscribes users for services or mailboxes. The audit function defined in X.740 describes logging the security violation events and can be applied to all three layers. X.741 defines a model that is very generalized and exhaustive to permit assigning access control privileges to the management activities independent of the targets. The model is rich in features by defining the ability to assign privileges at a fine-grained level of attributes of targets.

ITU-T Recommendation Q.816 has also adopted the generic security services defined in the Object Management Group (OMG) Forum for management activities performed using the CORBA paradigm.

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 recognised 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 authorisation 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 standardised 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 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 standardisation 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 standardisation 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 authorisations 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 authorisation 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 authorised/entitled, it is essential that the management of roles be distributed to competent authorities, rather than try to have it centralised, 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 authorisation 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 authorisation 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 initialisation time, then when specific professionals request actions, such as prescribe or dispense, the authorisation 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 17
The Salford Electronic Prescription System

Figure 17 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 authorisation (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 17, 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 authorised 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 authorised 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 X.509 enable today more generalized and global access to e-prescriptions.

7 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 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 IPCablecom, 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, restoration and disaster recovery being developed in several ITU-T Study Groups will be 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 and by designating a lead study group for security work in ITU-T.

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

Annex A: Security Terminology

The following acronym and terminology list has been extracted from relevant ITU-T Recommendations and other external sources, as accredited below. Also see Annex A.3 for complementary resources.

A.1   Frequently-used Security-related Acronyms

Acronym	Definition
3DES	[H.235] Triple DES
A	[M.3010] Agent
A/M	[M.3010] Agent/manager
AA	[X.509] Attribute Authority
AAA	[X.805] Authentication, Authorization and Accounting
AARL	[X.509] Attribute Authority Revocation List
ACI	[X.810] Access Control Information
ACRL	[X.509] Attribute Certificate Revocation List
AE	[M.3010] Application entity
AES	[H.235] [J.170] Advanced Encryption Standard Algorithm
AH	[J.170] Authentication header is an IPSec security protocol that provides message integrity for complete IP packets, including the IP header.
ASCII	[T.36] American Standard Code for Information Interchange
ASD	[J.170] Application-Specific Data. An application-specific field in the IPSec header that along with the destination IP address provides a unique number for each SA.
ASN.1	[H.680] Abstract Syntax Notation No.1
ASP	[X.805] Application Service Provider
ATM	[X.805] Asynchronous Transfer Mode
ATM	[M.3010] Asynchronous Transfer Mode
AuF	[H.530] Authentication Function, see ITU-T Rec. H.510 [6]
B(n)	[T.36] Base value (n)
BE	[H.530] Border Element, see ITU-T Rec. H.225.0 Annex G [2]
BES	[H.235] Backend Server
BML	[M.3010] Business management layer
B-OSF	[M.3010] Business Management Layer – Operations Systems Function
BPI+	[J.170] Baseline Privacy Interface Plus is the security portion of the J.112 standard that runs on the MAC layer.
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.
CARL	[X.509] Certification Authority Revocation List
CBC	[H.235] [J.170] Cipher Block Chaining
CCA	[H.234] Country Certification Authority
CFB	[H.235] Cipher Feedback Mode
CH$_n$	[H.530] Challenge number n
CM	[J.170] Cable Modem
CME	[X.790] Conformant Management Entity
CMIP	[M.3010] Common management information protocol
CMIS	[X.790] Common Management Information Service

Acronym	Definition
CMISE	[X.790] Common Management Information Service Element
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).
CMTS	[J.112] Cable Modem Termination System
CNM	[X.790] Customer Network Management
CORBA	[SANCHO] Common Object Request Broker Architecture
CRL	[H.235] [X.509] Certificate Revocation List
DCF	[M.3010] Data communication function
DCN	[M.3010] Data communication network
dCRL	[X.509] Delta Certificate Revocation List
DES	[H.235] [J.170] Data Encryption Standard
DH	[H.235] [H.350] Diffie-Hellman
DHCP	[J.170] [X.805] Dynamic Host Configuration Protocol
DIB	[X.509] Directory Information Base
DIT	[X.509] Directory Information Tree
DN	[X.790] Distinguished Name
DNS	[H.235] [J.170] [X.805] Domain Name Server
DOCSIS	[J.170] Data-Over-Cable Service Interface Specification
DoS	[X.805] Denial of Service
DQoS	[J.170] Dynamic Quality of Service
DS-3	[X.805] Digital Signal level 3
DSA	[X.509] Directory System Agent
DSCP	[J.170] DiffServ Code Point. A field in every IP packet that identifies the DiffServ Per Hop Behavior. In IP version 4, the TOS byte is redefined to be the DSCP. In IP version 6, the Traffic Class octet is used as the DSCP. See Annex C.
DSS	[H.235] Digital Signature Standard
DTMF	[H.235] [J.170] Dual-tone Multi Frequency (tones)
DUA	[X.509] Directory User Agent
EARL	[X.509] End-entity Attribute certificate Revocation List
ECB	[H.235] Electronic Code Book Mode
ECC, EC	[H.235] Elliptic Curve Cryptosystem (see section 8.7 of ATM Forum Security Specification Version 1.1). A public-key cryptosystem
EC-GDSA	[H.235] Elliptic curve digital signature with appendix analog of the NIST Digital Signature Algorithm (DSA) (see also [ISO/IEC 15946-2, chapter 5])
ECKAS-DH	[H.235] Elliptic Curve Key Agreement Scheme – Diffie-Hellman. The Diffie-Hellman key agreement scheme using elliptic curve cryptography
EML	[M.3010] Element management layer
EOFB	[H.235] Enhanced OFB mode
E-OSF	[M.3010] Element Management Layer – Operations Systems Function
EP	[H.235] Endpoint
EP$_{ID}$	[H.530] MT endpoint identifier, see ITU-T Rec. H.225.0 [1]
EPRL	[X.509] End-entity Public-key certificate Revocation List
ESH	[T.36] Encrypted and Scrambled plain Hash (24 decimal digits)
ESIM	[T.36] Encrypted Scrambled Integrity Message. A 12-decimal digit number
ESP	[J.170] IPSec Encapsulating Security
ESSK	[T.36] Encrypted Scrambled Secret Key. A 12-decimal digit number

Acronym	Definition
FDS	[M.3210.1] 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
FQDN	[J.170] Fully Qualified Domain Name. Refer to IETF RFC 821 for details.
FTP	[X.805] File Transfer Protocol
FU	[X.790] Functional Unit
GCA	[H.234] General Certification Authority
GDMI	[M.3210.1] Guidelines for the Definition of TMN Management Interface
GDMO	[M.3010] Guidelines for the Definition of Managed Objects
GK	[H.235] [H.510] [H.530] Gatekeeper
GK$_{ID}$	[H.530] Visited Gatekeeper identifier, see ITU-T Rec. H.225.0 [1]
GNM	[X.790] General Network Model
GRJ	[H.530] Gatekeeper Reject
GRQ	[H.530] Gatekeeper Request
GW	[H.235] Gateway
h[*]	[H.234] Result of function h applied to *
H-BE	[H.530] Home BE
HFC	[J.165] Hybrid Fibre/Coaxial (cable)
HFX	[T.30] [T.36] Hawthorne Facsimile Cipher
H-GK	[H.530] Home GK
HKM	[T.30] [T.36] Hawthorne Key Management algorithm
HKMD1	[T.36] Double encryption using the HKM algorithm
HLF	[H.530] Home Location Function
HMAC	[J.170] Hashed Message Authentication Code. A message authentication algorithm, based on either SHA-1 or MD5 hash and defined in RFC 2104.
HMAC-SHA1-96	[H.530] Hashed Message Authentication Code with Secure Hash Algorithm 1
HMAC$_Z$	[H.530] Key Hashed message authentication code/response with shared secret Z, if Z is not shown then the next-hop secret is applied
iCRL	[X.509] Indirect Certificate Revocation List
ICV	[H.235] Integrity Check Value
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).
Idx	[T.36] Last six digits of the facsimile identification (facsimile telephone number) of X
Idy	[T.36] Last six digits of the facsimile identification (facsimile telephone number) of Y
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.

Acronym	Definition
IM	[T.36] Integrity Message used to confirm or deny integrity of the received message (12 decimal digits)
IMT-2000	[M.3210.1] International Mobile Telecommunications 2000
Imy	[T.36] Integrity Message generated by Y to confirm or deny integrity of the received message. A 12?digit decimal number
IN	[M.3010] Intelligent Network
IP	[X.805] Internet Protocol
IPSec	[H.235] [H.530] [J.170] [X.805] Internet Protocol Security.
ISAKMP	[H.235] Internet Security Association Key Management Protocol
ISDN	[M.3010] Integrated services digital network
ISTP	[J.170] Internet Signalling Transport Protocol
IV	[H.235] Initialization Vector
IVR	[J.170] Interactive Voice Response System
K	[H.530] Dynamic session/link key
KDC	[J.170] Key Distribution Center
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.
MAF	[M.3010] Management application function
MAN	[M.3010] Metropolitan Area Network
MAPDU	[X.790] Management Application Protocol Data Unit
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 service
MO	[M.3010] Managed objects
mod n	[T.36] modulo arithmetic using base n
MPS	[H.235] Multiple Payload Stream
MPx	[T.36] Mutual Primitive of X. A 16-decimal digit number, only generable by X. MPx is produced by X using the HKM algorithm with primitives formed from UINx, UCNx, Idx and Idy
Mpy	[T.36] Mutual Primitive of Y
MRP	[H.530] Mobility Routing Proxy
MS	[M.3210.1] Management Services
MSB	[J.170] Most Significant Bit
MT	[H.530] Mobile Terminal, see ITU-T Rec. H.510 [6]
MTA	[J.170] Media Terminal Adapter.
NAT	[H.235] Network Address Translation
NCS	[J.170] Network Call Signalling
NE	[M.3010] [X.790] Network element
NEF	[M.3010] Network element function

Acronym	Definition
NEF-MAF	[M.3010] Network element function – Management application function
NML	[M.3010] [M.3210.1] Network management layer
NOC	[X.790] Network Operations Centre
N-OSF	[M.3010] Network management layer – Operations Systems Function
NTP	[H.530] Network Time Protocol
O	[M.3010] Optional
OA&M	[M.3010] Operations, Administration and Maintenance
OAM&P	[SANCHO] Operations, Administration, Maintenance & Provisioning
OCSP	[H.235] Online Certificate Status Protocol
ODP	[X.810] Open Distributed Processing
OFB	[H.235] Output Feedback Mode
OID	[H.235] [H.530] [J.170] [M.3010] Object Identifier
OS	[M.3010] [X.790] Operations system
OSF	[M.3010] Operations systems function
OSF-MAF	[M.3010] Operations systems function – Management application function
OSI	[M.3010] [X.790] [X.805] [X.810] Open Systems Interconnection
OSS	[J.170] Operations Systems Support. The back-office software used for configuration, performance, fault, accounting, and security management.
OT	[T.36] One-Time key. A 6- to 64-decimal digit number agreed by both users
Otx	[T.36] One-Time key as first used by X in X's registration with Y
Oty	[T.36] One-Time key as first used by Y, when Y initiates Y's registration with X to complete the mutual registration, whether it is different or identical to Otx
P(n)	[T.36] Phase value (n)
PBX	[M.3010] Private branch exchange
PDU	[H.235] Protocol Data Unit
PH	[T.36] Plain Hash of the message (24 decimal digits)
PKCROSS	[J.170] Utilizes PKINIT for establishing the inter-realm keys and associated inter-realm policies to be applied in issuing cross-realm service tickets between realms and domains in support of Intradomain and Interdomain CMS-to-CMS signalling (CMSS).
PKCS	[H.235] [J.170] [X.509] Public Key Cryptography Standards
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.
PMI	[X.509] Privilege Management Infrastructure
PRF	[H.235] Pseudo-Random Function
Primitive	[T.36] A 64-digit composite number formed from UIN and UCN
procREGxy	[T.36] Procedure for registration between X and Y
procSTKxy	[T.36] Procedure for the secure transmission of a secret key from X to Y
PRS	[T.36] Pseudorandom Sequence
PSTN	[SANCHO] Public Switched Telephone Network
PTO	[M.3010] Public Telecommunication Operator
PTR	[X.790] Provider Trouble Report
PVC	[X.805] Permanent Virtual Circuit
PW	[H.530] Mobile User Password
QA	[M.3010] Q adapter
QoS	[SANCHO] Quality of Service

Acronym	Definition
R	[M.3010] Resource
R$_1$	[H.530] Random number
RADIUS	[J.170] Remote Authentication Dial-In User Service
RBAC	[X.509] Role-Based Access Control
RC4	[J.170] A variable key length stream cipher offered in the ciphersuite, used to encrypt the media traffic in IPCablecom.
RCN	[T.36] Registered Crypt Number. A 16-decimal digit number
RDN	[X.790] Relative Distinguished Name
RIP	[H.530] Request in Progress
RKS	[J.170] Record Keeping Server. The device which collects and correlates the various Event Messages.
RNCn	[T.36] Non-secret random number associated with an SCn. A 4-decimal digit number
RNIM	[T.36] Non-secret random number associated with an IM. A 4-decimal digit number
RNK	[T.36] Non-secret random number used to provide variation of the primitives generated from MPx when encrypting an SK. A 4?decimal digit number
RNSRn	[T.36] Non-secret random number associated with an SRn. A 4-decimal digit number
RNSSn	[T.36] Non-secret random number associated with an SSn. A 4-decimal digit number
RRJ	[H.530] Registration Reject
RRQ	[H.530] Registration Request
RSA	[H.235] [T.30] [T.36] Rivest, Shamir and Adleman (public key algorithm)
RSVP	[J.170] Resource Reservation Protocol
RTCP	[H.235] [J.170] Realtime Transport Control Protocol
RTO	[J.170] Retransmission Timeout
RTP	[H.225.0] [H.235] [J.170] Real time protocol
SA	[J.170] Security Association.
SAFER K-64	[T.36] The Secure And Fast Encryption Routine with 64-bit key algorithm was introduced by J. L. Massey in 1993 and is an iterated blockcipher with 64-bit plaintext and ciphertext blocks (in A. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997).
SCn	[T.36] Secret Challenge key, number n. A 12-decimal digit number
SDH	[M.3010] Synchronous Digital Hierarchy
SDP	[J.170] Session Description Protocol.
SDU	[H.235] Service Data Unit
SG	[J.170] A Signalling Gateway is a signalling agent that receives/sends SCN native signalling at the edge of the IP network. In particular the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.
SH	[T.36] Scrambled plain Hash (24 decimal digits)
SHA1	[H.235] Secure Hash Algorithm No.1
SI	[X.810] Security Information
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.
SIP+	[J.170] Session Initiation Protocol Plus. An extension to SIP.
SK	[T.36] A Secret Key which may be an SCn, SRn, SSn, etc. A 12-decimal digit number
SMAPM	[X.790] System Management Application Protocol Machine
SMK	[M.3010] Shared management knowledge
SML	[M.3010] [M.3210.1] Service management layer
SMO	[X.790] Systems Management Overview
SMTP	[X.805] Simple Mail Transfer Protocol

Acronym	Definition
SNMP	[J.170] [X.805] Simple Network Management Protocol
SNTP	[H.530] Simple Network Time Protocol
SOA	[X.509] Source of Authority
SONET	[X.805] Synchronous Optical Network
S-OSF	[M.3010] Service management layer – Operations Systems Function
SRn	[T.36] Secret Response key, number n. A 12-decimal digit number
SRTP	[H.225.0] [H.235] Secure Real Time Protocol
SS	[T.36] Secret Session key used with the HFX40-I integrity algorithm (12 decimal digits)
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.
SSK	[T.36] Scrambled Secret Key. A 12-decimal digit number
SSL	[H.235] [X.805] Secure Socket Layer
SSn	[T.36] Secret Session key, number n, to be used with the carrier cipher and/or hash. A 12-decimal digit number
SSx	[T.36] Secret Session key generated by X to be used with the HFX40 cipher algorithm (12 decimal digits)
TCAP	[J.170] Transaction Capabilities Application Protocol. A protocol within the SS7 stack that is used for performing remote database transactions with a Signalling Control Point.
TD	[J.170] Timeout for Disconnect
TF	[M.3010] Transformation Function
TF-MAF	[M.3010] Transformation Function – Management application function
TFTP	[J.170] Trivial File Transfer Protocol
TGS	[J.170] The Ticket Granting Server is a sub-system of the KDC used to grant Kerberos tickets.
TKx	[T.36] Transfer Key, an encryption of MPx generated by X. A 16-decimal digit number
TLS	[H.235] Transport Level Security
TMN	[M.3010] [M.3210.1] [X.790] Telecommunications management network
T_n	[H.530] Timestamp number n
TSAP	[H.235] Transport Service Access Point
TSP	[X.790] Telecommunication Service Priority
TTP	[X.810] Trusted Third Party
TTR	[X.790] Telecommunications Trouble Report
UCN	[T.36] Unique Crypt Number, e.g. UCNx, UCNy. A 16-decimal digit number known only to the system
UDP	[J.170] User Datagram Protocol.
UIN	[T.36] Unique Identity Number, e.g. UINx, UINy, signifying a 48-decimal digit number known only to the system
V-BE	[H.530] Visited BE
V-GK	[H.530] Visited GK
VLF	[H.530] Visitor Location Function
VoIP	[X.805] Voice over IP
VPN	[X.805] Virtual Private Network
W	[H.530] Compound value with arithmetic combination of Diffie-Hellman half-keys
WSF	[M.3010] Workstation function
WSSF	[M.3010] Workstation Support function
WT	[H.530] Mobility ClearToken
X	[T.36] Name of one entity

Acronym	Definition
x	[T.36] Suffix identifying ownership or generation by X
X<<Y>>	[H.234] The certificate of Y generated by X
XOR'd	[T.36] [H.235] Exclusively OR'd
Xp	[H.234] Public RSA key of entity X
Xp[*]	[H.234] En/decryption of [*] with Xp. In the case of RSA this is performed by exponentiation
Xs	[H.234] Secret RSA key of entity X
Xs[*]	[H.234] En/decryption of [*] with Xs. In the case of RSA this is performed by exponentiation
XT	[H.530] CryptoToken for MT authentication
Y	[T.36] Name of a second entity
y	[T.36] Suffix identifying ownership or generation by Y
ZZ	[H.530] Shared secret/password of the mobile user, which is shared with the corresponding AuF
ZZMT	[H.530] Shared secret of the mobile terminal MT, which is shared with the corresponding AuF
ZZ$_n$	[H.530] Shared-secret number n

A.2 Frequently-used Security-related Definitions

Term	Definition
Access control	[H.235] [X.800] The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner (X.800). [J.170] 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.805] 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. In addition, Role-Based Access Control (RBAC) provides different access levels to guarantee that individuals and devices can only gain access to and perform operations on network elements, stored information, and information flows that they are authorized for.
Access control list	[X.800] A list of entities, together with their access rights, which are authorized to have access to a resource.
Access Node	[J.170] As used in this document, an Access Node is a layer two termination device that terminates the network end of the CM connection. It is technology specific. In J.112 Annex A it is called the INA while in Annex B it is the CMTS
Accountability	[X.800] The property that ensures that the actions of an entity may be traced uniquely to the entity.
Active threat	[X.800] The threat of a deliberate unauthorized change to the state of the system. (Note – Examples of security-relevant active threats may be: modification of messages, replay of messages, insertion of spurious messages, masquerading as an authorized entity and denial of service.)
Agent	[X.790] As defined in Recommendation X.701, the Systems Management Overview (SMO), but with the following restriction. With respect to a particular telecommunications service (or resource) instance, it shall be possible to manage the service with one system playing the manager role, and the other playing the agent role.
Alias	[X.790] Another name, besides the object identifier, by which a trouble report may be known, referenced or identified (usually by the customer).

Term	Definition
Application association	[X.790] A co-operative relationship between two application entities, formed by their exchange of application protocol control information through their use of presentation services.
Application context	[X.790] An explicitly identified set of application service elements, related options, and any other necessary information for the interworking of application entities on an application association.
Application entity	[X.790] The aspects of an application process pertinent to OSI.
Associated alarms	[X.790] Alarms directly related to a given identified trouble.
Asymmetric cryptographic algorithm	[X.810] An algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ. (NOTE – With some asymmetric cryptographic algorithms, decipherment of ciphertext or the generation of a digital signature requires the use of more than one private key.)
Attack	[H.235] 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.
Attribute	[X.790] Information concerning a managed object used to describe (either in part or in whole) that managed object. This information consists of an attribute type and its corresponding attribute value (single-valued) or values (multi-valued).
Attribute Authority	[X.509] An AA is an authority which assigns privileges by issuing attribute certificates.
Attribute Authority Revocation List	[X.509] An AARL is a revocation list containing a list of references to attribute certificates issued to AAs that are no longer considered valid by the issuing authority.
Attribute certificate	[X.509] A data structure, digitally signed by an Attribute Authority, that binds some attribute values with identification information about its holder.
Attribute Certificate Revocation List	[X.509] An ACRL is a revocation list containing a list of references to attribute certificates that are no longer considered valid by the issuing authority.
Attribute type	[X.790] The component of an attribute that indicates the class of information given by that attribute.
Attribute value	[X.790] A particular instance of the class of information indicated by an attribute type.
Audio Server	[J.170] An Audio Server plays informational announcements in IPCablecom network. Media announcements are needed for communications that do not complete and to provide enhanced information services to the user. The component parts of Audio Server services are Media Players and Media Player Controllers.
Audit	[X.800] See security audit.
Audit trail	[X.800] See security audit trail.

Term	Definition
Authentication	[H.235] [X.800] [X.811] The provision of assurance of the claimed identity of an entity See data origin authentication, and peer entity authentication. (Note – The term "authentication" is not used in connection with data integrity; the term "data integrity" is used instead). [J.170] The process of verifying the claimed identity of an entity to another entity. [X.805] 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.
Authentication exchange	[X.800] A mechanism intended to ensure the identity of an entity by means of information exchange.
Authentication function	[H.530] The AuF is the security functional entity in the home domain that maintains security relationship with the subscribed mobile users and the subscribed mobile terminals.
Authentication information	[X.800] Information used to establish the validity of a claimed identity.
Authentication token; (token)	[X.509] Information conveyed during a strong authentication exchange, which can be used to authenticate its sender.
Authenticity	[J.170] The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity that claims to have given the information.
Authority	[X.509] An entity, responsible for the issuance of certificates. Two types are defined in this Specification; certification authority which issues public-key certificates and attribute authority which issues attribute certificates.
Authority certificate	[X.509] A certificate issued to an authority (e.g. either to a certification authority or to an attribute authority).
Authorization	[H.235] The granting of permission on the basis of authenticated identification. [J.170] The act of giving access to a service or device if one has the permission to have the access. [X.800] The granting of rights, which includes the granting of access based on access rights.
Availability	[X.800] The property of being accessible and useable upon demand by an authorized entity.
Availability	[X.805] 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.
Base CRL	[X.509] A CRL that is used as the foundation in the generation of a dCRL.
Business management layer	[M.3010] A management layer responsible for the total enterprise and not subject to standardization.
CA-certificate	[X.509] A certificate for one CA issued by another CA.
Cancelled	[X.790] A manager can request the agent to "cancel" a trouble report. The manager wants to abort this trouble report (either because it was entered in error or because there is no longer any trouble condition). Under certain conditions (e.g. the trouble has not been dispatched or tested), the agent will "cancel" the trouble report by updating its status to "closed-out by customer request." "Cancelling" a trouble report may also have business ramifications beyond the scope of this Recommendation (e.g. whether the customer must pay for the trouble report).

Term	Definition
Capability	[X.800] A token used as an identifier for a resource such that possession of the token confers access rights for the resource.
Certificate	[H.235] 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 (X.810). In this Recommendation the term refers to "public key" 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.
Certificate policy	[X.509] 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.
Certificate Revocation List	[X.509] A CRL is 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.
Certificate serial number	[X.509] An integer value, unique within the issuing authority, which is unambiguously associated with a certificate issued by that CA.
Certificate user	[X.509] An entity that needs to know, with certainty, the public key of another entity.
Certificate validation	[X.509] The process of ensuring that a certificate was valid at a given time, including possibly the construction and processing of a certification path, and ensuring that all certificates in that path were valid (i.e. were not expired or revoked) at that given time.
Certificate-using system	[X.509] An implementation of those functions defined in this Directory Specification that are used by a certificate-user.
Certification Authority	[X.509] A CA is an authority trusted by one or more users to create and assign public-key certificates. Optionally the certification authority may create the users' keys. [X.810] 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.
Certification Authority Revocation List	[X.509] A CARL is a revocation list containing a list of public-key certificates issued to certification authorities, that are no longer considered valid by the certificate issuer.
Certification path	[X.509] An ordered sequence of certificates of objects in the DIT 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.
Channel	[X.800] An information transfer path.
Cipher	[H.235] A cryptographic algorithm, a mathematical transform. [J.170] An algorithm that transforms data between plaintext and ciphertext.
Ciphersuite	[J.170] A set, which must contain both an encryption algorithm and a message authentication algorithm (e.g., a MAC or an HMAC). In general, it may also contain a key management algorithm, which does not apply in the context of IPCablecom.
Ciphertext	[X.800] Data produced through the use of encipherment. The semantic content of the resulting data is not available. (Note – Ciphertext may itself be input to encipherment, such that super-enciphered output is produced.)

Term	Definition
Clearing trouble reports	[X.790] An assertion by an agent that actions which are identified in the trouble report or the repair activity object instances have been satisfactorily performed to resolve the trouble, or that such actions are no longer necessary, such that in either case the trouble report is a candidate for closure.
Cleartext	[X.800] Intelligible data, the semantic content of which is available.
Client	[X.790] User of a service provided by a system or a network.
Closed-out	[X.790] A trouble report is considered "closed-out" when the agent determines that the reported trouble has either been cleared or no longer exists, and the agent updates the trouble report status to indicate the trouble report is "closed-out". Only an agent can change the trouble report status to "closedOut". The status of a trouble report might change to "closedOutByCustReq" as a result of a request to cancel the trouble report from the manager.
Closing trouble reports	[X.790] An assertion by an Agent that the trouble is resolved such that the cleared trouble report may only be processed further to generate a trouble history record and/or be deleted.
Communication	[X.805] The Communication 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).
Conditionally trusted entity	[X.810] An entity that is trusted in the context of a security policy, but which cannot violate the security policy without being detected.
Confidentiality	[H.235] The property that prevents disclosure of information to unauthorized individuals, entities, or processes. [J.170] A way to ensure that information is not disclosed to any one other then the intended parties. Information is encrypted to provide confidentiality. Also known as privacy. [X.800] The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Conformant management entity	[X.790] A real open system which supports the interoperable interface defined in this Recommendation.
Contact	[X.790] A person who can provide additional information about the trouble on behalf of the manager or the agent.
Credential	[H.530] In this Recommendation, a credential [such as HMACZZ(GKID) or HMACZZ(W)] is understood as some piece of data to which the AuF cryptographically has applied its shared secret ZZ that it shares with the mobile user. The credential is transferred to prove authorization and timeliness in the authorization check.
Credentials	[X.800] Data that is transferred to establish the claimed identity of an entity.
CRL distribution point	[X.509] A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs.
Cryptanalysis	[J.170] The process of recovering the plaintext of a message or the encryption key without access to the key. [X.800] The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext.
Cryptographic algorithm	[H.235] Mathematical function that computes a result from one or several input values.

Term	Definition
Cryptographic chaining	[X.810] 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.
Cryptographic checkvalue	[X.800] Information which is derived by performing a cryptographic transformation (see cryptography) on the data unit. (Note – 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.)
Cryptographic system, cryptosystem	[X.509] A Cryptographic system, or cryptosystem, is a collection of transformations from plain text into ciphertext and vice versa, the particular transformation(s) to be used being selected by keys. A mathematical algorithm normally defines the transformations.
Cryptography	[X.800] The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. (Note – Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or method is cryptanalysis.)
Customer	[X.790] The customer is a user of telecommunications services provided by a service provider. Specifically, in the context of this Recommendation, the customer is a user who chooses to use the OS (Operations System) -to-OS OSI interface for network management across jurisdictions in order to achieve control of the telecommunications services (or resources) being used. The customer (or customer representative) acts in the manager role. There is no requirement that the interface be confined to cases where there is a traditional telecommunication service customer to service provider relationship between the parties. Two telecommunications service providers (carriers) may use this interface to exchange trouble reports in situations where their networks interwork in order to provide service to an end user. In that case, the Customer role may change from situation to situation. However, in any particular situation, one carrier will be the customer and will act in the manager role, while the other will be the supplier and will act in the agent role.
Data communication network	[M.3010] A communication network within a TMN or between TMNs which supports the data communication function (DCF).
Data confidentiality	[X.509] This service can be used to provide for protection of data from unauthorized disclosure. The authentication framework supports the data confidentiality service. It can be used to protect against data interception. [X.805] 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.
Data integrity	[X.800] The property that data has not been altered or destroyed in an unauthorized manner. [X.805] 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.
Data origin authentication	[X.800] The corroboration that the source of data received is as claimed.
Decipherment	[X.800] The reversal of a corresponding reversible encipherment.
Decryption	[X.800] See decipherment.

Term	Definition
Defer	[X.790] To postpone work on, or set aside, a trouble report until such time as when appropriate conditions are met and it can be progressed further.
Delegation	[X.509] Conveyance of privilege from one entity that holds such privilege, to another entity.
Delegation path	[X.509] An ordered sequence of certificates which, together with authentication of a privilege asserter's identity can be processed to verify the authenticity of a privilege asserter's privilege.
Delta-CRL	[X.509] A dCRL is a partial revocation list that only contains entries for certificates that have had their revocation status changed since the issuance of the referenced base CRL.
Denial of service	[X.800] The prevention of authorized access to resources or the delaying of time-critical operations.
Digital fingerprint	[X.810] 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.
Digital signature	[X.800] 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.
Distinguishing identifier	[X.810] Data that uniquely identifies an entity.
Downstream	[J.170] The direction from the head-end toward the subscriber location.
Element management layer	[M.3010] A management layer which is responsible for management of network elements on an individual or collective basis.
Encipherment	[H.235] 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 ciphertext is transformed to plaintext. [X.800] The cryptographic transformation of data (see cryptography) to produce ciphertext. (Note – Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed.)
Encryption	[J.170] A method used to translate information in plaintext into ciphertext. [X.800] See encipherment.
End entity	[X.509] A certificate subject that uses its private key for purposes other than signing certificates or an entity that is a relying party.
End-entity Attribute Certificate Revocation List	[X.509] An EARL is A revocation list containing a list of attribute certificates issued to holders, that are not also AAs, that are no longer considered valid by the certificate issuer.
End-entity Public-key Certificate Revocation List	[X.509] An EPRL is a revocation list containing a list of public-key certificates issued to subjects, that are not also CAs, that are no longer considered valid by the certificate issuer.
Endpoint	[J.170] A Terminal, Gateway or MCU.
End-to-end encipherment	[X.800] 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.)

Term	Definition
Environmental variables	[X.509] Those aspects of policy required for an authorization decision, that are not contained within static structures, but are available through some local means to a privilege verifier (e.g. time of day or current account balance).
Escalating a trouble report	[X.790] Identifying a trouble report which is to receive urgent and immediate supervisory attention to resolve the trouble.
Event	[X.790] An instantaneous occurrence that changes the global status of an object. This status change may be persistent or temporary, thus allowing for surveillance, monitoring, and performance measurement functionality, etc. Events may or may not generate reports; they may be spontaneous or planned; they may trigger other events or may be triggered by one or more other events.
Event Message	[J.170] Message capturing a single portion of a connection.
F interface	[M.3010] An interface applied at f reference points.
F reference points	[M.3010] A reference point that is located between the workstation function block (WSF) and the operations systems function block (OSF).
Fault management	[X.790] Fault Management consists of a set of functions that enable the detection, isolation, and correction of abnormal operation of the telecommunications network and its environment.
Full CRL	[X.509] A complete revocation list that contains entries for all certificates that have been revoked for the given scope.
Function block	[M.3010] The smallest (deployable) unit of TMN management functionality that is subject to standardization.
G reference points	[M.3010] A reference point located outside the TMN between the human users and the workstation function block (WSF). It is not considered to be part of the TMN even though it conveys TMN information.
Gateway	[J.170] Devices bridging between the IPCablecom Voice Communication world and the PSTN. Examples are the Media Gateway which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signalling Gateway which sends and receives circuit switched network signalling to the edge of the IPCablecom network.
Hash function	[X.509] A (mathematical) function which maps values from a large (possibly very large) domain into a smaller range. A "good" hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range. [X.810] A (mathematical) function that maps values from a (possibly very) large set of values into a smaller range of values.
Header	[J.170] Protocol control information located at the beginning of a protocol data unit.
Holder	[X.509] An entity to whom some privilege has been delegated either directly from the Source of Authority or indirectly through another Attribute Authority.
Home border element	[H.530] The H-BE is a border element (BE) placed within the home domain.
Identity-based security policy	[X.800] 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.
Indirect CRL	[X.509] An iCRL is a revocation list that at least contains revocation information about certificates issued by authorities other than that which issued this CRL.

Term	Definition
Integrity	[H.235] The property that data has not been altered in an unauthorized manner. [J.170] A way to ensure that information is not modified except by those who are authorized to do so. [X.800] See data integrity.
Interface	[M.3010] An architectural concept that provides interconnection between physical blocks at reference points.
Jurisdiction	[X.790] This refers to the functional separation of telecommunications networks. A jurisdiction is one of the following four types: a) Local Exchange Carrier Network; b) Interexchange Carrier Network; c) End User Network; and d) Some combination of the above.
Kerberos	[J.170] A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.
Key	[J.170] A mathematical value input into the selected cryptographic algorithm. [X.800] A sequence of symbols that controls the operations of encipherment and decipherment.
Key agreement	[X.509] A method for negotiating a key value on-line without transferring the key, even in an encrypted form, e.g. the Diffie-Hellman technique (see ISO/IEC 11770-1 for more information on key agreement mechanisms).
Key Exchange	[J.170] The swapping of public keys between entities to be used to encrypt communication between the entities.
Key management	[H.235] [X.800] The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.
Key-Management	[J.170] The process of distributing shared symmetric keys needed to run a security protocol.
Link-by-link encipherment	[X.800] The individual application of encipherment to data on each link of a communications system. See also end-to-end encipherment. (Note – The implication of link-by-link encipherment is that data will be in cleartext form in relay entities.)
Logical layered architecture	[M.3010] An architectural concept that organizes the management functions into a grouping of management layers and describes the relationship between the layers.
M reference points	[M.3010] A reference point located outside the TMN between a Q adapter function block (QAF) and managed entities that do not conform to TMN Recommendations.
Managed resource	[M.3010] The abstraction of those aspects of a telecommunication resource (logical or physical) required for telecommunications management.
Management application function	[M.3010] A function that represents (part of) the functionality of one or more management services.
Management domain	[M.3010] A set of managed resources subject to a common management policy.
Management function	[M.3010] The smallest part of a management service as perceived by the user of the service.
Management function set	[M.3010] TMN management function set is a grouping of TMN management functions that contextually belong together, i.e. they are related to a specific management capability (e.g. alarm reporting functions, traffic management control). The TMN management function set is the smallest reusable item of functional specification. The TMN management function set must be considered as a whole. It is similar to the requirements part of the OSI SMF (system management function).

Term	Definition
Management service	[M.3010] A management service is an offering fulfilling specific telecommunications management needs.
Management layer	[M.3010] An architectural concept that reflects particular aspects of management and implies a clustering of management information supporting that aspect.
Manager	[X.790] As defined in Recommendation X.701, the Systems Management Overview (SMO), but with the following restriction. With respect to a particular telecommunications service (or resource) instance, it shall be possible to manage the service with one system playing the manager role, and the other playing the agent role.
Manipulation detection	[X.800] A mechanism which is used to detect whether a data unit has been modified (either accidentally or intentionally).
Masquerade	[X.800] The pretence by an entity to be a different entity.
Media stream	[H.235] A media stream can be of type audio, video or data or a combination of any of them. Media stream data conveys user or application data (payload) but no control data.
Mobility routing proxy	[H.530] The MRP is an optional functional entity that acts as an intermediate functional entity, terminating the security association of a hop-by-hop link.
Network element	[M.3010] An architectural concept that represents telecommunication equipment (or groups/parts of telecommunication equipment) and supports equipments or any item or groups of items considered belonging to the telecommunications environment that performs network element functions (NEFs).
Network element function	[M.3010] A function block which represents the telecommunication functions and communicates with the TMN OSF function block for the purpose of being monitored and/or controlled.
Network management layer	[M.3010] A management layer responsible for the management, including coordination of activity, of a network view.
Non-repudiation	[H.235] Protection from denial by one of the entities involved in a communication of having participated in all or part of the communication. [J.170] The ability to prevent a sender from denying later that he or she sent a message or performed an action. [X.805] 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.
Notarization	[X.800] 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.
Object method	[X.509] An action that can be invoked on a resource (e.g. a file system may have read, write and execute object methods).
One-way function	[X.509] A (mathematical) function f which is easy to compute, but which for a general value y in the range, it is computationally difficult to find a value x in the domain such that $f(x) = y$. There may be a few values y for which finding x is not computationally difficult. [X.810] A (mathematical) function that is easy to compute but, when knowing a result, it is computationally infeasible to find any of the values that may have been supplied to obtain it.

Term	Definition
One-way hash function	[X.810] A (mathematical) function that is both a one-way function and a hash function.
Operations system	[M.3010] A physical block which performs operations systems functions (OSFs).
Operations systems function	[M.3010] A function block that processes information related to the telecommunications management for the purpose of monitoring/coordinating and/or controlling telecommunication functions including management functions (i.e. the TMN itself).
Outage	[X.790] Unavailability of a service or resource.
Passive threat	[X.800] The threat of unauthorized disclosure of information without changing the state of the system.
Password	[H.530] [X.800] Confidential authentication information, usually composed of a string of characters.
Peer-entity authentication	[X.800] The corroboration that a peer entity in an association is the one claimed.
Perceived severity	[X.790] The seriousness of the problem as seen by the person reporting the trouble.
Physical block	[M.3010] An architectural concept representing a realization of one or more function blocks.
Physical security	[X.800] The measures used to provide physical protection of resources against deliberate and accidental threats.
Policy	[X.800] See security policy.
Policy mapping	[X.509] Recognizing that, when a CA in one domain certifies a CA in another domain, a particular certificate policy in the second domain may be considered by the authority of the first domain to be equivalent (but not necessarily identical in all respects) to a particular certificate policy in the first domain.
Priority	[X.790] The degree of urgency with which the manager requires resolution of the problem.
Privacy	[H.235] 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. [J.170] A way to ensure that information is not disclosed to any one other then the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality. [X.800] The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. (Note – Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security). [X.805] 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 web-sites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a Service Provider network.
Private channel	[H.235] For this Recommendation, a private channel is one that is a result of prior negotiation on a secure channel. In this context it may be used to handle media streams.
Private Key	[J.170] The key used in public key cryptography that belongs to an individual entity and must be kept secret. [X.810] A key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity).

Term	Definition
Private key; Secret key (deprecated)	[X.509] (In a public key cryptosystem) that key of a user's key pair which is known only by that user.
Privilege	[X.509] An attribute or property assigned to an entity by an authority.
Privilege asserter	[X.509] A privilege holder using their attribute certificate or public-key certificate to assert privilege.
Privilege Management Infrastructure (PMI)	[X.509] The infrastructure able to support the management of privileges in support of a comprehensive authorization service and in relationship with a Public Key Infrastructure.
Privilege policy	[X.509] The policy that outlines conditions for privilege verifiers to provide/perform sensitive services to/for qualified privilege asserters. Privilege policy relates attributes associated with the service as well as attributes associated with privilege asserters.
Privilege verifier	[X.509] An entity verifying certificates against a privilege policy.
Proxy	[J.170] A facility that indirectly provides some service or acts as a representative in delivering information thereby eliminating the need for a host to support the service.
Public Key	[J.170] 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.810] A key that is used with an asymmetric cryptographic algorithm and that can be made publicly available.
Public Key Certificate	[J.170] A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
Public key cryptography	[H.235] An encryption system utilizing asymmetric keys (for encryption/decryption) in which the keys have a mathematical relationship to each other – which cannot be reasonably calculated. [J.170] A procedure that uses a pair of keys, a public key and a private key for encryption and decryption, also known as an asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A user's private key is kept secret and is the only key that can decrypt messages sent encrypted by the user's public key.
Public Key Infrastructure (PKI)	[X.509] The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.
Public Telecommunication Operator (PTO)	[M.3010] Is used for conciseness to include telecommunication administrations, recognized operating agencies, private (customer and third party) administrations and/or other organizations that operate or use a Telecommunications Management Network (TMN).
Public-key	[X.509] (In a public key cryptosystem) that key of a user's key pair which is publicly known.
Public-key certificate	[X.509] The public key of a user, together with some other information, rendered unforgeable by enciperment with the private key of the certification authority which issued it.
Q adapter	[M.3010] A physical block that is characterized by a contained Q adapter function block and which connects NE-like or OS-like physical entities with non-TMN compatible interfaces (at m reference points) to Q interfaces.
Q interface	[M.3010] An interface applied at q reference points.

Term	Definition
Q reference points	[M.3010] A reference point located between NEF and OSF, between QAF and OSF, and between OSF and OSF.
Reference point	[M.3010] An architectural concept used to delineate management function blocks and which defines a service boundary between two management function blocks.
Relying party	[X.509] A user or agent that relies on the data in a certificate in making decisions.
Repudiation	[X.800] Denial by one of the entities involved in a communication of having participated in all or part of the communication.
Revocation certificate	[X.810] A security certificate issued by a security authority to indicate that a particular security certificate has been revoked.
Revocation list certificate	[X.810] A security certificate that identifies a list of security certificates that have been revoked.
Role assignment certificate	[X.509] A certificate that contains the role attribute, assigning one or more roles to the certificate subject/holder.
Role specification certificate	[X.509] A certificate that contains the assignment of privileges to a role.
Root Private Key	[J.170] The private signing key of the highest-level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.
Routing control	[X.800] The application of rules during the process of routing so as to chose or avoid specific networks, links or relays.
Rule-based security policy	[X.800] 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.
Seal	[X.810] A cryptographic check value 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 sealed. (NOTE – 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.)
Secret key	[X.810] A key that is used with a symmetric cryptographic algorithm. Possession of a secret key is restricted (usually to two entities).
Secure interaction rules	[X.810] Security policy rules that regulate interactions between security domains.
Security administrator	[X.810] A person who is responsible for the definition or enforcement of one or more parts of a security policy.
Security audit	[X.800] 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.
Security audit trail	[X.800] Data collected and potentially used to facilitate a security audit.
Security authority	[X.810] An entity that is responsible for the definition, implementation or enforcement of security policy.

Term	Definition
Security certificate	[X.810] A set of security-relevant data issued by a security authority or trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data. (NOTE – All certificates are deemed to be security certificates (see the relevant definitions in ISO 7498-2). The term security certificate is adopted in order to avoid terminology conflicts with ITU-T Rec. X.509	ISO/IEC 9594-8; i.e. the directory authentication standard.)
Security certificate chain	[X.810] An ordered sequence of security certificates, in which the first security certificate contains security-relevant information, and each subsequent security certificate contains security information which can be used in the verification of previous security certificates.
Security domain	[X.810] A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain.
Security domain authority	[X.810] A security authority that is responsible for the implementation of a security policy for a security domain.
Security information	[X.810] Information needed to implement security services.
Security label	[X.800] The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource. (Note – The marking and/or binding may be explicit or implicit.)
Security policy	[X.509] The set of rules laid down by the security authority governing the use and provision of security services and facilities. [X.800] The set of criteria for the provision of security services (see also identity-based and rule-based security policy). (Note – A complete security policy will necessarily address many concerns which are outside of the scope of OSI.)
Security policy rules	[X.810] A representation of a security policy for a security domain within a real system.
Security profile	[H.235] A (sub)set of consistent, interoperable procedures and features out of ITU?T H.235 useful for securing H.323 multimedia communication among the involved entities in a specific scenario.
Security recovery	[X.810] Actions that are taken and procedures that are carried out when a violation of security is either detected or suspected to have taken place.
Security service	[X.800] A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.
Security token	[X.810] 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.
Selective field protection	[X.800] The protection of specific fields within a message which is to be transmitted.
Sensitivity	[X.509] Characteristic of a resource that implies its value or importance. [X.800] The characteristic of a resource which implies its value or importance, and may include its vulnerability.
Service	[X.790] This term represents telecommunications capabilities that the customer buys or leases from a service provider. Service is an abstraction of the network-element-oriented or equipment-oriented view. Identical services can be provided by different network elements, and different services can be provided by the same network elements.

Term	Definition
Service management layer	[M.3010] A management layer that is concerned with, and responsible for, the contractual aspects, including service order handling, complaint handling and invoicing, of services that are being provided to customers or available to potential new customers.
Service provider	[X.790] A system or a network that provides a telecommunication service to a customer. In the context of this document, a service provider is specifically a provider of telecommunications services who offers the OS-to-OS OSI interface to allow a customer the capability for network management across jurisdictions in order to control the services (or resources) being provided (See Customer). A service provider acts in the agent role. There is no requirement that the interface be confined to cases where there is a traditional telecommunication service customer to telecommunication service provider relationship between the parties. It is certainly possible that two telecommunications carriers, whose networks interwork to provide a telecommunications service to an end user, may use this interface. In that case, the customer and service provider roles may change from situation to situation. However, in any particular situation, one carrier will be the customer and have the manager role, while the other will be the supplier, and will have the agent role.
Service relationship	[H.530] References an established security association between two functional entities, assuming that at least a shared key is present.
Shared secret	[H.530] Refers to the security key for the cryptographic algorithms; it may be derived from a password.
Signature	[X.800] See digital signature.
Simple authentication	[X.509] Authentication by means of simple password arrangements.
Source of Authority	[X.509] A SOA is an Attribute Authority that a privilege verifier for a particular resource trusts as the ultimate authority to assign a set of privileges.
Spamming	[H.235] 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.
Status of a trouble report	[X.790] The stage that has been reached by a trouble report since its instantiation/creation while the trouble is being resolved.
Strong authentication	[X.509] Authentication by means of cryptographically derived credentials.
Symmetric (secret-key based) cryptographic algorithm	[H.235] 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).
Symmetric cryptographic algorithm	[X.810] An algorithm for performing encipherment or the corresponding algorithm for performing decipherment in which the same key is required for both encipherment and decipherment.
Telecommunications management network	[M.3010] An architecture for management, including planning, provisioning, installation, maintenance, operation and administration of telecommunications equipment, networks and services.
Threat	[H.235] A potential violation of security (X.800). [X.800] A potential violation of security.

Term	Definition
Time-stamp	[X.790] A time value used to indicate when a particular activity, action or an occurrence of an event took place.
Traffic analysis	[X.800] The inference of information from observation of traffic flows (presence, absence, amount, direction and frequency).
Traffic flow confidentiality	[X.800] A confidentiality service to protect against traffic analysis.
Traffic padding	[X.800] The generation of spurious instances of communication, spurious data units and/or spurious data within data units.
Transformation function	[M.3010] A function block which translates between a TMN reference point and a non-TMN (either proprietary or otherwise standardized) reference point. The non-TMN part of this function block is outside the TMN boundary.
Trouble	[X.790] Any cause that may lead to or contribute to a manager perceiving a degradation in the quality of service of one or more network services or one or more network resources being managed.
Trouble administration	[X.790] Trouble Administration consists of a set of functions that enable troubles to be reported and their status tracked. Trouble Administration services include request trouble report format, enter trouble report, add trouble information, cancel trouble report, request trouble report status, review trouble history, attribute value change notification (e.g. trouble report status/commitment time), object creation/deletion (trouble report), verify trouble repair completion, and modify trouble administration information.
Trouble history record	[X.790] A record of selected information from a trouble report that is retained for historical purposes after the trouble report is closed.
Trouble management	[X.790] The trouble reporting and tracking between CMEs interoperating co-operatively towards resolution of a trouble. (No distinction is made between inter-jurisdictional or intra-jurisdictional interfaces.)
Trouble reporting	[X.790] The act of communicating that a trouble has been detected so that trouble management may be used in its resolution.
Trouble resolution	[X.790] It is the process of diagnosis and repair action required to clear a problem. It includes the process of assigning specific work items or overall responsibility for clearing and closing the trouble report.
Trouble tracking	[X.790] The ability to follow the progress of a trouble report from its creation through to its closure.
Trouble type	[X.790] The description or category of the trouble that was detected.
Trust	[X.509] Generally, an entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects. This trust may apply only for some specific function. The key role of trust in this framework is to describe the relationship between an authenticating entity and a authority; an entity shall be certain that it can trust the authority to create only valid and reliable certificates. [X.810] Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.
Trusted entity	[X.810] 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.
Trusted functionality	[X.800] Functionality perceived to be correct with respect to some criteria, e.g. as established by a security policy.

Term	Definition
Trusted third party	[X.810] A security authority or its agent that is trusted with respect to some security-relevant activities (in the context of a security policy).
Unconditionally trusted entity	[X.810] A trusted entity that can violate a security policy without being detected.
User	[M.3010] A person or process applying management services for the purpose of fulfilling management operations.
Visited border element	[H.530] The V-BE is a border element (BE) placed within the visited domain.
Workstation	[M.3010] A physical block which performs workstation functions (WSFs).
Workstation function	[M.3010] A function block which interprets TMN information for the human user, and vice versa.
X interface	[M.3010] An interface applied at x reference points.
X reference points	[M.3010] A reference point located between OSF function blocks in different TMNs. (NOTE – Entities located beyond the x reference point may be part of an actual TMN (OSF) or part of a non-TMN environment (OSF-like). This classification is not visible at x reference points.)
X.509 certificate	[J.170] A public key certificate specification developed as part of the ITU-T X.500 standards directory.

A.3   Other ITU-T terms and definition resources

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.

Annex B: Catalogue of ITU-T Security-related Recommendations

B.1 Security aspects covered in this manual

F.400   *Message Handling System and Service overview*

This Recommendation 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 describes 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 +X.420), the EDI Messaging service (F.435 + X.435) and the Voice Messaging Service (F.440 + 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 facilities. **Security** capabilities of MHS is 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.   Question 11/17

F.440   *Message Handling Services: The Voice Messaging (VM-)Service.*

This Recommendation 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   Question 11/17

F.851 *Universal Personal Telecommunication (UPT) – Service description (service set 1)*

This Recommendation 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 identity authentication", and as optional user feature there is the UPT service provider authentication. Section 4.4 details security requirements.   Question 3/2

H.233 *Confidentiality system for audiovisual services*

A privacy system consists of two parts, the confidentiality mechanism or encryption process for the data, and a key management subsystem. This Recommendation describes the confidentiality part of a privacy system suitable for use in narrow-band audiovisual services. Although an encryption algorithm 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 confidentiality system 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.   Question G/16

H.234 *Encryption key management and authentication system for audiovisual services*

A privacy system consists of two parts, the confidentiality mechanism or encryption process for the data, and a key management subsystem. This Recommendation describes authentication and key management methods for a privacy system suitable for use in narrow-band audiovisual services. Privacy is achieved by the use of *secret keys*. The keys are loaded into the confidentiality part 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 key management are specified in this Recommendation.   Question G/16

H.235 *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*

Secure real-time communication over insecure networks generally involves *authentication* and *privacy* (data encryption).This Recommendation describes enhancements within the framework of interactive conferencing to incorporate such security services as endpoint authentication and media privacy, describes the security infrastructure and specific privacy techniques to be employed. The proposed scheme is applicable to both simple point-to-point and multipoint conferences for any terminals which utilize H.245 control protocol. This version (11/00) features elliptic curve cryptography, security profiles (simple password-based and sophisticated digital signature), security countermeasures (media anti-spamming), Advanced Encryption Algorithm (AES), backend service, object identifiers (see H.323 implementors guide).   Question G/16

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 actually security procedures from the signature profile in H.235 Annex E are 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 techniques 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.   Question G/16

H.323   *Packet-based multimedia communications system (Annex J: Security for Simple endpoint types)*

This Recommendation 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.   Question G/16

H.530   *Security for H.510 in H.323 Multimedia Mobile Environments*

The purpose of this Recommendation is to provide security procedures in H.323 mobility environments such as under scope of H.510 that describes mobility for H.323 multimedia systems and services. This Recommendation provides the details about the security procedures for H.510. So far, the signalling 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 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. As the mobile user is usually known only to the home domain where he or she is subscribed and assigned a password, the visited domain does not know the mobile user initially. 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 among 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.   Question G/16

J.93 *Requirements for conditional access in the secondary delivery of digital television or cable television systems*

This Recommendation defines the data privacy and access requirements protecting MPEG digital television signals passed on cable television networks between the cable headend and the ultimate subscriber. The exact cryptographic algorithms used in theis process are not in J.93 as they are regionally and/or industry determined.   SG 9

J.96 Amd 1 *Technical Method for Ensuring Privacy in Long-Distance International MPEG-2 Television Transmission Conforming to Recommendation J.89*

This Recommendation 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.   Question 6/9

J.170 *IPCablecom security specification (J.sec)*

This Recommendation defines the Security Architecture, protocols, algorithms, associated functional requirements and any technological requirements that can provide for the security of the system for the IPCablecom network. Authentication, access control, message and bearer content integrity, confidentiality and non-repudiation security services must be provided as defined herein for each of the network element interfaces.   SG 9

M.3010 *Principles for a telecommunications management network*

This Recommendation defines concepts of Telecommunications Management Network (TMN) architectures (TMN functional architecture, TMN information architecture, and TMN physical architectures) and their fundamental elements. This Recommendation 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. Only some parts of this Recommendation address security. A logical reference model for partitioning of management functionality, the Logical Layered Architecture (LLA), is provided. This Recommendation 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.   Question 7/4

M.3016 *Overview of TMN Security (M.3sec)*

This Recommendation 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 Recommendation is generic in nature and does not identify or address the requirements for a specific TMN interface.   Question 7/4

M.3210.1 *Security management for IMT2000Category – Requirements*

This Recommendation is one of the series of TMN Management Service Recommendations that provide description of management services, goals and context for management aspects of IMT2000 networks. This Recommendation 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. This Recommendation describes a subset of Security Management services to provide Requirements and

Analysis of the Security management and a profile for fraud management 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. Question 14/4

M.3320 *Requirements for the X interface*

This Recommendation 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 Recommendation is to define a requirements framework for all functional, service and network-level requirements for the TMN exchange of information between Administrations. This Recommendation 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. Question 9/4

M.3400 *TMN management functions*

This Recommendation 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. Question 7/4

Q.293 *Intervals at which security measures are to be invoked*

This is an extract from the BlueBook and contains only sections 8.5 (Intervals at which security measures are to be invoked) to 8.9 (Load sharing method) of Q.293 SG 4

Q.813 *Security transformations application service element for remote operations service element (STASE-ROSE)*

This Recommendation provides specifications to support security transformations, such as encryption, hashing, sealing and signing, focusing on whole Remote Operations Service Element (ROSE) Protocol Data Units (PDUs). Security transformations are used to provide various security services such as authentication, confidentiality, integrity and non-repudiation. 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. Question 18/4

Q.815 *Specification of a security module for whole message protection*

This Recommendation specifies an optional security module to be used with Recommendation 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 non-repudiation of origin and of receipt, as well as whole message integrity. Question 18/4

Q.817 *TMN PKI − Digital certificates and certificate revocation lists profiles*

This Recommendation 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. This Recommendation is intended to promote interoperability among TMN elements that use Public Key Infrastructure (PKI) to support security-related functions. The purpose of this Recommendation is to provide interoperable, scalable mechanism for key distribution and management within a TMN, across all interfaces, as well as in support of non-repudiation service 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, authentication, integrity, non-repudiation, and key exchange (M.3016). However, this Recommendation does not specify how such functions should be implemented, with or without PKI.   Question 18/4

Q.1531 *UPT security requirements for service Set 1*

This Recommendation specifies UPT security requirements for both user-to-network and inter-network communication applicable to UPT Service Set 1 as defined within Recommendation F.851. This Recommendation covers all aspects of security for UPT using DTMF accesses and out-band DSS 1 based user accesses.   SG 15

Q.1741.1 *IMT-2000 references to release 1999 of GSM evolved UMTS core network with UTRAN access network*

This Recommendation includes references to the following 3GPP security specifications:

       TS 21.133: Security threats and requirements

       TS 22.100: UMTS Phase 1

       TS 22.101: UMTS 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   SSG

Q.1741.2 *IMT-2000 references to release 4 of GSM evolved UMTS core network with UTRAN access network*

This Recommendation includes references to the following 3GPP security specifications:

       TS 21.133: 3G security; Security Threats and Requirements

       TS 22.048: Security Mechanisms for the (U)SIM application toolkit; Stage 1

       TS 22.101: Service aspects; Service principles

       TS 33.102: 3G security; Security Architecture

       TS 33.103: 3G security; Integration guidelines

       TS 33.105: Cryptographic Algorithm requirements

       TS 33.106: Lawful interception requirements

       TS 33.107: 3G security; 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: 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; (.205: General; .206: Algorithm specification; .207: Implementors' test data; .208: Design conformance test data)   SSG

Q.1741.3 *IMT-2000 references to release 5 of GSM evolved UMTS core network with UTRAN access network*

This Recommendation includes references to the following 3GPP security specifications:

       TS 22.101: Service aspects; Service principles

       TS 33.102: 3G security; Security Architecture

       TS 33.106: Lawful interception requirements

TS 33.107: 3G security; Lawful interception Architecture and Functions

TS 33.108: 3G security; Handover interface for Lawful Interception (LI)

TS 33.200: Network Domain Security – MAP

TS 33.203: 3G security; 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: 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; (.205: General; .206: Algorithm specification; .207: Implementors' test data; .208: Design conformance test data; .909: Summary and results of design and evaluation)   SSG

Q.1742.1   *IMT-2000 references to ANSI-41 evolved core network with cdma2000 access network*

This Recommendation associates the published core network standards from standards development organizations (SDOs) with those 3GPP2 specifications that were approved as of 17 July 2001 for the IMT-2000 family member "ANSI-41 evolved Core Network with cdma2000 Access Network." 3GPP2 specifications that were approved as of July 2002 will be associated with published core network standards in future ITU-T Rec. Q.1742.2. The radio interface and radio access network and standards from the SDOs for this IMT-2000 family member are associated in ITU-R M.1457. The associations for other IMT-2000 family members are identified in the ITU-T Q.174x series. This Recommendation combines and associates the relevant core network standards from a number of standards development organizations for this IMT-2000 family member into a global Recommendation.   SSG

Q.1742.2   *IMT-2000 references (approved as of 11 July 2002) to ANSI-41 evolved core network with cdma2000 access network*

This Recommendation associates the published core network standards from the regional standards development organizations (SDOs) with those 3GPP2 specifications that were approved as of 11 July 2002 for the IMT-2000 Family Member "ANSI-41 evolved Core Network with cdma2000 Access Network.". 3GPP2 specifications that were approved as of 17 July 2001 were associated with the published core network standards from the regional standards development organizations in ITU-T Q.1742.1. 3GPP2 specifications that are approved as of July 2003 will be associated with published core network standards in future ITU-T Recommendation Q1742.3. The radio interface and radio access network and standards from the SDOs for this IMT-2000 Family Member are associated in ITU-R M.1457. The associations for other IMT-2000 Family Members are identified in the ITU-T Q.174x series. This Recommendation combines and associates the regional standards for the core network of this IMT-2000 Family Member into a global recommendation.   SSG

Q.1742.3   *Technical Specifications referenced in Q.1742.3 with Security Aspects*

Intersystem Specifications:

     N.S0003-0   User Identity Module (Version 1.0; April 2001)

     N.S0005-0   Cellular Radiotelecommunications Intersystem Operations (Version 1.0; no date)

     N.S0009-0   IMSI (Version 1.0; no date)

     N.S0010-0   Advanced features in Wideband Spread Spectrum Systems (Version 1.0; no date)

     N.S0011-0   OTASP and OTAPA (Version 1.0; no date)

     N.S0014-0   Authentication Enhancements (Version 1.0; no date)

     N.S0018   TIA/EIA-41-D Prepaid Charging (Version 1.0.0; 14 July 2000)

     N.S0028   Network Interworking Between GSM MAP and ANSI-41 MAP Rev. B Revision: 0 (Version 1.0.0; April 2002)

Packet Data Specifications:

      P.S0001-A   Wireless IP Network Standard (Version 3.0.0; 16 July 2001)

      P.S0001-B   Wireless IP Network Standard (Version 1.0.0; 25 October 2002)

Services and system aspects specifications:

      S.R0005-B   Network Reference Model for cdma2000 Spread Spectrum Systems Revision: B (Version 1.0; 16 April 2001)

      S.R0006   Wireless Features Description Revision: 0 (Version 1.0.0; 13 December 1999)

      S.R0009-0   User Identity Module (Version 1.0; Stage 1) Revision: 0 (13 December 1999)

      S.R0018   Pre-Paid Charging (Version 1.0.0; Stage 1) Revision: 0 (13 December 1999)

      S.R0019   Location-Based Services System (Version 1.0.0; LBSS) Stage 1 Description (22 September 2000)

      S.R0032   Enhanced Subscriber Authentication (Version 1.0; ESA) and Enhanced Subscriber Privacy (ESP) (6 December 2000)

      S.R0037-0   IP Network Architecture Model for cdma2000 Spread Spectrum Systems (Version 2.0; 14 May 2002)

      S.R0048   3G Mobile Equipment Identifier (Version 1.0; MEID) (10 May 2001)

      S.S0053   Common Cryptographic Algorithms (Version 1.0; 21 January 2002)

      S.S0054   Interface Specification for Common Cryptographic Algorithms (Version 1.0; 21 January 2002)

      S.S0055   Enhanced Cryptographic Algorithms (Version 1.0; 21 January 2002)

      S.R0058   IP Multimedia Domain System Requirements (Version 1.0 ; 17 April 2003)

      S.R0059   Legacy MS Domain – Step 1 System Requirements (Version 1.0; 16 May 2002)

      S.R0066-0   IP Based Location Services Stage 1 Requirements (Version 1.0; 17 April 2003)

      S.R0071   Legacy System Packet Data Surveillance Requirements Stage 1 Requirements (Version 1.0; 18 April 2002)

      S.R0072   All IP Packet Data Surveillance Requirements Stage 1 Requirements (Version 1.0; 18 April 2002)

      S.R0073   Internet Over-the-Air Handset Configuration Management (Version 1.0; IOTA) Stage 1 (11 July 2002)

      S.S0078-0   Common Security Algorithms (Version 1.0; 12 December 2002)   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 RSA algorithm.   SG 16

T.36   *Security capabilities for use with Group 3 facsimile terminals*

This Recommendation 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 RSA algorithm.   SG 16

T.123rev Annex B   *Extended Transport Connections*

This annex to revised T.123 features a connection negotiation protocol (CNP) 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 key management, X.274/ ISO TLSP and GSS-API.   Question 1/16

T.503   *A document application profile for the interchange of Group 4 facsimile documents*

This Recommendation 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. SG 16

T.563   *Terminal Characteristics for Group 4 facsimile apparatus*

This Recommendation defines the general aspects of Group 4 facsimile apparatus and the interface to the physical network.   SG 16

T.611   *Programming Communication Interface (PCI) APPLI/COM for Facsimile Group 3, Facsimile Group 4, Teletex, Telex, E-mail and file transfer services*

This Recommendation 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 Recommendation describes the structure, contents of messages and the way to exchange them between two entities (i.e. LA, the Local Application and CA, the Communication Application). *Any communication is preceded by a login process and terminated by a logout process, both the processes facilitate the implementation of security schemes which are especially important on multi-user systems. They also provide means to implement security mechanisms between the LA and the CA.* This Recommendation forms a high level **API** (Application Programming Interface) which shields all telecommunication peculiarities but gives powerful control and monitoring on the telecommunication activity to the application designers.   SG 8

X.217   *Information technology – Open Systems Interconnection – Service definition for the association control service element –*

This Recommendation 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 Kernel functional unit is used to establish and release application-associations. The ACSE includes two optional functional units, one of them is the optional Authentication functional unit, which provides additional facilities for exchanging information in support of authentication during association establishment without adding new services. The ACSE authentication facilities may be used to support a limited class of authentication methods.

Amendment 1: Support of authentication mechanisms for the connectionless mode   Question 11/17

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 Kernel functional unit that is used to establish and release application-associations. The Authentication functional unit provides additional facilities for exchanging information in support of authentication during association establishment without adding new services. The ACSE authentication facilities can be used to support a limited class of authentication methods. 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 authentication-mechanism specification. 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". Question 11/17

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. Question 11/17

X.257 *Information technology – Open Systems Interconnection – Connectionless protocol for the Association Control Service Element: Protocol Implementation Conformance Statement (PICS) proforma*

This Recommendation 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. Question 11/17

X.272 *Data compression and privacy over frame relay networks*

This Recommendation defines Data Compression Service and Privacy Service for Frame Relay networks including negotiation and encapsulation of Data Compression, Secure data compression, authentication and encryption over frame relay. The presence of a data compression service 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 privacy of the data. In order to achieve optimum compression ratios, it is essential to compress the data before encrypting it. Hence, it is desirable to provide facilities in the data compression service to negotiate data encryption protocols as well. Since the task of compressing and then encrypting the data is computational intensive, efficiency is achieved through providing simultaneous data compression and encryption (secure data compression). 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). Question 10/17

X.273 *Information technology – Open Systems Interconnection – Network layer security protocol*

This Recommendation specifies the protocol to support the integrity, confidentiality, authentication and access control services 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 cryptographic mechanisms, security labeling and assigned security attributes, such as cryptographic keys. Question 11/17

X.274 *Information technology – Telecommunications and information exchange between systems – Transport layer security protocol*

This Recommendation specifies the protocol which can support the integrity, confidentiality, authentication and access control services identified in the OSI security model as relevant to the transport layer. The protocol supports these services through the use of cryptographic mechanisms, security labelling and assigned attributes, such as cryptographic keys.   Question 11/17

X.400/F.400 *Message handling system and service overview*

This Recommendation 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 confidentiality, integrity, authentication, non-repudiation and access control identified as relevant to the Application Layer. (See F.400)   Question 11/17

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 confidentiality, integrity, authentication, non-repudiation and access controls identified as relevant to the Application Layer.   Question 11/17

X.411 *Information technology – Message Handling Systems (MHS) – Message transfer system: Abstract service definition and procedures*

This Recommendation specifies mechanisms and procedures supporting confidentiality, integrity, authentication and non-repudiation services identified as relevant to the Application Layer. The protocol supports these services through the use of cryptographic mechanisms, security labeling, and digital signatures as identified in Recommendation X.509. Although this Recommendation specifies protocol that uses asymmetric cryptographic techniques, symmetric cryptographic techniques are also supported.   Question 11/17

X.413 *Information technology – Message Handling Systems (MHS): Message Store: Abstract service definition*

This Recommendation specifies mechanisms, protocol and procedures supporting integrity, access control, authentication, integrity and non-repudiation services identified as relevant to the Application Layer. The protocol supports these services on behalf of the Message Store direct user. Question 11/17

X.419 *Information technology – Message Handling Systems (MHS): Protocol specifications*

This Recommendation specifies procedures and application contexts to identify secure access for MHS entities and remote users by providing authentication and access control services identified as relevant to the Application Layer.   Question 11/17

X.420 *Information technology – Message Handling Systems (MHS) – Interpersonal messaging system*

This Recommendation specifies mechanisms, protocol and procedures for he 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 integrity, confidentiality, authentication and access control identified as relevant to the Application Layer.   Question 11/17

X.435 *Information technology – Message Handling Systems: Electronic data interchange messaging system*

This Recommendation specifies mechanisms, protocol and procedures for he exchange of objects between Electronic Data Interchange (EDI) User Agents on behalf of its direct user. The security services supported are integrity, confidentiality, authentication and access control identified as relevant to the Application Layer.   Question 11/17

X.440   *Information technology – Message Handling Systems: Voice messaging system*

This Recommendation specifies mechanisms, protocol and procedures for he exchange of objects between Voice User Agents on behalf of its direct user. The security services supported are integrity, confidentiality, authentication and access control identified as relevant to the Application Layer.

Question 11/17

X.500   *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*

This Recommendation specifies the Directory and its security features.   Question 9/17

X.501   *Information technology – Open Systems Interconnection – The Directory: Models*

This Recommendation specifies the Directory use of its X.509 Public-key and attribute certificate frameworks.   Question 9/17

X.509   *Information technology – Open Systems Interconnection – The Directory:*
        ---- Authentication framework (1993 edition – the second edition/version)
        ---- Authentication framework (1997 edition – the third edition/version)
        ---- Public-key and attribute certificate frameworks
          (2000 edition – the fourth edition/version)

This Recommendation 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: simple authentication, using a password as a verification of claimed identity; and strong authentication, 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 Public Key Infrastructures (**PKI**) and Privilege Management Infrastructures (**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 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 **PMI**, it does not define a **PMI** it its entirety. However, it provides the foundation upon which full **PMIs** and their specifications would be built. *Information objects* for holding PKI and PMI objects in the Directory and for comparing presented values with stored values are also defined.   Question 9/17

X.519   *Information technology – Open Systems Interconnection – The Directory: Protocol specification*

This Recommendation specifies procedures and application contexts to identify secure access during binding of Directory entities.   Question 9/17

X.733   *Information technology – Open Systems Interconnection – Systems Management: Alarm reporting function*

This Recommendation defines a Systems Management Function that 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 of the OSI reference model. 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.   Question 17/4

X.735 *Information technology – Open Systems Interconnection – Systems Management: Log control function*

This Recommendation 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. This Recommendation defines the Log Control function and consists of services and two functional units. This function is positioned in the application layer.   Question 17/4

X.736 *Information technology – Open Systems Interconnection – Systems Management: Security alarm reporting function*

This Recommendation | International Standard defines the security alarm reporting function. The security alarm reporting function is 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, as defined by CCITT Rec. X.700 | ISO/IEC 7498-4. This Recommendation | International Standard is positioned in the application layer of CCITT Rec. X.200 | ISO 7498 and is defined according to the model provided by ISO/IEC 9545. The role of systems management functions is described by CCITT Rec. X.701 | ISO/IEC 10040. The security alarm notifications defined by this systems management function provide information regarding operational condition and quality of service, pertaining to security.   Question 14/4

X.740 *Information technology – Open Systems Interconnection – Systems Management: Security audit trail function*

This Recommendation | International Standard 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, as defined by CCITT Rec. X.700 | ISO 7498-4. This Recommendation | International Standard is positioned in the application layer of CCITT Rec. X.200 | ISO 7498 and is defined according to the model provided by ISO/IEC 9545. The role of systems management functions is described by CCITT Rec. X.701 | ISO/IEC 10040.   Question 14/4

X.741 *Information technology – Open Systems Interconnection – Systems Management: Objects and attributes for access control*

This Recommendation | International Standard specifies an Access Control Security Model and the management information necessary for creating and administering access control associated with OSI Systems Management. Security policy adopted for any instance of use is not specified and is left as an implementation choice. This Specification is of generic application and is applicable to the security management of many types of application.   Question 14/4

X.800 *Security architecture for Open Systems Interconnection for CCITT applications*

This Recommendation 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.   Question 10/17

X.802   *Information technology – Lower layers security model*

This Recommendation 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.   Question 10/17

X.803   *Information technology – Open Systems Interconnection – Upper layers security model*

This Recommendation 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.

Question 10/17

X.805   *Security architecture for systems providing end-to-end communications*

This Recommendation 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.   Question 10/17

X.810   *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*

This Recommendation defines the framework within which security services for open systems are specified. This part of the Security Frameworks describes the organization of the security framework, defines security concepts 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 authentication as these apply to Open Systems, the relationship of authentication with other security functions such as access control and the management requirements for authentication.   Question 10/17

X.811   *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*

This Recommendation defines a general framework for the provision of authentication. The primary goal of authentication is to counter the threats of masquerade and replay.   Question 10/17

X.812   *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*

This Recommendation defines a general framework for the provision of access control. The primary goal of access control is to counter the threat of unauthorized operations involving a computer or communications system; these threats are frequently subdivided into classes known as unauthorized use, disclosure, modification, destruction and denial of service.   Question 10/17

X.813   *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*

This Recommendation defines a general framework for the provision of non-repudiation services. The goal of the Non-repudiation service is to collect, maintain, make available, and validate irrefutable evidence regarding identification of originators and recipients involved in data transfers.

Question 10/17

X.814 *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework*

This Recommendation defines a general framework for the provision of confidentiality services. Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes. Question 10/17

X.815 *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework*

This Recommendation defines a general framework for the provision of integrity services. The property that data has not been altered or destroyed in an unauthorized manner is called integrity.
Question 10/17

X.816 *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security Audit and Alarms framework*

This Recommendation describes a basic model for handling security alarms and for conducting a security audit for open systems. A security audit is an independent review and examination of system records and activities. 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. Question 10/17

X.830 *Information technology – Open Systems Interconnection – Generic upper layers security: Overview, models and notation*

This Recommendation 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 following: a) general models of security exchange protocol functions and security transformations; b) a set of notational tools 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 informative guidelines as to the application of the generic upper layer security facilities covered by this series of Recommendations. Question 10/17

X.831 *Information technology – Open Systems Interconnection – Generic upper layers security: Security Exchange Service Element (SESE) service definition*

This Recommendation 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 service provided by the Security Exchange Service Element (SESE). The SESE is an application-service-element (ASE) which facilitates the communication of security information to support the provision of security services within the Application Layer of OSI.
Question 10/17

X.832 *Information technology – Open Systems Interconnection – Generic upper layers security: Security Exchange Service Element (SESE) protocol specification*

This Recommendation 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 specifies the protocol provided by the Security Exchange Service Element (SESE). The SESE is an application-service-element (ASE) which facilitates the communication of security information to support the provision of security services within the Application Layer of OSI.
Question 10/17

X.833 *Information technology – Open Systems Interconnection – Generic upper layers security: Protecting transfer syntax specification*

This Recommendation 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 | International Standard defines the protecting transfer syntax, associated with Presentation Layer support for security services in the Application Layer.   Question 10/17

X.834 *Information technology – Open Systems Interconnection – Generic upper layers security: Security Exchange Service Element (SESE) Protocol Implementation Conformance Statement (PICS) proforma*

This Recommendation |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. This Recommendation provides a description of the standardized capabilities and options in a form that supports conformance evaluation of a particular implementation.   Question 10/17

X.835 *Information technology – Open Systems Interconnection – Generic upper layers security: Protecting transfer syntax Protocol Implementation Conformance Statement (PICS) proforma*

This Recommendation 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.   Question 10/17

X.841 *Information technology – Security techniques – Security Information Objects for access control*

This Recommendation on Security Information Objects (SIOs) for Access Control provides object definitions that are commonly needed in security standards 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 Recommendation covers only static aspects of Security Information Objects (SIOs).   Question 10/17

X.842 *Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services*

This Recommendation 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 Recommendation identifies different major categories of TTP services including time stamping, non-repudiation, key management, certificate management, and electronic notary public.   Question 10/17

X.843 *Information technology – Security techniques – Specification of TTP services to support the application of digital signatures*

This Recommendation defines the services required to support the application of digital signatures for non repudiation of creation of a document. Since this implies integrity of the document and authenticity of the creator, the services described can also be combined to implement integrity and authenticity services.   Question 10/17

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. It creates an architecture within which support of distribution, interworking and portability can be integrated. This Recommendation 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, who may include 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 Recommendation 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 protected against unauthorized access, unlawful use and any other threats or attacks. Security requirements are made more difficult to meet by remoteness of interactions, and mobility of parts of the system and of the system users. The security rules for ODP systems may define: the rules for detection of security threats; the rules for protection against security threats; the rules for limiting any damage caused by any security breaches.

Question 26/17

X.902   *Information technology – Open distributed processing – Reference Model: Foundations.*

This Recommendation contains the definition of the concepts and analytical framework for normalised 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 support Recommendation X.903 and to establish requirements for new specification techniques.

Question 26/17

X.903   *Information technology – Open distributed processing – Reference Model: Architecture.*

This Recommendation 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

Question 26/17

X.904   *Information technology – Open distributed processing – Reference Model: Architectural semantics.*

This Recommendation 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.

Question 26/17

B.2   Security aspects not covered in this manual (Reliability and Outside Plant physical protection)

Outside plant protection from corrosion, environment impact, fire accidents, human activities, and others forms of damage of all types of cable for public telecommunications and associated structures, is one of the elements that rise the security level of the information transport from the point of view of network reliability and availability. Equipment and cable construction, installation and monitoring are essential to guarantee the good performance of a link. The higher the quantity of information transported, as the higher the importance of the physical protection of a plant. The L-series Recommendations include techniques able to increase the security level of a plant and then of the information travelling from one side to another.

L.3   *Armouring of cables*

With cables laid directly in the soil, armouring contributes to safe installation and reliability of operation by ensuring protection of the cables against mechanical damage caused by stones and excavation equipment or tools, rodents and insects, chemical or electrolytic corrosion, effects of atmospheric discharges and indication phenomena due to the proximity of power lines.   Question 8/6

L.4   *Aluminium cable sheaths*

The generalized use of aluminium for sheathing cables is desirable whenever cable costs would not be increased compared with the use of lead, and also whenever aluminium sheaths satisfy the technical requirements to a greater extent. The use of cables with aluminium sheaths is particularly interesting in the case of trunk cables.   Question 8/6

L.5   *Cable sheaths made of metals other than lead or aluminium*

Other types of armouring, such as corrugated aluminium, copper tapes, etc. can be used depending on the particular applications   Question 8/6

L.7   *Application of joint cathodic protection*

By joint cathodic protection of several underground metallic structures is meant corrosion protection of these structures by means of common protective devices. A joint protection system for several underground metallic structures is composed of electrical bonds between the structures and of common protective devices complying with cathodic protection and electrical drainage requirements. Joint protection techniques enhance the reliability of buried structures, improve efficiency of cathodic protection devices and also reduce total investment and maintenance costs of the protective system.
                                                                                                     Question 7/6

L.16   *Conductive plastic material (CPM) as protective covering for metal cable sheaths*

The most important benefits of CPM cables are coordinated protection against corrosion, lightning, effects of electric power and traction lines, maintenance cost reduction especially for earthing, simplification of protection projects.   Question 8/6

L.20   *Creation of a fire security code for telecommunication facilities*

For existing buildings and the design and construction of new buildings, housing telecommunications installations administrations should create an internal fire security code, according to the anticipated specific use of each building, containing the minimum guidelines for fire safety and protection against fire.   Question 2/6

L.21   *Fire detection and alarm systems, detector and sounder devices*

In order to protect property and, when applicable, life, protective fire detection and alarm systems can be installed to initiate a number of different activities such as detection and location of a fire, provision of assistance to contain and/or extinguish the fire, emergency evacuation procedures, summoning of fire-fighting forces.   Question 2/6

L.22   *Fire protection*

Taking into account the serious damage that can occur when fires break out and the importance of fire prevention to the security, service provision and economics of communication systems, there are several aspects that should be considered, such as reduction of the fire-load coefficient, division of the building into compartments (fire sectors) to reduce and delay the spread of fire, fire statistics.
                                                                                                     Question 2/6

L.23   *Fire extinction – Classification and location of fire extinguishing installations and equipment on premises*

The fire-fighting means to be adopted in a telecommunication building may vary according to the usage and location of the premises and whether it is occupied. These are factors which determine the amount of fire service assistance initially allocated in case there should be a fire.   Question 2/6

L.25   *Optical fibre cable network maintenance*

Maintenance systems and procedure are capable of monitoring the quality of an optical fibre network independent of the transmission equipment.   Question 5/6

L.28   External additional protection for marinized terrestrial cables

For shallow-water cables, the probability of failures is higher than for deep-water application due to environmental phenomena (for example, sea-wave motion, underwater earthquakes and landslides, etc.) and human activities affecting the seabed (for example, fishing, laying and maintenance of other services and cables).

In addition to the various armour usually adopted for the cable construction – for example Rocky Armour (RA), steel wire armouring such as single armour (SA) or double armour (DA), additional external protections could be adopted if needed. Such protections can be applied both approaching the coast in shallow water and on shore in the portion between the water edge and the Beach Joint, or along the cable route where external factors or seabed features could damage the cables. Question 10/6

L.32   *Protection devices for through-cable penetrations of fire-sector partitions*

In view of the large number of through-cable penetrations in the fire-sector boundaries of a telecommunication building, which diminish the effectiveness of the fire-extinction system, an appropriate strategy would consist in adopting passive smoke- and fire-control measures, such as sealing of through-cable penetration positions with fire-stopping materials or the use of cable management (protection) systems.   Question 2/6

L.45   *Minimizing the effect on the environment from the outside plant in telecommunication networks*

It details the methodology adopted in order to minimize the effects (e.g. energy and CO_2) caused by the use of outside plant in the environment. This is based on life-cycle analysis, that is, *cradle to the grave* ownership of the products.   Question 1/6

L.46   *Protection of telecommunication cables and plant from biological attack*

It describes biological attacks and countermeasures for protection of telecommunication cables. It deals with the kinds of biological attack, weakness of cables, features of damage, and considers alternative ways of protecting the plant including dependence on cable position.   Question 1/6

The following Recommendations address availability provisions for SDH and OTN networks:

G.841   *Types and characteristics of SDH network protection architectures*

This Recommendation 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).   Questions Q.15, 16, 17, 18/15

G.842   *Interworking of SDH network protection architectures*

This Recommendation 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.
                                    Questions Q.15, 16, 17, 18/15

G.808.1 *Generic protection switching – Linear trail and subnetwork protection*

This recommendation 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

Questions Q.15, 16, 17, 18/15

G.873.1 *Optical Transport Network (OTN) – Linear protection*

This Recommendation 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.

Questions Q.15, 16, 17, 18/15

G.781 *Synchronization layer functions*

SDH and PDH Timing Source reliability. This Recommendation specifies a library of basic synchronization distribution building blocks, referred to as "atomic functions" and a set of rules by which they are combined in order to describe a digital transmission equipment's synchronization functionality.

Questions Q.15, 16, 17, 18/15

G.911 *Parameters and calculation methodologies for reliability and availability of fiber optic systems*

Reliability and availability of fiber optic systems: This Recommendation 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. This Recommendation also provides guidelines and methods for calculating the predicted reliability of devices, units and systems. Examples are included.

Questions Q.15, 16, 17, 18/15

G.784 *SDH management*

SDH management. G.784 addresses the Fault, Configuration, Accounting, Performance and Security Management (FCAPS) functions of SDH network elements. Security Management aspects in these Recs. are currently 'for further study'.

Question Q.14/15

G.874 *Management aspects of the optical transport network element*

OTN management. G.874 addresses the Fault, Configuration, Accounting, Performance and Security Management (FCAPS) functions of OTN network elements. Security Management aspects in these Recs. are currently 'for further study'.

Question Q.14/15

G.7712/Y.1703 *Architecture and specification of data communication network*

This Recommendation includes aspects for security of Management Communication Networks (MCN) and Signalling Communication Networks (SCN). The data communications functions provided in this recommendation support connection-less network services. Additional functions may be added in future versions of this recommendation to support connection-oriented network services.

Question Q.14/15

Note: Recommendations in the G.650, 660-690, 950-970 series may contain some reliability related elements.

Annex C: List of Study Groups and Security-related Questions

The standardization work of ITU-T is carried out by the technical 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 primarily in the form of study Questions. Each of these addresses technical studies in a particular area of telecommunication standardization. Each SG has a SG Chairman and a number of vice-chairmen appointed by the World Telecommunication Standardization Assembly (WTSA). The following is the list of ITU-T Study Groups for the 2001-2004 Study Period, their title and mandates, followed by a list of study Questions that address security work.

SG 2	Operational aspects of service provision, networks and performance *Lead Study Group on Service definition, Numbering, Routing and Global Mobility*
Mandate: 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.	
Main security-related Questions: - Q.5/2 – Service quality of networks	

SG 3	Tariff and accounting principles including related telecommunications economic and policy issues
Mandate: 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.	
Main security-related Questions: *None*	

SG 4	Telecommunication management, including TMN *Lead Study Group on TMN.*

As the lead study group for management activities, SG 4 work on security addresses the following areas:
 	
   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.	

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.

Main security-related Questions:
- Q.16/4 – TMN Management Support for IMT-2000 and Intelligent Networks

SG 5	Protection against electromagnetic environment effects

SG 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.

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 SG 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, SG5 has worked on several Questions and developed a number of Recommendations and Handbooks that contribute to the security of the network against electromagnetic threats.

The two principal area of electromagnetic security are

- Resistibility and immunity of telecommunication networks and equipment against malicious man-made high power transient phenomena. Such threats include

    – 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.

- Possibility of information leaks from telecommunication networks by unexpected radio emission from equipment.

Awareness of security threats related to these phenomena has increased recently as articles, news stories and television programs related to these issues have appeared in the mass media.

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.

Main security-related Questions:
- Q.2/5 – EMC related to broadband access systems (*Control of unwanted emissions from broadband access systems contributes to reducing the possibility of information leaks).*
- Q.4/5 – Resistibility of new types of communication equipment and access networks (*Resistibility of equipment to lightning improves resistibility of equipment to HEMP-induced surges*).
- Q.5/5 – Lightning protection of fixed, mobile and wireless systems (*Techniques used for lightning protection also provide a degree of hardening of the facility against HEMP and HPE*).
- Q.6/5 – Bonding configurations and earthing of telecommunication systems in the global environment (*Appropriate bonding and earthing measures also help hardening of the facility against HEMP and HPE*).
- Q.12/5 – Maintenance and enhancement of existing EMC Recommendations (*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*).
- Q.13/5 – Maintenance and enhancement of existing resistibility recommendations (*Resistibility of equipment to lightning improves resistibility of equipment to HEMP-induced surges*).

SG 6	Outside plant

Mandate: 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.

Main security-related Questions:
- 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 *Lead Study Group on integrated broadband cable and television networks.*

The ITU Study Group on "Integrated broadband cable networks and television and sound transmission" (SG9) is the lead Study Group on integrated broadband cable and television networks. The Study Group prepares and maintains recommendations on:

- 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.

- Use of telecommunication systems for contribution, primary distribution and secondary distribution of television, sound programmes and similar data services.

In this role, SG9 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.

Security related activities have focused on the following areas:

- *Secure broadband services:* 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.

- *Secure VoIP services:* 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.

- *Secure home networking services:* 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.

- *Secure application environments for interactive television services:* Interactive television services rely on the security services defined in Java and the Multimedia Home Platform (MHP) specification.

Main security-related Questions:
- Q.6/9 – Methods and practices for conditional access and copy protection for digital cable television distribution to the home
- Q13/9 – Voice and video IP applications over cable television networks

SG 11	Signalling requirements and protocols *Lead Study Group on intelligent networks.*

Mandate: 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.

Main security-related Questions:
- 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	End-to-end transmission performance of networks and terminals *Lead Study Group on Quality of Service and performance.*

Mandate: 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).

Main security-related Questions:
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	Multi-protocol and IP-based networks and their internetworking *Lead Study Group for IP related matters, B-ISDN, Global Information Infrastructure and satellite matters.*

Due to the nature of the responsibility of Study Group 13 and the studies related to

- Internetworking of heterogeneous networks encompassing multiple domains,

- Multiple protocols and innovative technologies with a goal to deliver high-quality, reliable networking.

- Specific aspects are architecture, interworking and adaptation, end-to-end considerations, routing and requirements for transport.

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 ITU-T 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 liberalised 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 SG17 and proposed to offer it to all ITU-T study groups

Further it was decided in SG13 that Recommendations having security-related specifications should be reported to ITU-T 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.

Main security-related Questions:

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	Optical and other transport networks *Lead Study Group on Access Network Transport and on Optical Technology.*

Question 14 in SG 15 (Q.14/15) is responsible for specifying the management and control requirements and supporting information models for transport equipment. Q14/15 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 Q14/15.

- 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.

- 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.

- 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).

- 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.

• Framework of ASON Management: G.fame 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 managements, and security management requirements for the Control plane components will be included.
Main security-related Questions: - Q.14/15 – Network Management for transport systems and equipment

SG 16	Multimedia services, systems and terminals *Lead Study Group on multimedia services, systems and terminals, e-business and e-commerce.*

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 WP2/16) covers "Security of Multimedia Systems and Services" and addresses the following security issues.
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.
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.
Main security-related Questions: - Q.G/16 – Security of Multimedia Systems and Services

SG 17	Data Networks and Telecommunication Software *Lead Study Group on frame relay, communication system security, languages and description techniques.*

Mandate: 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.
Security-related Questions: Q.9/17 – Directory Services and Systems Q.10/17 – Security Requirements, Models and Guidelines for Communication Systems and Services   (Note: Study Group 17 agreed to split Question 10/17 into 6 separate Questions: G/17 – Security Project; H/17 – Security Architecture and Framework; I/17 – Cyber Security; J/17 – Security Management; K/17 – Telebiometrics; and L/17 – Secure Communication Services)

SSG	Special Study Group "IMT-2000 and Beyond" *Lead Study Group on IMT 2000 and beyond and for mobility.*

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&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.

Main security-related Questions:
- 3/SSG – Identification of existing and evolving IMT-2000 systems
- 6/SSG – Harmonisation 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.805 – Security architecture for systems providing end-to-end communications
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

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

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

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

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

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 – IPCablecom 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

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

Telebiometrics, Security management, Mobility security, Emergency telecommunications

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