Part 2: ICT security standards and guidance documents

Version 2.1 February 1, 2007

Introduction

The purpose of this part of the Security Standards Roadmap is to provide a summary of existing, approved ICT security standards. Part 3 of the Roadmap will address standards that are under development.

The standards are listed by topic. Initially, the taxonomy for listing the standards will be kept very simple to ease the task of compilation. However, it is anticipated that the taxonomy will be expanded as the number of entries grows and as the editors gain experience in presenting the entries. It is also likely that some standards will occupy more than one category within the taxonomy.

Each entry provides the title of the standard, a short abstract or description, a document reference (e.g. ITU-T Rec. X.800, ISO/IEC 17799, IETF RFC 3631) the date of publication/approval and the responsible SDO. There is also provision for a short comment or linkage to the standard where it is available on-line.

This section includes standards of ETSI, IEEE, the IETF, ISO/IEC JTC 1, and ITU-T. Standards of other SDOs will be included as the Roadmap becomes more established. [Note: the listing of standards included in this section is not complete. In particular, the ISO/IEC listings are incomplete in that they include only standards from a subset of the Technical Committees.].

Taxonomy

The initial taxonomy chosen for this Roadmap is fairly simple though categories are likely to be added as the Roadmap is developed and expands. Currently, standards are listed under the following primary categories:

Intrusion Detection

Security services, mechanisms and techniques

Security services

- Generic Security Services
- Access Control services
- Authentication Services
- Trusted Third Party services
- Audit and Alarms services

Security mechanisms

- Authentication mechanisms
- Confidentiality mechanisms
    i. Encryption Algorithms & techniques
    ii. Key Management
    iii. Miscellaneous cryptographic mechanisms
- Integrity mechanisms
    i. Check systems
    ii. Hash Functions
- Non-repudiation mechanisms
    i. Trusted Third party mechanisms
    ii. Digital Signature mechanisms
    iii. Time Stamping

Network security

Transport Layer security

Security protocol standards

Secure messaging

PKI and Directory standards

Disaster Recovery

Next Generation Networks

Security terminology and glossaries

Sector-specific security standards

- Multimedia
- Security of television signals and services
- Facsimile
- Mobile
- Satellite
- Miscelaneous

Acronyms and Abbreviations

CD – Committee Draft (ISO/IEC)
Cor - Corrigendum
BCP – Best Current Practice (IETF)
ETSI – European Telecommunications Standards Institute
EG – ETSI Guide
EN – European Standard
ES – ETSI Standard
FCD – Final Committee Draft (ISO/IEC)
PDTR – Proposed Draft Technical Report (ISO/IEC)
FDIS – Final Draft International Standard (ISO/IEC)
IEEE – Institute of Electrical and Electronics Engineers
IETF – Internet Engineering Task Force
Info. – Informational (IETF)
IS – International Standard (ISO/IEC)
ISO/IEC – International Organization for Standardization/International Electrotechnical Commission
ITU-T –International Telecommunication Union, Telecommunication Standardization Sector

JTC 1 – Joint Technical Committee 1 (of ISO/IEC)
MI – Miscellaneous deliverable (ETSI)
NP – New work Proposal (ISO/IEC)
Rec. – ITU-T Recommendation
RFC – Request for Comment (IETF)
SC – Subcommittee (of ISO/IEC JTC 1)
SD – Standing Document (ISO/IEC JTC1 SC27)
SG – Study Group (of ITU-T)
SR – Special Report (ETSI)
TR – Technical Report (ISO/IEC)
TS – Technical Specification (ETSI)
WD – Working Draft (ISO/IEC)

General ICT security guidance documents

Organization	Reference	Title	Status	Date	Abstract
ITU-T SG17		Security in Telecommunications and IT Systems	Info. publication	10/ 2004	Provides an overview of the issues and the deployment of existing ITU-T Recommendations for secure telecommunications.
ITU-T SG17		Compendia	Info. publication	03/2005	Lists all ITU-T security-related recommendations http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000090001MSWE.doc
ITU-T SG2	E.408	Telecommunication networks security requirements	Rec	2004	Provides an overview of security requirements and a framework that identifies security threats to telecommunication networks in general (both fixed and mobile; both voice and data) and gives guidance for planning countermeasures that can be taken to mitigate the risks arising from the threats.
ITU-T SG 17	E.409	Incident Organization and Security Incident Handling: Guidelines for Telecommunications Organizations	Rec.	2004	Analyses, structures and suggests a method for establishing an incident management organization within a telecommunications organization involved in the provision of international telecommunications, where the flow and structure of an incident are focused.
ITU-T SG 17	X.1205 Com 17-R 17	Overview of Cybersecurity	Guide	2006	

ISO/IEC JTC1 SC27		Catalogue of SC27 Security Projects and standards	SD		Provides summaries of all SC27 standards and current projects. Access via the DIN SC27 site at www.ni.din.de/sc27 then go to documents, then to SD7 Catalogue of SC27 Projects and Standards.
ISO/IEC SC27	15292	Protection profile registration procedures	IS	2001	Defines the procedures to be applied by a Registration Authority in operating a Register of Protection Profiles and packages for the purposes of IT security evaluation. A Protection Profile is defined within ISO/IEC 15408 as an implementation-independent set of security requirements for a category of IT products or systems which meet specific consumer needs.
IETF	3365	Strong Security Requirements for Internet Engineering Task Force Standard Protocols.	BCP	Aug. 2002	It is the consensus of the IETF that IETF standard protocols MUST make use of appropriate strong security mechanisms. This document describes the history and rationale for this doctrine and establishes this doctrine as a best current practice.
IETF	3511	Benchmarking Methodology for Firewall Performance	Info.	April 2003	This document discusses and defines a number of tests that may be used to describe the performance characteristics of firewalls. In addition to defining the tests, this document also describes specific formats for reporting the results of the tests.
IETF	3523	Internet Emergency Preparedness (IEPREP) Telephony Topology Terminology	Info.	April 2003	This document defines the topology naming conventions that are to be used in reference to Internet Emergency Preparedness (IEPREP) phone calls.
IETF	3552	Guidelines for Writing RFC Text on Security Considerations	Info.	July 2003	All RFCs are required to have a Security Considerations section. Historically, such sections have been relatively weak. This document provides guidelines to RFC authors on how to write a good Security Considerations section.
IETF	3631	Security Mechanisms for the Internet	Info.	Dec 2003	Security must be built into Internet Protocols for those protocols to offer their services securely. However, even a proper implementation will have security problems if the fundamental protocol is itself exploitable. Exactly how security should be implemented in a protocol will vary, because of the structure of the protocol itself. However, there are many protocols for which standard Internet security mechanisms, already developed, may be applicable. The precise one that is appropriate in any given situation can vary. We review a number of different choices, explaining the properties of each.
IETF	3689	General Requirements for Emergency Telecommunication Service	Info	Feb 2004	This document presents a list of general requirements in support of Emergency Telecommunications Service (ETS).
IETF	3690	IP Telephony Requirements for Emergency Telecommunication Service	Info	Feb 2004	This document presents a list of requirements in support of Emergency Telecommunications Service (ETS) within the context of IP telephony. It is an extension to the general requirements presented in RFC 3689.

IETF	3702	Authentication, Authorization, and Accounting Requirements for the Session Initiation Protocol (SIP)	Info	Feb 2004	As Session Initiation Protocol (SIP) services are deployed on the Internet, there is a need for authentication, authorization, and accounting of SIP sessions. This document sets out the basic requirements for this work.
IETF	3833	Threat Analysis of the Domain Name System (DNS)	Info	Aug 2004	This note attempts to document some of the known threats to the DNS, and, in doing so, attempts to measure to what extent (if any) DNSSEC is a useful tool in defending against these threats.
IETF	3837	Security Threats and Risks for Open Pluggable Edge Services	Info	Aug 2004	The document investigates the security threats associated with the Open Pluggable Edge Services (OPES) and discusses the effects of security threats on the underlying architecture.
IETF	3871	Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure	Info	Sept 2004	This document defines a list of operational security requirements for networks (routers and switches). The goal is to provide network operators a clear, concise way of communicating their security requirements to vendors.
IETF	4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	RFC	Jun 2006	LDAP is an Internet protocol for accessing distributed directory services that act in accordance with X.500 data and service models. This document provides a road map of the LDAP Technical Specification.
ETSI	3GPP TR 33.900	Guide to 3G security	TR		
ETSI	133 901 3GPP SA 3 (3GPP TR 33.901)	Universal Mobile Telecommunications System (UMTS); 3G Security - Criteria for cryptographic Algorithm design process	TR		
ETSI	133 902 3GPP SA 3 (3GPP TR 33.902)	Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol	TR		
ETSI	133 908 3GPP SA 3 (3GPP TR 33.908)	Universal Mobile Telecommunications System (UMTS); Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	TR		

ETSI	133 909 3GPP SA 3 (3GPP TR 33.909)	Universal Mobile Telecommunications System (UMTS); 3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions	TR		
ETSI	3GPP TR 33.941	Presence service; Security	TR		
ETSI	133 978 (3GPP TR 33.978)	Universal Mobile Telecommunications System (UMTS); Security aspects of early IMS	TR		

Security Architectures, Models and Frameworks

Organization	Reference	Title	Status	Date	Abstract
ITU-T SG 17 ISO/IEC JTC 1	X.800 7498-2	Security architecture for Open Systems Interconnection	Rec IS	1991 1989	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.
ITU-T SG 17 ISO/IEC JTC 1	X.802 13594	OSI – Lower layers security model	Rec TR	1995 1995	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.
ITU-T SG 17 ISO/IEC JTC 1	X.803 10745	OSI – Upper layers security model	Rec IS	1994 1995	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.
ITU-T SG 17 ISO/IEC JTC 1	X.805 18028-2	Security architecture for systems providing end-to-end communications	Rec IS	2003	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.

ITU-T SG 17 ISO/IEC JTC 1	X.810 10181-1	OSI – Security frameworks for open systems: Overview	Rec IS	1995 1996	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 contr*ol and the management requirements for authentication.
ITU-T SG 17 ISO/IEC JTC 1	X.811 10181-2	IT OSI – Security frameworks for open systems: Authentication framework	Rec IS	1995 1996	Defines a general framework for the provision of authentication. The primary goal of authentication is *to counter the threats of masquerade and replay*.
ITU-T SG 17 ISO/IEC JTC 1	X.812 10181-3	OSI – Security frameworks for open systems: Access control framework	Rec IS	1995 1996	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*.
ITU-T SG 17 ISO/IEC JTC 1	X.813 10181-4	OSI – Security frameworks for open systems: Non-repudiation framework	Rec IS	1996 1997	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*.
ITU-T SG 17 ISO/IEC JTC 1	X.814 10181-5	OSI – Security frameworks for open systems: Confidentiality framework	Rec IS	1995 1996	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.
ITU-T SG 17 ISO/IEC JTC 1	X.815 10181-6	OSI – Security frameworks for open systems: Integrity framework	Rec IS	1995 1996	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
ITU-T SG 17 ISO/IEC JTC 1	X.816 10181-7	OSI – Security frameworks for open systems: Security Audit and Alarms framework	Rec IS	1995 1996	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.
ITU-T SG 17 ISO/IEC JTC 1	X.830 11586-1	OSI – Generic upper layers security (GULS): Overview, models and notation	Rec IS	1995 1996	Belongs to a series of Rec.s, which provide a set of facilities to aid the construction of OSI Upper Layer protocols, which support the provision of security services. This Rec. 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 Recs.

ITU-T SG 17 ISO/IEC JTC 1	X.831 11586-2	OSI – GULS: Security Exchange Service Element (SESE) service definition	Rec ISO/IEC	1995 1996	Belongs to a series of Rec.s, which provide a set of facilities to aid the construction of OSI Upper Layer protocols, which support the provision of security services. This Rec. *defines the ser*vice 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 serv*ices within the Application Layer of OSI.
ITU-T SG 17 ISO/IEC JTC 1	X.832 11586-3	OSI – GULS: Security Exchange Service Element (SESE) protocol specification	Rec IS	1995 1996	Belongs to a series of Rec.s, which provide a set of facilities to aid the construction of OSI Upper Layer protocols, which support the provision of security services. This Rec. *specifies the protocol* provided by the Security Exchange Service Element (SESE). The SESE is an application-service-element (ASE), which facilitates communication of *security information* to support the provision of *security services* within the Application Layer of OSI.
ITU-T SG 17 ISO/IEC JTC 1	X.833 11586-4	OSI – GULS: Protecting transfer syntax specification	Rec IS	1995 1996	Belongs to a series of Rec.s, which provide a set of facilities to aid the construction of OSI Upper Layer protocols, which support the provision of security services. This Rec. defines the protecting transfer syntax, associated with Presentation Layer support for *security services* in the Application Layer.
ITU-T SG 17 ISO/IEC JTC 1	X.834 11586-5	OSI – GULS: Security Exchange Service Element (SESE) PICS proforma	Rec IS	1996 1997	Belongs to a series of Rec.s on Generic Upper Layers Security (GULS). It is the Protocol Implementation Conformance Statement (PICS) proforma for the Security Exchange Service Element Protocol specified in ITU-T Rec. X.832 and the Security Exchange described in ITU-T Rec. X.830. Annex C. provides a description of the standardized capabilities and options in a form that supports conformance evaluation of a particular implementation.
ITU-T SG 17 ISO/IEC JTC 1	X.835 11586-6	OSI – GULS: Protecting transfer syntax PICS proforma	Rec IS	1996 1997	Belongs to a series of Rec.s 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 Rec. provides a description of the standardized capabilities and options in a form that supports conformance evaluation of a particular implementation.
ITU-T SG 17 ISO/IEC JTC 1	X.841 15816	Security techniques – Security Information Objects for access control	Rec IS	2000 2002	This Rec. 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 Rec. covers only static aspects of Security Information Objects (SIOs).

ITU-T SG 17 ISO/IEC JTC 1	X.217 15953	Information technology - Open Systems Interconnection (OSI) - Service definition for the association control service element	Rec IS	1995 1996	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.
ITU-T SG 17	X.1081 X.1081 Cor. 1	The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics	Rec Cor.	2004 2006	Defines a Telebiometric Multimodal Model that provides a common framework for the specification of four inter-connected security issues: Privacy, Authentication, Safety and Security. This Telebiometric Multimodal Model covers all the possibilities for safe and secure multimodal man-machine interactions, and is derived in part from ISO 31 and IEC 60027-1 standards.
ITU-T SG 17	X.1111	Framework of security technologies for home network	Rec	2006	This Recommendation describes security threats and security requirements to the home network from the point of view of home user and remote user. It excludes the security requirements from the service provider's viewpoint.
IETF	3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).	RFC	Dec. 2002	This document describes the User-based Security Model (USM) for Simple Network Management Protocol (SNMP) version 3 for use in the SNMP architecture. It defines the Elements of Procedure for providing SNMP message level security. This document also includes a Management Information Base (MIB) for remotely monitoring/managing the configuration parameters for this Security Model.
IETF	3513	Internet Protocol Version 6 (IPv6) Addressing Architecture	RFC	April 2003	This specification defines the addressing architecture of the IPv6 protocol. The document includes the IPv6 addressing model, text representations of IPv6 addresses, definition of IPv6 unicast addresses, anycast addresses, and multicast addresses, and an IPv6 node's required addresses.
IETF	3740	The Multicast Group Security Architecture	RFC	Mar 2004	This document provides an overview and rationale of the multicast security architecture used to secure data packets of large multicast groups. The document begins by introducing a Multicast Security Reference Framework, and proceeds to identify the security services that may be part of a secure multicast solution.
IETF	3837	Security Threats and Risks for Open Pluggable Edge Services	Info	Aug 2004	The document investigates the security threats associated with the Open Pluggable Edge Services (OPES) and discusses the effects of security threats on the underlying architecture.
IETF	3924	Cisco Architecture for Lawful Intercept in IP Networks.	Info.	Oct 2004	This document describes Cisco's Architecture for supporting lawful intercept in IP networks. It provides a general solution that has a minimum set of common interfaces. This document does not attempt to address any of the specific legal requirements or obligations that may exist in a particular country.

IETF	4046	Multicast Security (MSEC) Group Key Management Architecture	RFC	April 2005	This document defines the common architecture for Multicast Security (MSEC) key management protocols to support a variety of application, transport, and network layer security protocols. It also defines the group security association (GSA), and describes the key management protocols that help establish a GSA. The framework and guidelines described in this document permit a modular and flexible design of group key management protocols for a variety of different settings that are specialized to applications needs. MSEC key management protocols may be used to facilitate secure one-to-many, many-to-many, or one-to-one communication.
IETF	4301	Security Architecture for the Internet Protocol	RFC	Dec 2005	This document describes an updated version of the "Security Architecture for IP", which is designed to provide security services for traffic at the IP layer.
IETF	4422	Simple Authentication and Security Layer (SASL)	RFC	Jun 2006	The Simple Authentication and Security Layer (SASL) is a framework for providing authentication and data security services in connection-oriented protocols via replaceable mechanisms.
IEEE	P1619	Standard Architecture for Encrypted Shared Storage Media	New project	Aug. 2002	This standard specifies the architecture for protection-use-data in sector-level storage devices, describing the methods, algorithm(s), and modes of data protection to be used.
IEEE	1700	Information System Security Assurance Architecture (ISSAA) MP		Aug. 2004	This standard specifies the architecture of a systematic approach for managing the health/state of the security controls of information systems, including the cost-effective selection, documentation, implementation, and ongoing assessment of security controls, and for making and maintaining system security accreditation decisions.
ETSI	3GPP TR 33.810 3G	Security; Network Domain Security /Authentication Framework (NDS/AF); Feasibility Study to support NDS/IP evolution	TR		
ETSI	133 919 3GPP SA 3 (3GPP TR 33.919)	Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); System description	TR		
OASIS	AVDL 1.0	Application Vulnerability Description Language	OASIS Standard	May 2004	Specifies a uniform method for describing application security vulnerabilities
OASIS	WAS 1.0	Web Application Security			Specifies a threat model and classification scheme for web security vulnerabilities

Security management standards and guidance documents

Organization	Reference	Title	Status	Date	Abstract
ISO/IEC JTC 1/SC 27	17799	Code of practice for information security management (See also 27000)	IS	2005	This international standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this standard provide general guidance on the commonly accepted goals of information security management.
ISO/IEC JTC 1/SC 27	13335-1	Management of information and communications technology security (MICTS) - Part 1: Concepts and models for information and communications technology security management	TR	2004	Presents the concepts and models fundamental to a basic understanding of ICT security, and addresses the general management issues that are essential to the successful planning, implementation and operation of ICT security.
ISO/IEC JTC 1/SC 27	13335-2	Guidelines for the management of IT security - Part 2: Managing and planning IT security	CD	2005	
ISO/IEC JTC 1/SC 27	13335-3	Guidelines for the management of IT security (GMITS) - Part 3: Techniques for the management of IT security	TR	1998	Provides techniques for the management of IT security based on general guidelines laid out in Part 1 and Part 2 of ISO/IEC 13335. These guidelines are designed to assist the implementation of IT security.
ISO/IEC JTC 1/SC SC 27	13335-4	Guidelines for the management of IT security (GMITS) - Part 4: Selection of safeguards	TR	2000	Provides guidance on the selection of safeguards, taking into account business needs and security concerns. It describes a process for the selection of safeguards according to security needs and the specific environment of an organization. It shows how to achieve appropriate protection, and how this can be supported by the application of baseline security.
ISO/IEC JTC 1/SC 27	13335-5	Guidelines for the management of IT security (GMITS) - Part 5: Management guidance on network security	TR	2001	Provides guidance to an organization connecting its IT systems to external networks. This guidance includes the selection and use of safeguards to provide security for the external connections and the services supported by those connections, and additional safeguards required for the IT systems because of the connections.

ISO/IEC JTC 1/SC 27	24743	Information security management system requirements specification	FCD		The objective of this standard is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) this is designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to customers and other interested parties.
ISO/IEC JTC 1/SC 27	27000	Information security management systems - Fundamentals and vocabulary	NP	2006	The scope of this standard is to specify the fundamental principles, concepts and vocabulary for the ISO/IEC 27000 (information security management system) series of documents.
ISO/IEC JTC 1/SC 27	27001	Information security management systems - Requirements	IS	Oct 2005	This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. (This part of the 27000 series replaces IS 17799)
ISO/IEC JTC 1/SC 27	27003	Information security management system implementation guidance	WD	Nov 2005	This draft standard will provide help and guidance in implementing the Information Security Management System (ISMS) requirements
ISO/IEC JTC 1/SC 27	27004	Information security management measurements	WD	Nov 2005	This International Standard provides guidance on the specification and use of measurement techniques for providing assurance as regards the effectiveness of information security management systems.
ISO/IEC JTC 1/SC 27	27005	Management of information and communications technology security (MICTS) - Part 2: Techniques for information and communications technology security risk management	CD	Jan 2006	ISO/IEC 27005 provides techniques for information security risk management that includes information and communications technology security risk management.
ISO/IEC JTC 1/SC 27	27006	International accreditation guidelines for the accreditation of bodies operating certification / Registration of information security management systems	NP	2006	The scope of this standard is to specify general requirements a third-party body operating ISMS (in accordance with ISO/IEC 27001:2005) certification/registration has to meet, if it is to be recognized as comptent and reliable in the operation of ISMS certification / registration.

ITU-T SG 4	X.790	Trouble management function for ITU-T applications	Rec	1995	Is concerned with the management of malfunction in systems and communications networks from the perspective of a provider of service and user of that service. Malfunction, referred to as “trouble” is a problem that has an adverse effect on the quality of service perceived by network users. When a trouble is detected, possibly as a result of an alarm report, a trouble report may be entered by a user or the system may raise a report automatically. Management of that trouble report is necessary to ensure that it receives attention and that the trouble is cleared to restore the service to its previous level of capability. A report format is defined to allow a user to report a trouble, which will then be progressed to resolution by a provider. During the resolution by the service provider, the service user may determine the current state of resolution by issuing a request for this information. When cleared the provider may notify the user. Particular types of troubles are included; however, the use of this Rec. by a particular application may require trouble types specific to that application to be used – this is catered for in this Rec.. At the time of a trouble, a network may have been interworking with another network to provide a service, and the problem or malfunction may be due to the other network. Therefore it may be necessary to exchange trouble management information between management systems across interfaces which may be client to service provider or service provider to service provider interfaces and may represent inter-jurisdictional as well as intra-jurisdictional boundaries. In addition to exchanging information on trouble that has already been detected, advance information on service inaccessibility may also need to be exchanged. Thus, a service provider may need to inform a customer of future service inaccessibility (because of planned maintenance, for example). The scope of this Rec. includes all of the above processes for exchange of management information.
ITU-T SG17	X.1051	Requirements for Telecommunications of Information Security Management System (T-ISMS)	Rec	2004	This Rec. specifies the requirements of information security management for telecommunications organizations to establish, implement, operate, monitor, review, maintain and improve a documented ISMS, and specifies requirements for the implementation of security controls customized to the needs of individual telecommunications or parts thereof.
IETF	4013	SASLprep: Stringprep Profile for User Names and Passwords	RFC	Feb 2005	This document describes how to prepare Unicode strings representing user names and passwords for comparison. The document defines the "SASLprep" profile of the "stringprep" algorithm to be used for both user names and passwords. This profile is intended to be used by Simple Authentication and Security Layer (SASL) mechanisms (such as PLAIN, CRAM-MD5, and DIGEST-MD5), as well as other protocols exchanging simple user names and/or passwords.

Security policy and policy mechanisms

IETF	4534	Group Security Policy Token v1	RFC	June 2006	The Group Security Policy Token is a structure used to specify the security policy and configurable parameters for a cryptographic group, such as a secure multicast group. This document specifies the structure of such a token.

Security assessment and evaluation criteria

ISO/IEC JTC 1/SC 27	15408-1	Evaluation criteria for IT security - Part 1: Introduction and general model. (Draft Technical Corrigendum 1 to be incorporated into the 2nd edition of 15408-1)	IS	2005	This part 1 of the multi-part ISO is the introduction to the standard. Part 1 defines general concepts and principles of IT security evaluation and presents a general model for evaluation.
ISO/IEC JTC 1/SC 27	15408-2	Evaluation criteria for IT security - Part 2: Security functional requirements. (Draft Technical Corrigendum 1 to be incorporated into the 2nd edition of 15408-2)	IS	2005	Defines the required structure and content of security functional components. In addition, it provides a catalogue of predefined functional components that will meet the common security functionality requirements of many Targets of Evaluation.
ISO/IEC JTC 1/SC 27	15408-3	Evaluation criteria for IT security - Part 3: Security assurance requirements. (Draft Technical Corrigendum 1 to be incorporated into the 2nd edition of 15408-3)	IS	2005	In order to allow an evaluation of the assurance in a Target of Evaluation (TOE), seven evaluation assurance levels labelled are defined in this part of the standard, representing ascending levels of confidence in the IT security of the TOE.

ISO/IEC JTC 1/SC 27	15443-1	A framework for IT Security assurance - Part 1: Overview and framework	TR	Feb. 2005	Provides an overview of the fundamental concepts and general description of assurance methods
ISO/IEC JTC 1/SC 27	15443-2	A framework for IT Security assurance - Part 2: Assurance methods	TR	2005	Describes a variety of assurance methods and approaches and relates them to the assurance framework in Part 1
ISO/IEC JTC 1/SC 27	15443-3	A framework for IT Security assurance - Part 3 Analysis of Assurance methods	WD	2006	
ISO/IEC JTC 1/SC 27	15446	Guide on the production of protection profiles and security targets	TR	July 2004	Provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with ISO/IEC 15408 (the 'Common Criteria')
ISO/IEC JTC 1/SC 27	18044	Information security incident management	TR	Oct 2004	This TR provides advice and guidance on information security incident management for information security managers, and information system managers.
ISO/IEC JTC 1/SC 27	19791	Security assessment of operational systems	TR	2006	Aims to define an approach to the assessment of the security of a specific composite IT system.
ISO/IEC JTC 1/SC 27	18045	Methodology for IT security evaluation	IS	2005	This standard is intended to support the consistent and therefore predictable evaluation work performed by IT Security Evaluation Facilities (ITSEFs) around the world, performing IS 15408 evaluations.
ISO/IEC JTC 1/SC 27	19792	Security evaluation of biometrics	CD	2006	This International Standard (IS) specifies the specific aspects which shall be considered during each security evaluation of a biometric product.
ISO/IEC JTC 1/SC 27	21827	Systems Security Engineering - Capability Maturity Model (SSE-CMM®)	IS	2002	The Systems Security Engineering Capability Maturity Model® (SSE-CMM®) describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The SSE-CMM® does not prescribe a particular process or sequence, but captures practices generally observed in industry. The model is a standard metric for security engineering practices covering:

Baseline security requirements

IEEE	P2200	Standard for Baseline Operating Systems Security (TM) (BOSS TM)	New project	June 2003	This standard identifies reasonable security requirements for general-purpose, commercial-off-the-shelf operating systems, expressed in terms of the International Organization for Standardization Common Criteria framework.
IEEE	2600	Standard for Information Technology: Hardcopy Device and System Security MP	New Project	Sept 2006	This standard defines security requirements (all aspects of security including but not limited to authentication, authorization, privacy, integrity, device management, physical security and information security) for manufacturers, users and others on the selection, installation, configuration and usage of hardcopy devices and systems; including printers, copiers, and multifunction devices.

Intrusion Detection

ISO/IEC JTC 1/SC 27	15947	IT intrusion detection framework	TR	2002	This Technical Report explains the role of intrusion detection in IT risk management. It seeks to establish common definitions for intrusion detection terms and concepts. It defines a framework for intrusion detection systems.
ISO/IEC JTC 1/SC 27	18043	Selection deployment and operations of intrusion detection systems (IDS)	FDIS	2006	This TR will: provide a brief overview of the intrusion detection process; discuss what an IDS can and cannot do; provide a checklist that helps identify the best IDS features a specific IT environment; describe various deployment strategies, provide guidance on managing alerts from IDSs and discuss management and legal considerations.
IETF	3620	Exchange for Intrusion Detection - the TUNNEL Profile	RFC	October 2003	This memo describes a Blocks Extensible Exchange Protocol (BEEP) profile that allows a BEEP peer to serve as an application-layer proxy. It allows authorized users to access services through a firewall.

Security services, mechanisms and techniques

a) Security services

Organization	Reference	Title	Status	Date	Abstract
Generic Security Services					
IETF	4178	The Simple and Protected Generic Security Service Application Program Interface (GSS-API) Negotiation Mechanism	RFC	Oct 2005	This document specifies a negotiation mechanism for the Generic Security Service Application Program Interface (GSS-API), which is described in RFC 2743. GSS-API peers can use this negotiation mechanism to choose from a common set of security mechanisms. If per-message integrity services are available on the established mechanism context, then the negotiation is protected against an attacker that forces the selection of a mechanism not desired by the peers.
IETF	4261	Common Open Policy Service (COPS) Over Transport Layer Security (TLS)	RFC	Dec 2005	This document describes how to use Transport Layer Security (TLS) to secure Common Open Policy Service (COPS) connections over the Internet.
Access Control services					
ITU-T SG 17 ISO/IEC JTC 1/SC 27	X.841 15816	Security information objects for access control	Rec IS	2000 2002	Provides object definitions that are needed in more than one security standard to avoid multiple and different definitions of the same functionality. It references existing definitions in other International Standards. The document contains methods and guidelines for defining basic security-related information objects and for constructing new ones from existing components. It also provides a collection of generic and specific SIO definitions.
ITU-T SG17 ISO/IEC	X.741 10164-9	IT – OSI – Systems Management: Objects and attributes for access control	Rec IS	1995 1995	Defines specifications applicable to the provision of access control for applications that use OSI management services and protocols. The access control information identified by this Rec. may be used in support of access control schemes based on access control lists, capabilities, security labels, and contextual constraints.
Authentication Services					
IETF	3539	Authentication, Authorization and Accounting (AAA) Transport Profile.	RFC	June 2003	This document discusses transport issues that arise within protocols for Authentication, Authorization and Accounting (AAA). It also provides recommendations on the use of transport by AAA protocols.
IETF	4014	Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option	RFC	Feb 2005	The RADIUS Attributes suboption enables a network element to pass identification and authorization attributes received during RADIUS authentication to a DHCP server.

IETF	4120	The Kerberos Network Authentication Service (V5)	RFC	July 2005	This document provides an overview and specification of Version 5 of the Kerberos protocol, and it obsoletes RFC 1510 to clarify aspects of the protocol and its intended use that require more detailed or clearer explanation than was provided in RFC 1510. This document is intended to provide a detailed description of the protocol, suitable for implementation, together with descriptions of the appropriate use of protocol messages and fields within those messages.
OASIS	SAML	Identity Authentication - Security Assertion Markup Language	OASIS Standard	Q1/2005	Specifies a standardized way to convey identity and authorization data
OASIS	WS-Security	Identity Authentication – Web Services Security	OASIS Standard	Apr 2004	Specifies a standard method for attaching security data to a web services message. Includes profiles (modules) for: Username-token/ password pairs, X.509 PKI, SAML and rights expression languages
OASIS	XCBF	Identity Authentication – eXtensible Common Biometric Format	OASIS Standard	Aug 2003	Specifies a method for conveying biometric identity data such as retina scans and fingerprints. This standard is coordinated with other world efforts, including ITU-T standards and the ANSI X9.84 banking industry biometrics initiative
OASIS	SPML	Identity Authentication – Service Provisioning Markup Language	OASIS Standard		Specifies a method for conveying cross-system identity provisioning requests. This standard is fully integrated with SAML and is built using wide range of open web services standards. It defines a simple client-oriented request/response protocol for id provisioning request exchange and becomes the missing link in secure web services subscription and Identity Mgmt
OASIS	XACML	Digital Signature Services	OASIS Standard	Nov 2003	Method for conveying and applying data access policies & controls
Trusted Third Party services					
ITU-T SG 17 ISO/IEC JTC 1/SC 27	X.843 15945	Specification of TTP services to support the application of digital signatures	Rec IS	2000 2002	Defines those TTP services needed to support the application of digital signatures in commercial applications. Also defines interfaces and protocols to enable interoperability between entities associated with these TTP services. This standard does not describe the management of TTPs or other organizational, operational or personal issues.
Audit and Alarms services					
ITU-T SG 4 ISO/IEC JTC 1	X.733 10164-4	Information technology (IT) – Open Systems Interconnection (OSI) – Systems Management: Alarm reporting function	Rec IS	1992 1992	Defines a Systems Management Function which may be used by an application process in a centralized or decentralized management environment to interact for the purpose of systems management. This Rec. defines a function which consists of generic definitions, services and functional units, is positioned in the application layer. The alarm notifications defined by this function provides information that a manager may need to act upon pertaining to a system's operational condition and quality of service.

ITU-T SG 4 ISO/IEC JTC 1	X.735 10164-6	IT – OSI – Systems Management: Log control function	Rec IS	1992 1993	Defines a Systems Management Function which may be used by an application process in a centralized or decentralized management environment to interact for the purpose of systems management. This Rec. defines the Log Control function and consists of services and two functional units. This function is positioned in the application layer.
ITU-T SG 4 ISO/IEC JTC 1	X.736 10164-7	IT – OSI – Systems Management: Security alarm reporting function	Rec IS	1992 1992	Defines the security alarm reporting function, a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information for the purpose of systems management. This Rec. is positioned in the application layer. The security alarm notifications defined by this systems management function provide information regarding operational condition and quality of service, pertaining to security.
ITU-T SG 4 ISO/IEC JTC 1	X.740 10164-8	IT – OSI – Systems Management: Security audit trail function	Rec IS	1992 1993	Defines the security audit trail function. The security audit trail function is a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information and commands for the purpose of systems management. This function is positioned in the application layer.
IETF	3877	Alarm Management Information Base (MIB)	RFC	Sept 2004	This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes management objects used for modelling and storing alarms.
IETF	3878	Alarm Reporting Control Management Information Base (MIB)	RFC	Sept 2004	This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it defines objects for controlling the reporting of alarm conditions
IETF	3881	Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications.	RFC	Sept 2004	This document defines the format of data to be collected and minimum set of attributes that need to be captured for security auditing in healthcare application systems. The format is defined as an XML schema, which is intended as a reference for healthcare standards developers and application designers. It consolidates several previous documents on security auditing of healthcare data.

b) Security mechanisms

Organization	**Reference**	**Title**	**Status**	**Date**	**Abstract**
Authentication mechanisms					
ISO/IEC JTC 1/SC 27	9797-1	Message authentication codes (MACs) – Part 1: Mechanisms using a block cipher	IS	Dec. 1999	Specifies six MAC algorithms that use secret key and an n-bit block cipher to calculate a MAC

ISO/IEC JTC 1/SC 27	9797-2	Message authentication codes (MACs) – Part 2: Mechanisms using a dedicated hash-function	IS	June 2002	Specifies three MAC algorithms that are based on a dedicated hash-function (selected from ISO/IEC 10118-3)
ISO/IEC JTC 1/SC 27	9798-1	Entity authentication – Part 1: General	IS	Aug. 1997	Describes the general model for the entity authentication mechanisms of ISO/IEC 9798-2 (using symmetric encipherment algorithms), ISO/IEC 9798-3 (using a public key algorithm), ISO/IEC 9798-4 (using a cryptographic check function) and the future ISO/IEC 9798-5 (using asymmetric zero knowledge techniques). It contains definitions and notation, describes the authentication model and discusses requirements and constraints common to the other parts. The standard also contains informative annexes on the use of text fields, on time variant parameters (time stamps, sequence numbers, or random numbers), and on certificates.
ISO/IEC JTC 1/SC 27	9798-2	Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms	IS	July 1999	Describes the required content of messages necessary to set up the conditions for entity authentication. This may be unilateral authentication or mutual authentication. This part of ISO/IEC 9798 specifies four authentication mechanisms where no trusted third party is involved. Two of these four are concerned with unilateral authentication while the other two specify mechanisms for mutual authentication. In addition, two mechanisms involving a trusted third party are specified.
ISO/IEC JTC 1/SC 27	9798-3	Entity authentication - Part 3: Mechanisms using digital signature techniques	IS	Oct 1998	Describes two mechanisms for unilateral authentication and three mechanisms for mutual authentication.
ISO/IEC JTC 1/SC 27	9798-4	Entity authentication - Part 4: Mechanisms using a cryptographic check function	IS	Dec. 1999	This part of ISO/IEC 9798 specifies four authentication mechanisms. Two of these four are concerned with unilateral authentication while the other two specify mechanisms for mutual authentication.
ISO/IEC JTC 1/SC 27	9798-5	Entity authentication - Part 5: Mechanisms using zero knowledge techniques	IS	Dec. 2004	This part of ISO/IEC 9798 specifies three entity authentication mechanisms using zero knowledge techniques. All the mechanisms specified in this part of ISO/IEC 9798 provide unilateral authentication. These mechanisms are constructed using the principles of zero knowledge, but they are not zero knowledge according to the strict (mathematical) definition.

ISO/IEC JTC 1/SC 27	9798-6	Entity authentication - Part 6: Mechanisms using manual data transfer	FDIS	2005	This part of ISO/IEC 9798 specifies four entity authentication mechanisms based on manual data transfer between authenticating devices. The four mechanisms are appropriate for different types of devices. Specifically, * the first and fourth mechanisms are appropriate for the case where one device has a simple input interface and the other has a simple output interface, * the second mechanism is appropriate for the case where both devices have a simple input interface, and * the third mechanism is appropriate for the case where both devices have a simple output interface.
ISO/IEC JTC 1/SC 27	19772	Authenticated encryption	CD	2006	This International Standard specifies six methods for authenticated encryption
ISO/IEC JTC 1/SC 27	24745	Security techniques Biometric template protection	WD	2005	This international Standard describes the security techniques for Biometric Template Protection
ISO/IEC JTC 1/SC 27	24760	A framework for identity management	WD	2005	This standard aims to provide a framework for the definition of identity and the secure, reliable, and private management of identity information.
ISO/IEC JTC 1/SC 27	24761	Authentication context of biometrics	WD	2005	This document defines the structure and the data elements of Authentication Context for Biometrics (ACBio), by which the service provider (verifier) can judge whether the biometric verification result is acceptable or not.
IETF	3567	Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication.	Info.	July 2003	This document describes the authentication of Intermediate System to Intermediate System (IS-IS) Protocol Data Units (PDUs) using the Hashed Message Authentication Codes - Message Digest 5 (HMAC-MD5)algorithm as found in RFC 2104. IS-IS is specified in IS10589, with extensions to support IPv4 described in RFC 1195. The base specification includes an authentication mechanism that allows for multiple authentication algorithms. The base specification only specifies the algorithm for cleartext passwords. This document proposes an extension to that specification that allows the use of the HMAC-MD5 authentication algorithm to be used in conjunction with the existing authentication mechanisms.
IETF	3575	IANA Considerations for RADIUS (Remote Authentication Dial In User Service).	RFC	July 2003	This document describes the IANA considerations for the Remote Authentication Dial In User Service (RADIUS).

IETF	3576	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS).	Info.	July 2003	This document describes a currently deployed extension to the Remote Authentication Dial In User Service (RADIUS) protocol, allowing dynamic changes to a user session, as implemented by network access server products. This includes support for disconnecting users and changing authorizations applicable to a user session.
IETF	3579	RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP).	RFC	July 2003	This document defines Remote Authentication Dial In User Service RADIUS) support for the Extensible Authentication Protocol (EAP), an authentication framework which supports multiple authentication mechanisms. In the proposed scheme, the Network Access Server (NAS) forwards EAP packets to and from the RADIUS server, encapsulated within EAP-Message attributes. This has the advantage of allowing the NAS to support any EAP authentication method, without the need for method-specific code, which resides on the RADIUS server. While EAP was originally developed for use with PPP, it is now also in use with IEEE 802.
IETF	3580	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines	Info	July 2003	This document provides suggestions on Remote Authentication Dial In User Service (RADIUS) usage by IEEE 802.1X Authenticators.
IETF	3645	Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG).	RFC	Oct 2003	The Secret Key Transaction Authentication for DNS (TSIG) protocol provides transaction level authentication for DNS. TSIG is extensible through the definition of new algorithms. This document specifies an algorithm based on the Generic Security Service Application Program Interface (GSS-API)
IETF	4462	Generic Security Service Application Program Interface (GSS-API) Authentication and Key Exchange for the Secure Shell (SSH) Protocol	RFC	May 2006	The Generic Security Service Application Program Interface (GSS-API)provides security services to callers in a mechanism-independent fashion.
IETF	4505	Anonymous Simple Authentication and Security Layer (SASL) Mechanism	RFC	Jun 2006	On the Internet, it is common practice to permit anonymous access to various services. Traditionally, this has been done with a plain- text password mechanism using "anonymous" as the user name and using optional trace information, such as an email address, as the password. As plain-text login commands are not permitted in new IETF protocols, a new way to provide anonymous login is needed within the context of the Simple Authentication and Security Layer (SASL) framework.
IETF	4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms	RFC	Jun 2006	This document describes authentication methods and security mechanisms of LDAP. This document details establishment of Transport Layer Security (TLS) using the StartTLS operation.
IETF	4552	Authentication/Confidentiality for OSPFv3	RFC	Jun 2006	This document describes means and mechanisms to provide authentication/confidentiality to OSPFv3 using an IPv6 Authentication Header/Encapsulating Security Payload (AH/ESP) extension header.

IETF	4590	RADIUS Extension for Digest Authentication	RFC	July 2006	This document defines an extension to the Remote Authentication Dial-In User Service (RADIUS) protocol to enable support of Digest Authentication, for use with HTTP-style protocols like the Session Initiation Protocol (SIP) and HTTP.
Electronic Signatures					
ETSI	102 044	Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates	TR		
ETSI	102 045	Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model	TR		
ETSI	102 046	Electronic Signatures and Infrastructures (ESI); Maintenance of ETSI standards from EESSI phase 2 and 3	TR		
ETSI	102 047	Electronic Signatures and Infrastructures (ESI); International Harmonisation of Electronic Signature Formats	TR		
ETSI	102 040	Electronic Signatures and Infrastructures (ESI); International Harmonisation of Policy Requirements for CAs issuing Certificates	TR		
ETSI	102 231	Electronic Signatures and Infrastructures (ESI); Provision of harmonised Trust Service Provider status information	TS		
ETSI	102 158	Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates	TS		
ETSI	102 153	Electronic Signatures and Infrastructures (ESI); Pre-study on certificate profiles	TR		
ETSI	002 176	Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures	SR		

ETSI	101 733	Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)	TS		
ETSI	102 280	X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons	TS		
ETSI	102 272	Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies	TR		
ETSI	101 456	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates	TS		
ETSI	102 042	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates	TS		
ETSI	102 317	Electronic Signatures and Infrastructures (ESI); Process and tool for maintenance of ETSI deliverables	TR		
ETSI	101 903	Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)	TS		
ETSI	101 862	Electronic Signatures and Infrastructures (ESI); Qualified Certificate profile	TS		
ETSI	102 176-1	Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms	TS		
ETSI	102 176-2	Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices	TS		

ETSI	102 041	SEC ESI; Signature Policies Report	TR		
ETSI	102 023	Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities	TS		
ETSI	101 861	SEC ESI; Electronic Signatures and Infrastructures (ESI); Time stamping profile	TS		
ETSI	102 038	XML format for signature policies	TR		
ETSI	102 030	SEC ESI; Provision of harmonised Trust Service Provider status information	TR		
ETSI	102 438	Electronic Signatures and Infrastructures (ESI); Application of Electronic Signature Standards in Europe	TR		
ETSI	102 458	Electronic Signatures and Infrastructures (ESI); US Federal PKI to EU Qualified Certificate Policy (TS 101 456) mapping	TR		
Smart cards					
ETSI	101 220	Smart Cards; ETSI numbering system for telecommunication application providers	TS		
ETSI	102 124	Smart Cards; Transport Protocol for UICC based Applications; Stage 1	TS		
ETSI	102 151	Smart Cards; Measurement of Electromagnetic Emission of SIM Cards	TR		
ETSI	102 221	Smart cards; UICC-Terminal interface; Physical and logical characteristics	TS		
ETSI	102 223	Smart cards; Card Application Toolkit (CAT)	TS		
ETSI	102 224	Smart Cards; Security mechanisms for UICC based Applications - Functional requirements	TS		

ETSI	102 225	Smart Cards; Secured packet structure for UICC based applications	TS		
ETSI	102 226	Smart Cards; Remote APDU Structure for UICC based Applications	TS		
ETSI	102 230	Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification	TS		
ETSI	102 240	Smart Cards; UICC Application Programming Interface and Loader Requirements; Service description	TS		
ETSI	122 907	Universal Mobile Telecommunications System (UMTS); Terminal and smart card concepts (3GPP TR 22.907)	TR		
ETSI	102 222	Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications	TS		
ETSI	102 310	Smart Cards; Extensible Authentication Protocol support in the UICC	TS		
Confidentiality mechanisms					
Encryption Algorithms & techniques					
ISO/IEC JTC 1/SC 27	10116	Modes of operation for an n-bit block cipher algorithm	IS	April 1997	Specifies four modes of operation for an n-bit block cipher algorithm: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB), and Cipher Feedback (CFB).
ISO/IEC JYC 1/SC 27	15946-1	Cryptographic techniques based on elliptic curves – Part 1: General	IS	Dec 2002	Describes the mathematical background and general techniques necessary for implementing any of the mechanisms described in other parts of ISO/IEC 15946.
ISO/IEC JTC 1/SC 27	15946-2	Cryptographic techniques based on elliptic curves – Part 2: Digital signatures	IS	Dec 2002	Describes mechanisms for digital signatures based on elliptic curves

ISO/IEC JTC 1/SC 27	15946-3	Cryptographic techniques based on elliptic curves – Part 3: Key establishment	IS	Dec 2002	Specifies techniques for key agreement and for key transport that use elliptic curves.
ISO/IEC JTC 1/SC 27	15946-4	Cryptographic techniques based on elliptic curves – Part 4: Digital signatures giving message recovery	IS	Oct 2004	Describes mechanisms for digital signatures giving message recovery.
ISO/IEC JTC 1/SC 27	18033-1	Encryption algorithms – Part 1: General	IS	2005	Provides definitions that apply in subsequent parts of this standard. The nature of encryption is introduced, and certain general aspects of its use are described. The criteria used to select the algorithms specified in subsequent parts of this standard are defined, and the relationship of this standard to the Register of algorithms is also specified.
ISO/IEC JTC 1/SC 27	18033-2	Encryption algorithms – Part 2: Asymmetric ciphers	IS	2006	Specifies a general method for building hybrid encryption schemes. The two basic components are a key encapsulation mechanism (KEM), which uses asymmetric cryptographic techniques to generate and encrypt a random symmetric key, and a data encapsulation mechanism (DEM) to actually encrtpt a message using this symmetric key
ISO/IEC JTC 1/SC 27	18033-3 18033-3/DCOR 1	Encryption algorithms – Part 3: Block ciphers	IS DCOR 1	2005 2006	Describes the specifications of block ciphers.
ISO/IEC JTC 1/SC 27	18033-4	Encryption algorithms – Part 4: Stream ciphers	IS	2005	Specifies stream cipher algorithms including modes for generating key-stream and modes for a stream cipher, and describes dedicated pseudorandom generators for producing key-stream.
ISO/IEC JTC 1/SC 27	24759	Test requirements for cryptographic modules	WD	2005	Describes the methods that will be used by accredited laboratories to test whether the cryptographic module conforms to the requirements of ISO/IEC 19790
ISO/IEC JTC 1/SC 27	19790	Security requirements for cryptographic modules	IS	2006	Specifies the technical requirements for cryptographic modules used to protect sensitive information in computer and telecommunication systems (including voice system).

ITU-T SG17	X.272	Data compression and privacy over frame relay networks	Rec	2000	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 Rec. 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).
IETF	2440	OpenPGP Message Format	RFC	1998	This document is maintained in order to publish all necessary information needed to develop interoperable applications based on the OpenPGP format. It describes only the format and methods needed to read, check, generate, and write conforming packets crossing any network. Open-PGP software uses a combination of strong public-key and symmetric cryptography to provide security services for electronic communications and data storage. These services include confidentiality, key management, authentication, and digital signatures. This document specifies the message formats used in OpenPGP.
IETF	2631	Diffie-Hellman Key Agreement Method	RFC	June 1999	This document standardizes one particular Diffie-Hellman variant, based on the ANSI X9.42 draft, developed by the ANSI X9F1 working group. Diffie-Hellman is a key agreement algorithm used by two parties to agree on a shared secret. An algorithm for converting the shared secret into an arbitrary amount of keying material is provided. The resulting keying material is used as a symmetric encryption key. The Diffie-Hellman variant described requires the recipient to have a certificate, but the originator may have a static key pair (with the public key placed in a certificate) or an ephemeral key pair
IETF	2984	Use of the CAST-128 Encryption Algorithm in CMS	RFC	Oct 2000	This document specifies how to incorporate CAST-128 (RFC2144) into the S/MIME Cryptographic Message Syntax (CMS) as an additional algorithm for symmetric encryption. The relevant OIDs and processing steps are provided so that CAST-128 may be included in the CMS specification (RFC2630) for symmetric content and key encryption.
IETF	2876	Use of the KEA and SKIPJACK Algorithms in CMS July 2000	RFC		This document describes the conventions for using the Key Exchange Algorithm (KEA) and SKIPJACK encryption algorithm in conjunction with the Cryptographic Message Syntax [CMS] enveloped-data and encrypted-data content types.

IETF	3058	Use of the IDEA Encryption Algorithm in CMS	RFC	Feb 2001	This memo specifies how to incorporate International Data Encryption Algorithm (IDEA) into CMS or S/MIME as an additional strong algorithm for symmetric encryption. For organizations who make use of IDEA for data security purposes it is of high interest that IDEA is also available in S/MIME. The intention of this memo is to provide the OIDs and algorithms required that IDEA can be included in S/MIME for symmetric content and key encryption.
IETF	3156	MIME Security with OpenPGP	RFC	August2001	This document describes how the OpenPGP Message Format can be used to provide privacy and authentication using the Multipurpose Internet Mail Extensions (MIME) security content types described in RFC 1847.
IETF	3185	Reuse of CMS Content Encryption Keys	RFC	Oct 2001	This document describes a way to include a key identifier in a CMS (Cryptographic Message Syntax) enveloped data structure, so that the content encryption key can be re-used for further enveloped data packets.
IETF	3217	Triple-DES and RC2 Key Wrapping	RFC	Dec 2001	This document specifies the algorithm for wrapping one Triple-DES key with another Triple-DES key and the algorithm for wrapping one RC2 key with another RC2 key. These key wrap algorithms were originally published in section 12.6 of RFC 2630. They are republished since these key wrap algorithms have been found to be useful in contexts beyond those supported by RFC 2630.
IETF	3278	Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)	RFC	April 2002	This document describes how to use Elliptic Curve Cryptography (ECC) public-key algorithms in the Cryptographic Message Syntax (CMS). The ECC algorithms support the creation of digital signatures and the exchange of keys to encrypt or authenticate content. The definition of the algorithm processing is based on the ANSI X9.62 standard, developed by the ANSI X9F1 working group, the IEEE 1363 standard, and the SEC 1 standard.
IETF	3394	Advanced Encryption Standard (AES) Key Wrap Algorithm	RFC	Sept 2002	This document specifies the conventions for using the Camellia encryption algorithm for encryption with the Cryptographic Message Syntax (CMS).
IETF	3537	Wrapping a Hashed Message Authentication Code (HMAC) key with a Triple-Data Encryption Standard (DES) Key or an Advanced Encryption Standard (AES)	RFC	May 2003	This document defines two methods for wrapping an HMAC (Hashed Message Authentication Code) key. The first method defined uses a Triple DES (Data Encryption Standard) key to encrypt the HMAC key. The second method defined uses an AES (Advanced Encryption Standard)key to encrypt the HMAC key. One place that such an algorithm is used is for the Authenticated Data type in CMS (Cryptographic Message Syntax).
IETF	3565	Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)	RFC	July 2003	This document specifies the conventions for using the Advanced Encryption Standard (AES) algorithm for encryption with the Cryptographic Message Syntax (CMS).

IETF	3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec	RFC	Sept 2003	A Message Authentication Code (MAC) is a key-dependent one way hash function. One popular way to construct a MAC algorithm is to use a block cipher in conjunction with the Cipher-Block-Chaining (CBC) mode of operation. The classic CBC-MAC algorithm, while secure for messages of a pre-selected fixed length, has been shown to be insecure across messages of varying lengths such as the type found in typical IP datagrams. This memo specifies the use of AES in CBC mode with a set of extensions to overcome this limitation.
IETF	3602	The AES-CBC Cipher Algorithm and Its Use with IPsec	RFC	Sept 2003	This document describes the use of the Advanced Encryption Standard (AES) Cipher Algorithm in Cipher Block Chaining (CBC) Mode, with an explicit Initialization Vector (IV), as a confidentiality mechanism within the context of the IPsec Encapsulating Security Payload (ESP).
IETF	3657	Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)	RFC	Jan 2004	This document specifies the conventions for using the Camellia encryption algorithm for encryption with the Cryptographic Message Syntax (CMS).
IETF	3664	The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)	RFC	Jan 2004	Some implementations of IP Security (IPsec) may want to use a pseudo-random function derived from the Advanced Encryption Standard (AES). This document describes such an algorithm, called AES-XCBC-PRF-128.
IETF	3686	Using Advanced Encryption Standard (AES) Counter Mode With Ipsec Encapsulating Security Payload (ESP)	RFC	Jan 2004	This document describes the use of Advanced Encryption Standard (AES) Counter Mode, with an explicit initialization vector, as an Ipsec Encapsulating Security Payload confidentiality mechanism.
IETF	3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	RFC	June 2004	This document describes a symmetric encryption protocol that supplements the protocols described in the User-based Security Model (USM), which is a Security Subsystem for version 3 of the Simple Network Management Protocol for use in the SNMP Architecture. The symmetric encryption protocol described in this document is based on the Advanced Encryption Standard (AES) cipher algorithm used in Cipher FeedBack Mode (CFB), with a key size of 128 bits.
IETF	3957	Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4	RFC	March 2005	
IETF	3961	Encryption and Checksum specifications for Kerberos 5	RFC	Feb 2005	This document describes a framework for defining encryption and checksum mechanisms for use with the Kerberos protocol, defining an abstraction layer between the Kerberos protocol and related protocols, and the actual mechanisms themselves. The document also defines several mechanisms. Some are taken from RFC 1510, modified in form to fit this new framework and occasionally modified in content when the old specification was incorrect.

IETF	3962	Advanced Encryption Standard (AES) Encryption for Kerberos 5	RFC	Feb 2005	This document is a specification for the addition of the AES algorithm to the Kerberos cryptosystem suite.
IETF	3972	Cryptographically Generated Addresses	RFC	March 2005	
IETF	4010	Use of the SEED Encryption Algorithm in Cryptographic Message Syntax (CMS)	RFC	Feb 2005	This document specifies the conventions for using the SEED encryption algorithm for encryption with the Cryptographic Message Syntax (CMS).
IETF	4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	RFC	Dec 2005	The IPsec series of protocols makes use of various cryptographic algorithms in order to provide security services. The Encapsulating Security Payload (ESP) and the Authentication Header (AH) provide two mechanisms for protecting data being sent over and IPsec Security Association (SA).
IETF	4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	RFC	Dec 2005	This document defines the current set of algorithms that are mandatory to implement as part of IKEv2, as well as algorithms that should be implemented because they may be promoted to mandatory at some future time.
IETF	4308	Cryptographic Suites for IPsec	RFC	Dec 2005	This document specifies optional suites of algorithms and attributes that can be used to simplify the administration of IPsec when used in manual keying mode, with IKEv1 or with IKEv2.
IETF	4309	Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)	RFC	Dec 2005	This document describes the use of Advanced Encryption Standard (AES) in Counter with CBC-MAC (CCM) Mode, with an explicit initialization vector (IV), as an IPsec Encapsulating Security Payload (ESP) mechanism to provide confidentiality, data origin authentication, and connectionless integrity.
IETF	4312	The Camellia Cipher Algorithm and Its Use With IPsec	RFC	Dec 2005	This document describes the use of the Camellia block cipher algorithm in Cipher Block Chaining Mode, with an explicit Initialization Vector, as a confidentiality mechanism within the context of the IPsec Encapsulating Security Payload (ESP).
IETF	4359	The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)	RFC	Jan 2006	This memo describes the use of the RSA digital signature algorithm as an authentication algorithm within the revised IP Encapsulating Security Payload (ESP) as described in RFC 4303 and the revised IP Authentication Header (AH) as described in RFC 4302.

IETF	4490	Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)	RFC	May 2006	This document describes the conventions for using the cryptographic algorithms GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 with the Cryptographic Message Syntax (CMS). The CMS is used for digital signature, digest, authentication, and encryption of arbitrary message contents.
IETF	4494	The AES-CMAC-96 Algorithm and Its Use with IPsec	RFC	June 2006	This memo specifies the use of CMAC mode on the authentication mechanism of the IPsec Encapsulating Security Payload (ESP) and the Authentication Header (AH) protocols. This new algorithm is named AES-CMAC-96.
IETF	4509	Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)	RFC	May 2006	This document specifies how to use the SHA-256 digest type in DNS Delegation Signer (DS) Resource Records (RRs). DS records, when stored in a parent zone, point to DNSKEYs in a child zone.
IETF	4537	Kerberos Cryptosystem Negotiation Extension	RFC	Jun 2006	This document specifies an extension to the Kerberos protocol as defined in RFC 4120, in which the client can send a list of supported encryption types in decreasing preference order, and the server then selects an encryption type that is supported by both the client and the server.
IETF	4543	The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH	RFC	May 2006	This memo describes the use of the Advanced Encryption Standard (AES) GMAC as a mechanism to provide data origin authentication, but not confidentiality, within the IPsec Encapsulating Security Payload (ESP) and Authentication Header (AH).
IEEE	1619.1	Authenticated Encryption with Length Expansion for Storage Devices MP			This standard specifies requirements for cryptographic modules that provide encryption and authentication for data contained within storage media. Furthermore, this standard facilitates interchange between two compliant solutions through the specification of standard encryption algorithms
ETSI	SAGE-0008	SAGE Cryptographic algorithm for Public NetworkOperators	MI		
ETSI	101 053-1	Security Algorithms Group of Experts (SAGE); Rules forthe management of the TETRA standard encryption algorithms; Part 1:TEA1	TR		
ETSI	SAGE-00010-2	Standard Trans European Trunked RAdio (TETRA)air interface encryption algorithm TEA1 and TEA2	MI		

ETSI	101 053-2	Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 2: TEA2	TR		
ETSI	101 052	Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard authentication and key management algorithm set TAA1	TR		
ETSI	SAGE-00011-2	SAGE Trans European Trunked RAdio (TETRA) set of air interface authentication and key management algorithms TAA1	MI		
ETSI	101 054	Security Algorithms Group of Experts (SAGE); Rules for the management of the HIPERLAN Standard Encryption Algorithm (HSEA)	TR		
ETSI	SAGE-00012-2	SAGE Standard air interface encryption algorithm for HIPERLAN	MI		
ETSI	101 375	Security Algorithms Group of Experts (SAGE); Report on the specification, evaluation and usage of the GSM GPRS Encryption Algorithm (GEA)	TR		
ETSI	SAGE-00015-2	Security Algorithms Group of Experts (SAGE); GPRS encryption algorithm	MI		

ETSI	101 690	Security Algorithms Group of Experts (SAGE); Rules for the management of the GSM CTS standard Authentication and Key Generation Algorithms (CORDIAL)	TR		
ETSI	SAGE-00016-2	Security Algorithms Group of Experts (SAGE); CTS Authentication and Key Generation Algorithm	MI		
ETSI	SAGE-00017-2	/Security Algorithms Group of Experts (SAGE); TEA3 and TEA4 Security Algorithms	MI		
ETSI	101 053-3	Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 3:TEA3	TR		
ETSI	101 053-4	Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 4: TEA4	TR		
ETSI	SAGE-00018	SAGE Design of the 3GPP Encryption and Integrity algorithms	MI		
ETSI	101 740	Security algorithms Group of Experts (SAGE); Rules of the management of the standard GSM GPRS Encryption Algorithm 2 (GEA2)	TR		
ETSI	SAGE-00019-2	SAGE: Design of a Standard GSM GPRS Encryption algorithm 2 (GEA2)	MI		
ETSI	SAGE-00020-2	SAGE: Design of authentication algorithm for UMTS	MI		

Key Management					
ISO/IEC JTC 1/SC 27	11770-1	Key management – Part 1: Framework	IS	1996	Identifies the objectives of key management of key management, describes general models on which key management mechanisms are based, defines the basic concepts of key management common to all parts of this multi-part standard, defines key management services, identifies the characteristics of key management mechanisms, specifies requirements for the management of keying material during its life cycle and describes a framework for the management of keying material during its life cycle. The document addresses both - the automated and manual aspects of key management, including data elements and sequences of operations which are used to obtain key management services. It does not specify details of protocol exchanges.
ISO/IEC JTC 1/SC 27	11770-2 See also COR 1	Key management – Part 2: Mechanisms using symmetric techniques Draft Technical Corrigendum 1 (to be published 2005)	IS	1996	Defines key establishment mechanisms using symmetric cryptographic techniques (symmetric encipherment algorithms or cryptographic check functions). The document does not explicitly address the issue of interdomain key management. Furthermore, it does not define the implementation of key management mechanisms; there may be different products that comply with this part of ISO/IEC 11770 and yet are not compatible.
ISO/IEC JTC 1/SC 27	11770-3	Key management - Part 3: Mechanisms using asymmetric techniques	IS	1999	Defines key management mechanisms based on asymmetric cryptographic techniques. Some of the mechanisms of this part of ISO/IEC 11770 are based on the corresponding authentication mechanisms in ISO/IEC 9798-3. It does not cover aspects of key management such as key lifecycle management and mechanisms to store, archive, delete, destruct, etc. keys. It also does not cover the implementations of the transformations used in the key management mechanisms.
ISO/IEC JTC 1/SC 27	11770-4	Key management – Part 4: Mechanisms based on weak secrets	FCD		Defines key establishment mechanisms based on weak secrets. It specifies cryptographic techniques specifically designed to establish one or more secret keys based on a weak secret derived from a memorized password, while preventing off-line brute-force attacks associated with the weak secret. It does not cover aspects of key management such as lifecycle management of weak secrets, strong secrets and established secret keys, and mechanisms to store, archive, delete, destroy, etc. weak secrets, strong secrets, and established secret keys.
ITU-T SG17	X.1035 (X.pak)	Password authenticated key exchange protocol	Rec	Dec 2006	This Recommendation specifies a protocol, which ensures mutual authentication of both parties in the act of establishing a symmetric cryptographic key via Diffie-Hellman exchange.
IETF	3129	Requirements for Kerberized Internet Negotiation of Keys	RFC	June 2001	The goal of this document is to produce a streamlined, fast, easily managed, and cryptographically sound protocol without requiring public key

IETF	3547	The Group Domain of Interpretation	RFC	July 2003	This document presents an ISAMKP Domain of Interpretation (DOI) for group key management to support secure group communications. The GDOI manages group security associations, which are used by IPSEC and potentially other data security protocols running at the IP or application layers. These security associations protect one or more key-encrypting keys, traffic-encrypting keys, or data shared by group members.
IETF	3560	Use of the RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS)	RFC	July 2003	This document describes the conventions for using the RSAES-OAEP key transport algorithm with the Cryptographic Message Syntax (CMS). The CMS specifies the enveloped-data content type, which consists of an encrypted content and encrypted content-encryption keys for one or more recipients. The RSAES-OAEP key transport algorithm can be used to encrypt content-encryption keys for intended recipients.
IETF	3634	Key Distribution Center (KDC) Server Address Sub-option for the Dynamic Host Configuration Protocol (DHCP) CableLabs Client Configuration (CCC) Option	RFC	Dec 2003	This document defines a new sub-option for the CableLabs Client Configuration (CCC) Dynamic Host Configuration Protocol (DHCP) option code for conveying the network addresses of Key Distribution Center (KDC) servers.
IETF	3830	MIKEY: Multimedia Internet KEYing	RFC	Aug 2004	This document describes a key management scheme that can be used for real-time applications (both for peer-to-peer communication and group communication). In particular, its use to support the Secure Real-time Transport Protocol is described in detail.
IETF	4279	Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)	RFC	Dec 2005	This document specifies three sets of new ciphersuites for the TLS protocol to support authentication based on pre-shared keys. The first set of ciphersuites uses only symmetric key operations for authentication. The second set uses a Diffie-Hellman exchange authenticated with a pre-shared key, and the third set combines public key authentication of the server with pre-shared key authentication of the client.
IETF	4402	A Pseudo-Random Function (PRF) for the Kerberos V Generic Security Service Application Program Interface Mechanism	RFC	Feb 2006	This document defines the Pseudo-Random Function (PRF) for the Kerberos V mechanism for the Generic Security Service Application Program Interface (GSS-API), based on the PRF defined for the Kerberos V cryptographic framework, for keying application protocols given an established Kerberos V GSS-API security context.
IETF	4419	Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol	RFC	Mar 2006	This memo describes a new key exchange method for the Secure Shell SSH) protocol. It allows the SSH server to propose new groups on which to perform the Diffie-Hellman key exchange to the client.
IETF	4430	Kerberized Internet Negotiation of Keys (KINK)	RFC	Mar 2006	KINK defines a low-latency, computationally inexpensive, easily managed, and cryptographically sound protocol to establish and maintain security associations using the Kerberos authentication system.

IETF	4432	RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol	RFC	Mar 2006	This memo describes a key-exchange method for the Secure Shell (SSH)protocol based on Rivest-Shamir-Adleman (RSA) public-key encryption. It uses much less client CPU time than the Diffie-Hellman algorithm specified as part of the core protocol, and hence is particularly suitable for slow client systems.
IETF	4434	The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)	RFC	Feb 2006	Some implementations of IP Security (IPsec) may want to use a pseudo-random function derived from the Advanced Encryption Standard.
IETF	4535	GSAKMP: Group Secure Association Key Management Protocol	RFC	Jun 2006	This document specifies the Group Secure Association Key Management Protocol (GSAKMP). The GSAKMP provides a security framework for creating and managing cryptographic groups on a network. It provides mechanisms to disseminate group policy and authenticate users, rules to perform access control decisions during group establishment and recovery, capabilities to recover from the compromise of group members, delegation of group security functions, and capabilities to destroy the group. It also generates group keys.
IETF	4555	IKEv2 Mobility and Multihoming Protocol (MOBIKE)	RFC	Jun 2006	This document describes the MOBIKE protocol, a mobility and multihoming extension to Internet Key Exchange (IKEv2). MOBIKE allows the IP addresses associated with IKEv2 and tunnel mode IPsec Security Associations to change.
IETF	4567	Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)	RFC	July 2006	This document defines general extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP) to carry messages, as specified by a key management protocol, in order to secure the media.
Miscellaneous cryptographic mechanisms					
ISO/IEC JTC 1/SC 27	18031	Random bit generation	IS	2005	Specifies a conceptual model for a random bit generator for cryptographic purposes, together with its elements.
ISO/IEC JTC 1/SC 27	18032	Prime number generation	IS	2005	Presents methods for generating prime numbers as required in cryptographic protocols and algorithms.
IETF	2875	Diffie-Hellman Proof-of-Possession Algorithms	RFC	July 2000	This document describes two methods for producing an integrity check = value from a Diffie-Hellman key pair. This behavior is needed for such operations as creating the signature of a PKCS #10 certification request. These algorithms are designed to provide a proof-of- possession rather than general purpose signing.
IETF	4449	Securing Mobile IPv6 Route Optimization Using a Static Shared Key	RFC	June 2006	A mobile node and a correspondent node may preconfigure data useful for precomputing a Binding Management Key that can subsequently be used for authorizing Binding Updates.

Integrity mechanisms					
Check systems					
ISO/IEC JTC 1/SC 27	7064	Check character systems	IS	2003	Specifies a set of check character systems capable of protecting strings against errors which occur when people copy or key data.
Hash Functions					
ISO/IEC JTC 1/SC 27	10118-1	Hash-functions – Part 1: General	IS	2000	This part of ISO/IEC 10118 contains definitions, symbols, abbreviations and requirements which are common to all the other parts of ISO/IEC 10118.
ISO/IEC JTC 1/SC 27	10118-2	Hash-functions – Part 2: Hash-functions using an n-bit block cipher algorithm	IS	2000	Specifies hash-functions which make use of an n-bit block cipher algorithm. Two types of hash-functions are specified. The first provides hash- codes of length smaller than or equal to n, where n is the block-length of the algorithm used. The second provides hash-codes of length less than or equal to 2n.
ISO/IEC JTC 1/SC 27	10118-3	Hash-functions – Part 3: Dedicated hash-functions	IS	2004	Specifies dedicated hash-functions based on the iterative use of a round-function. Seven distinct round-functions are specified, giving rise to distinct dedicated hash-functions.
ISO/IEC JTC 1/SC 27	10118-4	Hash-functions – Part 4: Hash-functions using modular arithmetic	IS	1998	Specifies two collision-resistant hash-functions which make use of modular arithmetic employing a round-function using a composite modulus as a product of two large primes, and a reduction-function using a prime number only. These hash-functions compress messages of arbitrary but limited length to a hash-code whose length is determined by the length of the prime number used in the reduction-function. Thus, the hash- code is easily scaled to the input length of any mechanism (e.g., signature algorithm, identification scheme).
IETF	3874	A 224-bit One-way Hash Function: SHA-224	RFC	Sept 2004	This document specifies a 224-bit one-way hash function, called SHA-224. SHA-224 is based on SHA-256, but it uses a different initial value and the result is truncated to 224 bits.
Non-repudiation mechanisms					
ISO/IEC JTC 1/SC 27	13888-1	Non-repudiation – Part 1: General	IS	2004	Describes a model for non-repudiation mechanisms providing evidence based on cryptographic check values generated by using symmetric or asymmetric cryptographic techniques.
ISO/IEC JTC 1/SC 27	13888-2	Non-repudiation – Part 2: Using symmetric techniques	IS	1998	Specifies mechanisms for generation, exchange, and validation non-repudiation tokens using symmetric techniques, relying on the existence of an on-line mutually Trusted Third Party, available in an exchange.

ISO/IEC JTC 1/SC 27	13888-3	Non-repudiation – Part 3: Using asymmetric techniques	IS	1997	This part of ISO/IEC 13888 specifies two mechanisms for the provision of non-repudiation services using asymmetric cryptographic techniques.
Trusted Third party mechanisms					
ITU-T SG17 ISO/IEC JTC 1/SC 27	X.842 14516	Guidelines for the use and management of Trusted Third Party services	Rec TR	2002	Provides guidance for the use and management of TTPs, 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. It is intended primarily for system managers, developers, TTP operators and enterprise users to select those
Digital Signature mechanisms					
ISO/IEC JTC 1/SC 27	9796-2	Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms	IS	2002	Specifies a digital signature scheme for messages of any length.
ISO/IEC JTC 1/SC 27	14888-1	Digital signatures with appendix - Part 1: General	IS	1999	This part of the standard covers general principles and requirements for digital signature with appendix.
ISO/IEC JTC 1/SC 27	14888-2	Digital signatures with appendix - Part 2: Integer factorization based mechanisms	IS	1999	This standard specifies the fundamental structure, the mathematical functions and possible data objects which constitute the signature and verification processes of an identity-based digital signature mechanism with appendix for messages of arbitrary length.
ISO/IEC JTC 1/SC 27	14888-3	Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms	IS	1999	Specifies digital signature mechanisms with appendix whose security is based on the discrete logarithm problem. The standard provides a general description of a digital signature with appendix mechanism, and a variety of mechanisms that provide digital signatures with appendix.
IETF	3125	Electronic Signature Policies	RFC	Sept 2001	This document defines signature policies for electronic signatures. A signature policy is a set of rules for the creation and validation of an electronic signature, under which the validity of signature can be determined. A given legal/contractual context may recognize a particular signature policy as meeting its requirements.
IETF	3126	Electronic Signature Formats for long term electronic signatures	RFC	Sept 2001	This document defines the format of an electronic signature that can remain valid over long periods. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (i.e., repudiates the validity of the signature).

Time Stamping					
ISO/IEC JTC 1/SC 27	18014-1	Time stamping services – Part 1: Framework	IS	2002	Identifies the objective of a time-stamping authority, describes a general model on which time-stamping services are based, defines time-stamping services and the basic protocols of time-stamping, specifies the basic protocols between the involved entities and describes linking protocols for a Time-stamping Authority.
ISO/IEC JTC 1/SC 27	18014-2	Time stamping services – Part 2: Mechanisms producing independent tokens	IS	2002	This standard defines time-stamping mechanisms that produce independent tokens, that is proofs of existence that can be verified one by one.
ISO/IEC JTC 1/SC 27	18014-3	Time stamping services – Part 3: Mechanisms producing linked tokens	IS	2004	Describes a general model for time-stamping services producing linked tokens and the basic components used to construct a time-stamping service of this type, it defines the data structures and protocols used to interact with a time-stamping service of this type, and it describes specific instances of such time-stamping services.
IETF	3628	Policy Requirements for Time-Stamping Authorities (TSAs)	RFC	Nov 2003	This document defines requirements for a baseline time-stamp policy for Time-Stamping Authorities (TSAs) issuing time-stamp tokens, supported by public key certificates, with an accuracy of one second or better. A TSA may define its own policy which enhances the policy defined in this document. Such a policy shall incorporate or further constrain the requirements identified in this document.

Network security

Organization	Reference	Title	Status	Date	Abstract
ISO/IEC JTC 1	18028-1	Network Security Management	FDIS	2006	Defines and describes the concepts associated with, and provides management guidance on, network security
ITU-T SG 17 ISO/IEC JTC 1	X.805 18028-2	Security architecture for systems providing end-to-end communications	Rec IS	2003	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.

ISO/IEC JTC 1	18028-3	IT network security – Part 3 - Securing communications between networks using security gateways	IS	2005	Defines techniques for securing information flows between networks using security gateways.
ISO/IEC JTC 1/SC 27	18028-4	IT network security – Part 4: Securing remote access	IS	2005	Describes a method to remotely connect a computer either to another computer or to a network using public networks and its implication to IT security.
ISO/IEC JTC 1	18028-5	IT network security – Part 5 – Securing communications across networks using VPNs	FDIS	2006	Defines techniques for securing inter-network connections that are established using virtual private networks.

Transport Layer security

Organization	Reference	Title	Status	Date	Abstract
IETF	4507	Transport Layer Security (TLS) Session Resumption without Server-Side State	RFC	May 2006	This document describes a mechanism that enables the Transport Layer Security (TLS) server to resume sessions and avoid keeping per-client session state. The TLS server encapsulates the session state into a ticket and forwards it to the client. The client can subsequently resume a session using the obtained ticket.

Security protocol standards

Organization	Reference	Title	Status	Date	Abstract
ITU-T SG 17 ISO/IEC JTC 1/SC 6	X.273 11577	Network layer security protocol	Rec IS	1994 1995	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.
ITU-T SG 17 ISO/IEC JTC 1/SC 6	X.274 IS10736	Transport layer security protocol	Rec IS	1994 1995	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 labeling and assigned attributes, such as cryptographic keys.

ITU-T SG 16	T.123 Annex B	Extended Transport Connections	Rec.	1999	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.
IETF	2246	The TLS Protocol Version 1.0	RFC	Jan 1999	This document specifies Version 1.0 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
IETF	2712	Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)	RFC	Oct 1999	The 40-bit ciphersuites defined in this memo are included only for the purpose of documenting the fact that those ciphersuite codes have already been assigned. 40-bit ciphersuites were designed to comply with US-centric, and now obsolete, export restrictions. They were never secure, and nowadays are inadequate even for casual applications. Implementation and use of the 40-bit ciphersuites defined in this document, and Elsewhere, is strongly discouraged.
IETF	2817	Upgrading to TLS Within HTTP/1.1	RFC	May 2000	This memo explains how to use the Upgrade mechanism in HTTP/1.1 to initiate Transport Layer Security (TLS) over an existing TCP connection. This allows unsecured and secured HTTP traffic to share the same well known port (in this case, http: at 80 rather than https: at 443). It also enables "virtual hosting", so a single HTTP + TLS server can disambiguate traffic intended for several hostnames at a single IP address.
IETF	2818	HTTP Over TLS	RFC	May 2000	This memo describes how to use TLS to secure HTTP connections over the Internet. Current practice is to layer HTTP over SSL (the predecessor to TLS), distinguishing secured traffic from insecure traffic by the use of a different server port. This document documents that practice using TLS.
IETF	3157	Securely Available Credentials - Requirements	RFC	Aug 2001	This document describes requirements to be placed on Securely Available Credentials (SACRED) protocols.
IETF	3164	The BSD syslog Protocol	RFC	Aug 2001	This document describes the observed behavior of the syslog protocol. This protocol has been used for the transmission of event notification messages across networks for many years. While this protocol was originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, its value to operations and management has led it to be ported to many other operating systems as well as being embedded into many other networked devices.
IETF	3195	Reliable Delivery for syslog	RFC	Nov 2001	The BSD Syslog Protocol describes a number of service options related to propagating event messages. This memo describes two mappings of the syslog protocol to TCP connections, both useful for reliable delivery of event messages. The first provides a trivial mapping maximizing backward compatibility. The second provides a more complete mapping. Both provide a degree of robustness and security in message delivery that is unavailable to the usual UDP-based syslog protocol, by providing encryption and authentication over a connection-oriented protocol.

IETF	3268	Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)	RFC	June 2002	This document proposes several new ciphersuites. At present, the symmetric ciphers supported by Transport Layer Security (TLS) are RC2, RC4, International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES), and triple DES. The protocol would be enhanced by the addition of Advanced Encryption Standard (AES) ciphersuites.
IETF	3436	Transport Layer Security over Stream Control Transmission Protocol	RFC	Dec 2002	This document describes the usage of the Transport Layer Security (TLS) protocol, as defined in RFC 2246, over the Stream Control Transmission Protocol (SCTP), as defined in RFC 2960 and RFC 3309.
IETF	3456	Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode	RFC	Jan. 2003	This memo explores the requirements for host configuration in IPsec tunnel mode, and describes how the Dynamic Host Configuration Protocol (DHCPv4) may be leveraged for configuration.
IETF	3546	Transport Layer Security (TLS) Extensions	RFC	June 2003	This document describes extensions that may be used to add functionality to Transport Layer Security (TLS). It provides both generic extension mechanisms for the TLS handshake client and server hellos, and specific extensions using these generic mechanisms. The extensions may be used by TLS clients and servers.
IETF	3585	IPsec Configuration Policy Information Model	RFC	Aug 2003	This document presents an object-oriented information model of IP Security (IPsec) policy designed to facilitate agreement about the content and semantics of IPsec policy, and enable derivations of task-specific representations of IPsec policy such as storage schema, distribution representations, and policy specification languages used to configure IPsec-enabled endpoints. The information model described in this document models the configuration parameters defined by IPSec. The information model also covers the parameters found by the Internet Key Exchange protocol (IKE).
IETF	3586	IP Security Policy (IPSP) Requirements	RFC	Aug 2003	This document describes the problem space and solution requirements for developing an IP Security Policy (IPSP) configuration and management framework. The IPSP architecture provides a scalable, decentralized framework for managing, discovering and negotiating the host and network security policies that govern access, authorization, authentication, confidentiality, data integrity, and other IP Security properties.
IETF	3711	The Secure Real-time Transport Protocol (SRTP)	RFC	March 2004	This document describes the Secure Real-time Transport Protocol SRTP), a profile of the Real-time Transport Protocol (RTP), which can provide confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP, the Real-time Transport Control Protocol (RTCP).
IETF	3723	Securing Block Storage Protocols over IP	RFC	Apr 2004	This document discusses how to secure block storage and storage discovery protocols running over IP (Internet Protocol) using Ipsec and IKE (Internet Key Exchange).
IETF	3748	Extensible Authentication Protocol	RFC	Jun 2004	This document defines the Extensible Authentication Protocol (EAP), an authentication framework which supports multiple authentication methods. EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP.

IETF	3749	Transport Layer Security Protocol Compression Methods	RFC	May 2004	The Transport Layer Security (TLS) protocol (RFC 2246) includes features to negotiate selection of a lossless data compression method as part of the TLS Handshake Protocol and to then apply the algorithm associated with the selected method as part of the TLS Record Protocol. TLS defines one standard compression method which specifies that data exchanged via the record protocol will not be compressed. This document describes an additional compression method associated with a lossless data compression algorithm for use with TLS, and it describes a method for the specification of additional TLS compression methods.
IETF	3760	Securely Available Credentials (SACRED) - Credential Server Framework	RFC	April 2004	As the number, and more particularly the number of different types, of devices connecting to the Internet increases, credential mobility becomes an issue for IETF standardization. This document responds to the requirements on protocols for secure exchange of credentials listed in RFC 3157, by presenting an abstract protocol framework.
IETF	3767	Securely Available Credentials Protocol	RFC	June 2004	This document describes a protocol whereby a user can acquire cryptographic credentials (e.g., private keys, PKCS #15 structures) from a credential server, using a workstation that has locally trusted software installed, but with no user-specific configuration. The protocol's payloads are described in XML. This memo also specifies a Blocks Extensible Exchange Protocol (BEEP) profile of the protocol. Security requirements are met by mandating support for TLS and/or DIGEST-MD5 (through BEEP).
IETF	3788	Security Considerations for Signaling Transport (SIGTRAN) Protocols	RFC	June 2004	This document discusses how Transport Layer Security (TLS) and Ipsec can be used to secure communication for SIGTRAN protocols. The maingoal is to recommend the minimum security means that a SIGTRAN node must implement in order to attain secured communication. The support of IPsec is mandatory for all nodes running SIGTRAN protocols. TLS support is optional.
IETF	3943	Transport Layer Security (TLS) Protocol Compression Using Lempel-Ziv-Stac (LZS)	RFC	Nov 2004	The Transport Layer Security (TLS) protocol (RFC 2246) includes features to negotiate selection of a lossless data compression method as part of the TLS Handshake Protocol and then to apply the algorithm associated with the selected method as part of the TLS Record Protocol. TLS defines one standard compression method, which specifies that data exchanged via the record protocol will not be compressed. This document describes an additional compression method associated with the Lempel-Ziv-Stac (LZS) lossless data compression algorithm for use with TLS. This document also defines the application of the LZS algorithm to the TLS Record Protocol.
IETF	4016	Protocol for Carrying Authentication and Network Access (PANA) Threat Analysis and Security Requirements	RFC	March 2005	This document discusses the threats to protocols used to carry authentication for network access.
IETF	4017	Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs	RFC	March 2005	This document defines requirements for EAP methods used in IEEE 802.11 wireless LAN deployments.

IETF	4030	The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option	RFC	March 2005	The Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option (RFC 3046) conveys information between a DHCP Relay Agent and a DHCP server. This specification defines an authentication suboption for that option, containing a keyed hash in its payload. The suboption supports data integrity and replay protection for relayed DHCP messages.
IETF	4033	DNS Security Introduction and Requirements	RFC	March 2005	The Domain Name System Security Extensions (DNSSEC) add data origin authentication and data integrity to the Domain Name System. This document introduces these extensions and describes their capabilities and limitations. This document also discusses the services that the DNS security extensions do and do not provide.
IETF	4034	Resource Records for the DNS Security Extensions	RFC	March 2005	This document defines the public key (DNSKEY), delegation signer (DS), resource record digital signature (RRSIG), and authenticated denial of existence (NSEC) resource records. The purpose and format of each resource record is described in detail, and an example of each resource record is given.
IETF	4035	Protocol Modifications for the DNS Security Extensions	RFC	March 2005	This document is part of a family of documents that describe the DNS Security Extensions (DNSSEC). The DNS Security Extensions are a collection of new resource records and protocol modifications that add data origin authentication and data integrity to the DNS
IETF	4082	Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction	RFC	June 2005	This document introduces Timed Efficient Stream Loss-tolerant Authentication (TESLA). TESLA allows all receivers to check the integrity and authenticate the source of each packet in multicast or broadcast data streams. TESLA requires no trust between receivers, uses low-cost operations per packet at both sender and receiver, can tolerate any level of loss without retransmissions, and requires no per-receiver state at the sender. TESLA can protect receivers against denial of service attacks in certain circumstances. Each receiver must be loosely time-synchronized with the source in order to verify messages, but otherwise receivers do not have to send any messages. TESLA alone cannot support non-repudiation of the data source to third parties. This informational document is intended to assist in writing standardizable and secure specifications for protocols based on TESLA in different contexts.
IETF	4121	The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2	RFC	July 2005	This document defines protocols, procedures, and conventions to be employed by peers implementing the Generic Security Service Application Program Interface (GSS-API) when using the Kerberos Version 5 mechanism.
IETF	4132	Addition of Camellia Cipher Suites to Transport Layer Security (TLS)	RFC	July 2005	This document proposes the addition of new cipher suites to the Transport Layer Security (TLS) protocol to support the Camellia encryption algorithm as a bulk cipher algorithm

IETF	4217	Securing FTP with TLS	RFC	Oct. 2005	Describes a mechanism that can be used by FTP clients and servers to implement security and authentication using the TLS protocol defined by RFC 2246, "The TLS Protocol Version 1.0.", and the extensions to the FTP protocol defined by RFC 2228, "FTP Security Extensions".
IETF	4252	The Secure Shell (SSH)Authentication Protocol	RFC	Jan 2006	This document describes the SSH authentication protocol framework and public key, password, and host-based client authentication methods.
IETF	4253	The Secure Shell (SSH) Transport Layer Protocol	RFC	Jan 2006	This document describes the SSH transport layer protocol, which typically runs on top of TCP/IP.
IETF	4254	The Secure Shell (SSH) Connection Protocol	RFC	Jan 2006	This document describes the SSH Connection Protocol.
IETF	4255	Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints	RFC	Jan 2006	This document describes a method of verifying Secure Shell (SSH) host keys using Domain Name System Security (DNSSEC).
IETF	4256	Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)	RFC	Jan 2006	This document describes a general purpose authentication method for the SSH protocol, suitable for interactive authentications where the authentication data should be entered via a keyboard (or equivalent alphanumeric input device).
IETF	4303	IP Encapsulating Security Payload (ESP)	RFC	Dec 2005	This document describes an updated version of the Encapsulating Security Payload (ESP) protocol, which is designed to provide a mix of security services in IPv4 and IPv6.
IETF	4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)	RFC	Dec 2005	This document describes extensions to the Internet IP Security Domain of Interpretation (DOI) for the ISAKMP.
IETF	4306	Internet Key Exchange (IKEv2) Protocol	RFC	Dec 2005	This document describes version 2 of the Internet Key Exchange (IKE)protocol.
IETF	4344	The Secure Shell (SSH) Transport Layer Encryption Modes	RFC	Jan 2006	Researchers have discovered that the authenticated encryption portion of the current SSH Transport Protocol is vulnerable to several attacks. This document describes new symmetric encryption methods for the Secure Shell (SSH) Transport Protocol and gives specific recommendations on how frequently SSH implementations should rekey.
IETF	4345	Improved Arcfour Modes for the Secure Shell (SSH) Transport Layer Protocol	RFC	Jan 2006	This document specifies methods of using the Arcfour cipher in the Secure Shell (SSH) protocol that mitigate the weakness of the cipher's key-scheduling algorithm.

IETF	4346	The Transport Layer Security (TLS) Protocol Version 1.1	RFC	Apr 2006	This document specifies Version 1.1 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
IETF	4347	Datagram Transport Layer Security	RFC	Apr 2006	The DTLS protocol provides communications privacy for datagram protocols. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
IETF	4366	This memo describes the use of the RSA digital signature algorithm as an authentication algorithm within the revised IP Encapsulating Security Payload as described in RFC 4303 and the revised IP Authentication Header as described in RFC 4302.	RFC	Apr 2006	This document describes extensions that may be used to add functionality to Transport Layer Security.
IETF	4568	Session Description Protocol (SDP) Security Descriptions for Media Streams	RFC	July 2006	This document defines a Session Description Protocol (SDP)cryptographic attribute for unicast media streams.
IEEE	802.1AE-2006	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security	Approved standard	Aug. 2006	This standard specifies how all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802® LANs to communicate. MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity.
IEEE	802.1af	Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control - Amendment 1: Authenticated Key Agreement for Media Access Control (MAC) Security	Approved standard	Feb. 2004	This standard will facilitate secure communication over publicly accessible LAN/MAN media for which security has not otherwise been defined, and allow the use of IEEE Std 802.1X, already widespread and supported by multiple vendors, in additional applications
IEEE	802.11i-2004	Local and metropolitan area networks- Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements	Approved standard	July 2004	Wireless LAN Medium Access Control (MAC) and Physical Layer specificationsAmendment 6: Medium Access Control (MAC) Security Enhancements
IEEE	1244.2	Media Management System (MMS) Session Security, Authentication, Initialization Protocol (SSAIP)	Special Publication	Dec. 2000	The syntax and semantics of the protocol messages that pass between the MMS clientor MMS module and the MM are described. Since this protocol is only used in the context of theMMS, this standard cannot be understood without a thorough understanding of its architecture asdescribed in IEEE Std 1244.1-2000

IEEE	P1667	Protocol for Authentication in Host Attachments of Transient Storage Devices	New Project	Nov. 2004	This project defines a standard protocol for secure authentication of dynamically attached devices, such as USB flash drives.

Secure messaging

Organization	Reference	Title	Status	Date	Abstract
ITU-T SG 17 ISO/IEC JTC 1/SC 6	F.400/X.400 10021-1	Message handling system and service overview	Rec IS	1999 2003	Provides an overview to define the overall system and service of an MHS and serves as a general overview of MHS 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.
ITU-T SG17 ISO/IEC JTC 1/SC 6	X.402 10021-2	Message Handling Systems (MHS): Overall architecture	REC IS	1999 2003	Specifies security procedures and Object Identifiers for use in MHS protocols to realize the services of *confidentiality, integrity, authentication, non-repudiation* and *access control*s identified as relevant to the Application Layer.
ITU-T SG17 ISO/IEC JTC 1/SC 6	X.419 10121-6	Message Handling Systems (MHS) – Protocol specifications	Rec IS	1999 2003	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.
ITU-T SG 17	F.440	Message Handling Services: The Voice Messaging Service. Annex G: Secure voice messaging elements of service. Annex H: Voice Messaging security overview	Rec	1992	Specifies the general, operational and quality of service aspects of the public international Voice Messaging service
ITU-T SG 17	X.440	Message Handling Systems (MHS) – Voice messaging system	Rec	1999	Specifies mechanisms, protocol and procedures for the exchange of objects between Voice User Agents on behalf of its direct user. The security services supported are *integrity, confidentiality, authentication and access control* identified as relevant to the Application Layer.
ITU-T SG 17 ISO/IEC JTC 1/SC 6	X.420 10121-7	Message Handling Systems (MHS) – Interpersonal messaging system	Rec IS	1999 2003	Specifies mechanisms, protocol and procedures for the exchange of objects between Interpersonal Messaging Users or User Agents on behalf of its direct user identified relevant to the Application Layer. The security services supported are *integrity, confidentiality, authentication and access control* identified as relevant to the Application Layer.

ITU-T SG 17 ISO/IEC JTC 1/SC 6	X.435 10121-9	Message Handling Systems (MHS) – Electronic data interchange messaging system	Rec IS	1999 1999	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.
IETF	2311	S/MIME Version 2 Message Specification	RFC	March 1998	S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a consistent way to send and receive secure MIME data. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption). The information in this document is historical material being published for the public record. It is not an IETF standard.
IETF	2312	S/MIME Version 2 Certificate Handling	RFC	March 1998	This memo describes the mechanisms S/MIME uses to create and validate keys using certificates.
IETF	2634	Enhanced Security Services for S/MIME	RFC	June 1999	This document describes four optional security service extensions for S/MIME. The services are: - signed receipts - security labels - secure mailing lists - signing certificates
IETF	3183	Domain Security Services using S/MIME	RFC	Oct 2001	This document describes how the S/MIME (Secure/Multipurpose Internet Mail Extensions) protocol can be processed and generated by a number of components of a communication system, such as message transfer agents, guards and gateways to deliver security services. These services are collectively referred to as 'Domain Security Services'
IETF	3218	Preventing the Million Message Attack on Cryptographic Message Syntax	RFC	Jan 2002	This memo describes a strategy for resisting the Million Message Attack.
IETF	3274	Compressed Data Content Type for Cryptographic Message Syntax (CMS)	RFC	June 2002	This document defines a format for using compressed data as a Cryptographic Message Syntax (CMS) content type. Compressing data before transmission provides a number of advantages, including the elimination of data redundancy which could help an attacker, speeding up processing by reducing the amount of data to be processed by later steps (such as signing or encryption), and reducing overall message size. Although there have been proposals for adding compression at other levels (for example at the MIME or SSL level), these don't address the problem of compression of CMS content unless the compression is supplied by an external means (for example by intermixing MIME and CMS).

IETF	3370	Cryptographic Message Syntax (CMS) Algorithms	RFC	August 2002	This document describes the conventions for using several cryptographic algorithms with the Cryptographic Message Syntax (CMS). The CMS is used to digitally sign, digest, authenticate, or encrypt arbitrary message contents.
IETF	3850	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling	RFC	July 2004	This document specifies conventions for X.509 certificate usage by Secure/Multipurpose Internet Mail Extensions (S/MIME) agents. S/MIME provides a method to send and receive secure MIME messages, and certificates are an integral part of S/MIME agent processing. S/MIME agents validate certificates as described in RFC 3280, the Internet X.509 Public Key Infrastructure Certificate and CRL Profile. S/MIME agents must meet the certificate processing requirements in this document as well as those in RFC 3280.
IETF	3851	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification	RFC	July 2004	This document defines Secure/Multipurpose Internet Mail Extensions (S/MIME) version 3.1. S/MIME provides a consistent way to send and receive secure MIME data. Digital signatures provide authentication, message integrity, and non-repudiation with proof of origin. Encryption provides data confidentiality. Compression can be used to reduce data size.
IETF	3852	Cryptographic Message Syntax (CMS)	RFC	July 2004	This document describes the Cryptographic Message Syntax (CMS). This syntax is used to digitally sign, digest, authenticate, or encrypt arbitrary message content.
IETF	3853	S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP). J. Peterson. July 2004	RFC	July 2004	RFC 3261 currently specifies 3DES as the mandatory-to-implement ciphersuite for implementations of S/MIME in the Session Initiation Protocol (SIP). This document updates the normative guidance of RFC 3261 to require the Advanced Encryption Standard (AES) for S/MIME.
IETF	3854	Securing X.400 Content with Secure/Multipurpose Internet Mail Extensions (S/MIME)	RFC	July 2004	This document describes a protocol for adding cryptographic signature and encryption services to X.400 content with Secure/Multipurpose Internet Mail Extensions (S/MIME).
IETF	3855	Transporting Secure/Multipurpose Internet Mail Extensions (S/MIME) Objects in X.400	RFC	July 2004	This document describes protocol options for conveying objects that have been protected using the Cryptographic Message Syntax (CMS) and Secure/Multipurpose Internet Mail Extensions S/MIME) version 3.1 over an X.400 message transfer system.
IETF	4056	Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS)	RFC	June 2005	This document specifies the conventions for using the RSASSA-PSS (RSA Probabilistic Signature Scheme) digital signature algorithm with the Cryptographic Message Syntax (CMS).
IETF	4134	Examples of S/MIME Messages	RFC	July 2005	This document gives examples of message bodies formatted using S/MIME. Specifically, it has examples of Cryptographic Message Syntax (CMS) objects and S/MIME messages (including the MIME formatting). It includes examples of many common CMS formats. The purpose of this document is to help increase interoperability for S/MIME and other protocols that rely on CMS.

IETF	4262	X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities	RFC	Dec 2005	This document defines a certificate extension for inclusion of Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities in X.509 public key certificates, as defined by RFC 3280.
IETF	4289	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures	BCP	Dec 2005	This document specifies IANA registration procedures for MIME external body access types and content-transfer-encodings.

PKI and Directory standards

Organization	Reference	Title	Status	Date	Abstract
ITU-T SG17 ISO/IEC JTC 1/SC 6	X.500 9594-1	The Directory: Overview of concepts, models and services	Rec IS	2005	Together with other Recommendations, has been produced to facilitate the interconnection of information processing systems to provide directory services. A set of such systems, together with the directory information that they hold, can be viewed as an integrated whole, called the Directory. The information held by the Directory, collectively known as the Directory Information Base (DIB), is typically used to facilitate communication between, with or about objects such as application entities, people, terminals and distribution lists. This Rec. introduces and models the concepts of the Directory and of the DIB and overviews the services and capabilities, which they provide.
ITU-T SG17 ISO/IEC JTC 1/SC 6	X.501 9594-2	The Directory: Models	Rec IS	2005	Provides a number of different models for the Directory as a framework for the other ITU-T Rec.s in the X.500 series. The models are the overall (functional) model, the administrative authority model, generic Directory Information models providing Directory User and Administrative User view on Directory information, generic Directory System Agent (DSA) and DSA information models and operational framework and a security model. This Rec. specifies the Directory use of its X.509 Public-key and attribute certificate frameworks.
ITU-T SG17 ISO/IEC JTC 1/SC 6	X.509 9594-8	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*)	Rec IS	2005	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.
ITU-T SG17 ISO/IEC JTC 1/SC 6	X.519 I9594-5	The Directory: Protocol specification	Rec IS	2005	Specifies procedures and application contexts to identify secure access during binding of Directory entities.

ITU-T SG16	H.350.2	Directory services architecture for H.235	Rec	2003	Describes an LDAP schema to represent H.235 elements. It is an auxiliary class related to H.350 and derives much of its functionality from that architecture. Implementers should review H.350 in detail before proceeding with this Rec. Its attributes include H.235 identity, password and certificate elements. These elements can be downloaded to an endpoint for automatic configuration or accessed by a gatekeeper for call signalling and authentication. The scope of this Rec. does not include normative methods for the use of the LDAP directory itself or the data it contains. The purpose of the schema is not to represent all possible data elements in the H.235 protocol, but rather to represent the minimal set required to accomplish the design goals enumerated in H.350.
ITU-T SG17	X.1122	Guideline for implementing secure mobile systems based on PKI	Rec	2004	This Rec. provides a guideline to construct secure mobile systems based on PKI technology.
IETF	2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	RFC	Jan 1999	This memo profiles the X.509 v3 certificate and X.509 v2 CRL for use in the Internet. An overview of the approach and model are provided as an introduction. The X.509 v3 certificate format is described in detail, with additional information regarding the format and semantics of Internet name forms (e.g., IP addresses). Standard certificate extensions are described and one new Internet-specific extension is defined. A required set of certificate extensions is specified. The X.509 v2 CRL format is described and a required extension set is defined as well. An algorithm for X.509 certificate path validation is described. Supplemental information is provided describing the format of public keys and digital signatures in X.509 certificates for common Internet public key encryption algorithms (i.e., RSA, DSA, and Diffie-Hellman). ASN.1 modules and examples are provided in the appendices.
IETF	2528	Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates	RFC	March 1999	The Key Exchange Algorithm (KEA) is a classified algorithm for exchanging keys. This specification profiles the format and semantics of fields in X.509 V3 certificates containing KEA keys. The specification addresses the subjectPublicKeyInfo field and the keyUsage extension.
IETF	2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	RFC	June 1999	This document specifies a protocol useful in determining the current status of a digital certificate without requiring CRLs. Additional mechanisms addressing PKIX operational requirements are specified in separate documents.
IETF	2585	Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP	RFC	May 1999	The protocol conventions described in this document satisfy some of the operational requirements of the Internet Public Key Infrastructure (PKI). This document specifies the conventions for using the File Transfer Protocol (FTP) and the Hypertext Transfer Protocol (HTTP) to obtain certificates and certificate revocation lists (CRLs) from PKI repositories.

IETF	2797	Certificate Management Messages over CMS	RFC	April 2000	This document defines a Certificate Management protocol using CMS (CMC). This protocol addresses two immediate needs within the Internet PKI community: 1. The need for an interface to public key certification products and services based on [CMS] and [PKCS10], and 2. The need in [SMIMEV3] for a certificate enrollment protocol for DSA-signed certificates with Diffie-Hellman public keys.
IETF	2797-bis-2	Certificate Management Messages over CMS	RFC		This document defines the base syntax for CMC, a Certificate Management protocol using CMS (Cryptographic Message Syntax). This protocol addresses two immediate needs within the Internet PKI community: 1. The need for an interface to public key certification products and services based on CMS and PKCS #10 (Public Key Crytpography Standard), and 2. The need in S/MIME (Secure MIME) for a certificate enrollment protocol for DSA-signed certificates with Diffie-Hellman public keys.
IETF	3029	Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols	RFC	Feb 2001	This document describes a general Data Validation and Certification Server (DVCS) and the protocols to be used when communicating with it. The Data Validation and Certification Server is a Trusted Third Party (TTP) that can be used as one component in building reliable non-repudiation services.
IETF	3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	RFC	August 2001	This document describes the format of a request sent to a Time Stamping Authority (TSA) and of the response that is returned. It also establishes several security-relevant requirements for TSA operation, with regards to processing requests to generate responses.
IETF	3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	RFC	April 2002	This document specifies algorithm identifiers and ASN.1 encoding formats for digital signatures and subject public keys used in the Internet X.509 Public Key Infrastructure (PKI). Digital signatures are used to sign certificates and certificate revocation list (CRLs). Certificates include the public key of the named subject.
IETF	3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	RFC	April 2002	This memo profiles the X.509 v3 certificate and X.509 v2 Certificate Revocation List (CRL) for use in the Internet. An overview of this approach and model are provided as an introduction. The X.509 v3 certificate format is described in detail, with additional information regarding the format and semantics of Internet name forms. Standard certificate extensions are described and two Internet-specific extensions are defined. A set of required certificate extensions is specified. The X.509 v2 CRL format is described in detail, and required extensions are defined. An algorithm for X.509 certification path validation is described. An ASN.1 module and examples are provided in the appendices.

IETF	3281	An Internet Attribute Certificate Profile for Authorization	RFC	April 2002	This specification defines a profile for the use of X.509 Attribute Certificates in Internet Protocols. Attribute certificates may be used in a wide range of applications and environments covering a broad spectrum of interoperability goals and a broader spectrum of operational and assurance requirements. The goal of this document is to establish a common baseline for generic applications requiring broad interoperability as well as limited special purpose requirements. The profile places emphasis on attribute certificate support for Internet electronic mail, IPSec, and WWW security applications.
IETF	3280bis	Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile	RFC	July 2005	This memo profiles the X.509 v3 certificate and X.509 v2 Certificate Revocation List (CRL) for use in the Internet. An overview of this approach and model are provided as an introduction. The X.509 v3 certificate format is described in detail, with additional information regarding the format and semantics of Internet name forms. Standard certificate extensions are described and two Internet-specific extensions are defined. A set of required certificate extensions is specified. The X.509 v2 CRL format is described in detail, and required extensions are defined. An algorithm for X.509 certification path validation is described. An ASN.1 module and examples are provided in the appendices.
IETF	3379	Delegated Path Validation and Delegated Path Discovery Protocol Requirements	RFC	Sept 2002	This document specifies the requirements for Delegated Path Validation (DPV) and Delegated Path Discovery (DPD) for Public Key Certificates. It also specifies the requirements for DPV and DPD policy management.
IETF	3447	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1	Info.	Feb. 2003	This memo represents a republication of PKCS #1 v2.1 from RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, and change control is retained within the PKCS process.
IETF	3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	RFC	Nov 2003	This document presents a framework to assist the writers of certificate policies or certification practice statements for participants within public key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a certificate policy or a certification practice statement.
IETF	3709	Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates	RFC	Feb 2004	This document specifies a certificate extension for including logotypes in public key certificates and attribute certificates.
IETF	3739	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile	RFC	March 2004	This document forms a certificate profile, based on RFC 3280, for identity certificates issued to natural persons. The profile defines specific conventions for certificates that are qualified within a defined legal framework, named Qualified Certificates. However, the profile does not define any legal requirements for such Qualified Certificates. The goal of this document is to define a certificate profile that supports the issuance of Qualified Certificates independent of local legal requirements. The profile is however not limited to Qualified Certificates and further profiling may facilitate specific local needs.

IETF	3766	Determining Strengths For Public Keys Used For Exchanging Symmetric Keys	BCP	April 2004	This document explains how to determine the length of an asymmetric key as a function of a symmetric key strength requirement. Some rules of thumb for estimating equivalent resistance to large-scale attacks on various algorithms are given. The document also addresses how changing the sizes of the underlying large integers (moduli, group sizes, exponents, and so on) changes the time to use the algorithms for key exchange.
IETF	3779	X.509 Extensions for IP Addresses and AS Identifiers	RFC	June 2004	This document defines two X.509 v3 certificate extensions. The first binds a list of IP address blocks, or prefixes, to the subject of a certificate. The second binds a list of autonomous system identifiers to the subject of a certificate. These extensions may be used to convey the authorization of the subject to use the IP addresses and autonomous system identifiers contained in the extensions.
IETF	3820	Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile	RFC	June 2004	This document forms a certificate profile for Proxy Certificates, based on X.509 Public Key Infrastructure (PKI) certificates as defined in RFC 3280, for use in the Internet. The term Proxy Certificate is used to describe a certificate that is derived from, and signed by, a normal X.509 Public Key End Entity Certificate or by another Proxy Certificate for the purpose of providing restricted proxying and delegation within a PKI based authentication system.
IETF	4043	Internet X.509 Public Key Infrastructure Permanent Identifier	RFC	May 2005	This document defines a new form of name, called permanent identifier, that may be included in the subjectAltName extension of a public key certificate issued to an entity. The permanent identifier is an optional feature that may be used by a CA to indicate that two or more certificates relate to the same entity, even if they contain different subject name (DNs) or different names in the subjectAltName extension, or if the name or the affiliation of that entity stored in the subject or another name form in the subjectAltName extension has changed.
IETF	4055	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	RFC	June 2005	This document supplements RFC 3279. It describes the conventions for using the RSA Probabilistic Signature Scheme (RSASSA-PSS) signature algorithm, the RSA Encryption Scheme - Optimal Asymmetric Encryption Padding (RSAES-OAEP) key transport algorithm and additional one-way hash functions with the Public-Key Cryptography Standards (PKCS) #1 version 1.5 signature algorithm in the Internet X.509 Public Key Infrastructure (PKI). Encoding formats, algorithm identifiers, and parameter formats are specified.
IETF	4059	Internet X.509 Public Key Infrastructure Warranty Certificate Extension	RFC	May 2005	This document describes a certificate extension to explicitly state the warranty offered by a Certificate Authority (CA) for the certificate containing the extension.
IETF	4158	Internet X.509 Public Key Infrastructure: Certification Path Building	RFC	Sept 2005	This document provides guidance and recommendations to developers building X.509 public-key certification paths within their applications. By following the guidance and recommendations defined in this document, an application developer is more likely to develop a robust X.509 certificate-enabled application that can build valid certification paths across a wide range of PKI environments.

IETF	4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)	RFC	Sept 2005	This document describes the Internet X.509 Public Key Infrastructure (PKI) Certificate Management Protocol (CMP). Protocol messages are defined for X.509v3 certificate creation and management. CMP provides on-line interactions between PKI components, including an exchange between a Certification Authority (CA) and a client system.
IETF	4211	Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)	RFC	Sept 2005	This document describes the Certificate Request Message Format (CRMF) syntax and semantics. This syntax is used to convey a request for a certificate to a Certification Authority (CA), possibly via a Registration Authority (RA), for the purposes of X.509 certificate production. The request will typically include a public key and the associated registration information. This document does not define a certificate request protocol.
IETF	4325	Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension	RFC	Dec 2005	This document updates RFC 3280 by defining the Authority Information Access Certificate Revocation List (CRL) extension.
IETF	4334	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)	RFC	Feb 2006	This document defines two Extensible Authentication Protocol (EAP)extended key usage values and a public key certificate extension to carry Wireless LAN (WLAN) System Service identifiers (SSIDs).
IETF	4386	Internet X.509 Public Key Infrastructure Repository Locator Service	RFC	Feb 2006	This document defines a Public Key Infrastructure (PKI) repository locator service.
IETF	4387	Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP	RFC	Feb 2006	The protocol conventions described in this document satisfy some of the operational requirements of the Internet Public Key Infrastructure (PKI).
IETF	4476	Attribute Certificate (AC) Policies Extension	RFC	May 2006	This document describes one certificate extension that explicitly states the Attribute Certificate Policies (ACPs) that apply to a given Attribute Certificate (AC). The goal of this document is to allow relying parties to perform an additional test when validating an AC, i.e., to assess whether a given AC carrying some attributes can be accepted on the basis of references to one or more specific ACPs.
IETF	4491	Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 PKI Certificate and CRL Profile	RFC	May 2006	This document supplements RFC 3279. It describes encoding formats,identifiers, and parameter formats for the algorithms GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 for use in Internet X.509 Public Key Infrastructure (PKI).
IETF	4511	Lightweight Directory Access Protocol (LDAP): The Protocol	RFC	Jun 2006	This document describes the protocol elements, along with their semantics and encodings, of LDAP. LDAP provides access to distributed directory services that act in accordance with X.500 data and service models.

IETF	4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models	RFC	Jun 2006	This document describes the X.500 Directory Information Models, as used in LDAP.
IETF	4514	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names	RFC	Jun 2006	The X.500 Directory uses distinguished names (DNs) as primary keys to entries in the directory. This document defines the string representation used in LDAP to transfer distinguished names.
IETF	4515	Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters	RFC	Jun 2006	LDAP search filters are transmitted in the LDAP protocol using a binary representation that is appropriate for use on the network. This document defines a human-readable string representation of LDAP search filters that is appropriate for use in LDAP URLs (RFC 4516) and in other applications.
IETF	4516	Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator	RFC	Jun 2006	This document describes a format for an LDAP Uniform Resource Locator (URL).
IETF	4517	Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules	RFC	Jun 2006	This document defines a base set of syntaxes and matching rules for use in defining attributes for LDAP directories.
IETF	4518	Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation	RFC	Jun 2006	This document defines string preparation algorithms for character-based matching rules defined for use in LDAP.
IETF	4519	Lightweight Directory Access Protocol (LDAP): Schema for User Applications	RFC	Jun 2006	This document is an integral part of the LDAP technical specification. It provides a technical specification of attribute types and object classes intended for use by LDAP directory clients for many directory services, such as White Pages.
IETF	4520	Internet Assigned Numbers Authority (IANA) Considerations for LDAP	BCP	Jun 2006	This document provides procedures for registering extensible elements of the LDAP. The document also provides guidelines to the Internet Assigned Numbers Authority (IANA) describing conditions under which new values can be assigned.
IETF	4521	Considerations for LDAP Extensions	BCP	Jun 2006	LDAP is extensible. It provides mechanisms for adding new operations, extending existing operations, and expanding user and system schemas. This document discusses considerations for designers of LDAP extensions.
IETF	4523	LDAP Schema Definitions for X.509 Certificates	RFC	Jun 2006	This document describes schema for representing X.509 certificates, X.521 security information, and related elements in directories accessible using LDAP.
IETF	4556	Public Key Cryptography for Initial Authentication in Kerberos	RFC	Jun 2006	This document describes protocol extensions to the Kerberos protocol specification. These extensions provide a method for integrating public key cryptography into the initial authentication exchange, by using asymmetric-key signature and/or encryption algorithms in pre-authentication data fields.
IETF	4557	Online Certificate Status Protocol (OCSP) Support for Public Key Cryptography for Initial Authentication in Kerberos	RFC	Jun 2006	This document defines a mechanism to enable in-band transmission of Online Certificate Status Protocol (OCSP) responses in the Kerberos network authentication protocol.

Disaster Recovery

Organization	Reference	Title	Status	Date	Abstract
ISO/IEC JTC 1/SC 27	24762	Guidelines for information and communications technology disaster recovery services	WD	2005-11	This standard specifies the guidelines for the information & communication technology disaster recovery (ICT DR) services focusing on the desired disaster recovery (DR) facilities and services capability.

Next Generation Networks

Organization	Reference	Title	Status	Date	Abstract
ETSI	202 382	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles	ES		
ETSI	202 383	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets	ES		
ETSI	202 387	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables	EG		
ETSI	102 419	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security analysis of IPv6 application in telecommunications standards	TR		
ETSI	187 004	TISPAN NGN Security – Framework and Requirements - Release Independent [145] TR 187 002; TISPAN NGN Security -Threat and Risk Analysis – NGN Release 1	TS		
ETSI	187 003	TISPAN NGN Security - Security Architecture – NGN Release 1	TS		

ETSI	102 165-1	TISPAN 07 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protocol Framework Definition; Methods and Protocols for Security; Part 1 Threat Analysis	TS		
ETSI	102 165-2	TISPAN 07 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures	TS		

Security terminology and glossaries

Organization	Reference	Title	Status	Date	Abstract
ITU-T SG 17		Compendium of ITU-T approved security definitions extracted from ITU-T recommendations		2005	http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0001MSWE.doc
ISO/IEC JTC 1/SC 27	SD 6	Terminology - Standing Document			www.ni.din.de/sc27 Then go to Documents and select Standing Document 6 (SD6)
IETF		Internet Security Glossary			http://www.ietf.org/rfc/rfc2828.txt
ETSI	232	Glossary of security terminology	ETR		http://webapp.etsi.org/WorkProgram/Expert/QueryForm.asp Then chose “ETR” in the “Type” box and “232” in the “number” box.

Sector-specific security standards

Organization	Reference	Title	Status	Date	Abstract
Multimedia					
ITU-T SG 16	H.233	Confidentiality system for audiovisual services	Rec	2002	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.
ITU-T SG 16	H.234	Encryption key management and authentication system for audiovisual services	Rec	2002	A *privacy system* consists of two parts, the *confidentiality mechanism* or *encryption process* for the data, and a *key management* subsystem. This Rec. 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 Rec.

ITU-T SG 16	H.235.0	H.323 security framework: Security framework for H-series (H.323 and other H.245-based) multimedia systems	Rec	2005	Describes enhancements within the framework of the H.3xx-series Recommendations to incorporate security services such as *Authentication* and *Privacy* (data encryption). The proposed scheme is applicable to both simple point-to-point and multipoint conferences for any terminals which utilize ITU-T Rec. H.245 as a control protocol; further also to H.323 systems that use the H.225.0 RAS and/or Call Signalling Protocol. For example, H.323 systems operate over packet-based networks which do not provide a guaranteed quality of service. For the same technical reasons that the base network does not provide QOS, the network does not provide a secure service. Secure real-time communication over insecure networks generally involves two major areas of concern – *authentication* and *privacy*. Describes the security infrastructure and specific privacy techniques to be employed by the H.3xx-series of multimedia systems. This Recommendation will cover areas of concern for interactive conferencing. These areas include, but are not strictly limited to, authentication and privacy of all real-time media streams that are exchanged in the conference. This Recommendation provides the protocol and algorithms needed between the H.323 entities. Utilizes the general facilities supported in ITU-T Rec. H.245 and as such, any standard which operates in conjunction with this control protocol may use this security framework. It is expected that, wherever possible, other H-series terminals may interoperate and directly utilize the methods described in this Recommendation. This Recommendation will not initially provide for complete implementation in all areas, and will specifically highlight endpoint authentication and media privacy. Includes the ability to negotiate services and functionality in a generic manner, and to be selective concerning cryptographic techniques and capabilities utilized. The specific manner in which they are used relates to systems capabilities, application requirements and specific security policy constraints. This Recommendation supports varied cryptographic algorithms, with varied options appropriate for different purposes; e.g., key lengths. Certain cryptographic algorithms may be allocated to specific security services (e.g., one for fast media stream encryption and another for signalling encryption).
ITU-T SG 16	H.235.1	H.323 security framework: Baseline security profile	Rec	2005	Provides authentication and integrity protection, or authentication-only for H.225.0 RAS and call signalling, H.225.0, and tunnelled H.245 using password-based HMAC-SHA1-96 hash protection of H.225.0 RAS and Call Signaling messages by using secure password-based cryptographic techniques. The security profile is applicable to H.323 terminal- to-gatekeeper, gatekeeper-to-gatekeeper, H.323 gateway-to-gatekeeper and to other H.323 entities in administered environments with symmetric assigned keys/passwords.
ITU-T SG 16	H.235.2	H.323 security framework: Signature security profile	Rec	2005	Describes an optional security profile for deploying digital signatures to secure the H.225.0 signalling.
ITU-T SG 16	H.235.3	H.323 security framework: Hybrid security profile	Rec	2005	Describes an efficient and scalable, PKI-based hybrid security profile for version 2 or higher of ITU-T Rec. H.235. The hybrid security profile contained herein takes advantage of the security profiles in H.235.1 and H.235.2 by deploying digital signatures from H.235.2 and deploying the baseline security profile from H.235.1.

ITU-T SG 16	H.235.4	H.323 security framework: Direct and selective routed call security	Rec	2005	The purpose of H.235.4 is to provide recommendations of security procedures for using direct-routed call signalling in conjunction with H.235.1 and H.235.3 security profiles. This security profile is offered as an option and may complement the security profiles in H.235.1 and H.235.3. It also provides implementation details for the H.235.0 clause 8.4 using symmetric key management techniques. In earlier versions of the H.235 sub-series, this profile was contained in H.235 Annex I. Appendices IV, V, VI to H.235.0 contain a complete section, figure, and table mapping between H.235 versions 3 and 4.
ITU-T SG 16	H.235.5	H.323 security framework: Framework for secure authentication in RAS using weak shared secrets	Rec	2005	Provides the framework for mutual party authentication during H.225.0 RAS exchanges. The "proof-of-possession" methods described permit secure use of shared secrets such as passwords which, if used by themselves, would not provide sufficient security. Extensions to the framework to permit simultaneous negotiation of Transport Layer Security parameters for protection of a subsequent call signalling channel are also described.
ITU-T SG 16	H.235.6	H.323 security framework: Voice encryption profile with native H.235/H.245 key management	Rec	2005	Holds the security procedures for the voice encryption profile (formerly in H.235 Annex D) including the accompanying native H.235/H.245 key management.
ITU-T SG 16	H.235.7	H.323 security framework: Usage of the MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235	Rec	2005	Describes security procedures for H.323/H.235-based systems for using the MIKEY key management protocol in conjunction with the Secure Real Time Transport Protocol.
ITU-T SG 16	H.235.8	H.323 security framework: Key exchange for SRTP using secure signalling channels	Rec	2005	Describes security procedures for key exchange for SRTP using secure signalling channels over H.323/H.235 networks.
ITU-T SG 16	H.235.9	H.323 security framework: Security gateway support for H.323	Rec	2005	Defines a method for the discovery of Security Gateways in the signalling path between communicating H.323 entities, and for sharing of security information between a gatekeeper and the SGs in order to preserve signalling integrity and privacy.

ITU-T SG16	H.323	Packet-based multimedia communications system	Rec	2003	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. Annex J: Security for Simple endpoint types
ITU-T SG16	H.530	Security for H.510 in H.323 Multimedia Mobile Environments	Rec	2002	Provides security procedures in H.323 mobility environments such as under scope of H.510 that describes mobility for H.323 multimedia systems and services. This Rec. provides the details about the security procedures for H.510. So far, the signaling capabilities of H.235 in version 1 and 2 are designed to handle security in mostly static H.323 environments. Those environments and multimedia systems can achieve some limited mobility within gatekeeper zones; H.323 in general and H.235 specifically provide only very little support for secure roaming of mobile users and terminals across different domains with many involved entities in a mobility, distributed environment for example. The H.323 mobility scenarios depicted in H.510 regarding terminal mobility pose a new situation with their flexible and dynamic character also from a security point of view. Roaming H.323 users and mobile terminals have to be authenticated by a foreign, visited domain. Likewise, the mobile user would like to obtain evidence about the true identity of the visited domain. In addition to that, it may be also useful to obtain evidence about the identity of the terminals complementing user authentication. Thus, these requirements demand for mutual authentication of the user and the visited domain and optionally also of the identity of the terminal. Usually initially only the home domain knows the mobile user, where he or she is subscribed and assigned a password; the visited domain does not know the mobile user. As such, the visited domain does not share any established security relationship with the mobile user and the mobile terminal. In order let the visited domain achieve the authentication and authorization assurance for the mobile user and the mobile terminal, the visited domain would relay certain security tasks such as authorization checks or key-management to the home domain through intermediate network and service entities. This requires securing the communication and key management between the visited domain and the home domain too. While in principle, mobility H.323 environments are more open than closed H.323 networks; there is of course also need to secure the key management tasks appropriately. It is also true, that communication within and across the mobility domains deserves protection against malicious tampering.

ITU-T SG 4	M.3010	Principles for a telecommunications management network	Rec	2000	Defines concepts of Telecommunications Management Network (TMN) architectures (TMN functional architecture, TMN information architecture, and TMN physical architectures) and their fundamental elements and describes the relationship among the three architectures and provides a framework to derive the requirements for the specification of TMN physical architectures from the TMN functional and information architectures. A logical reference model for partitioning of management functionality, the Logical Layered Architecture (LLA), is provided. This Rec. also defines how to demonstrate TMN conformance and compliance for the purpose of achieving interoperability. The requirements of the TMN involve the ability to ensure secure access to management information by authorized management information users. TMN includes functional blocks for which security functionality is performed by security techniques to protect the TMN environment in order to assure the safety of the information exchanged over the interfaces and residing in the management application. Security principles and mechanisms are also related to the control of access rights of the TMN users to information associated with TMN applications.
ITU-T SG 4	M.3016.0	Security for the management plane: Overview	Rec	2005	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
ITU-T SG 4	M.3016.1	Security for the management plane: Security requirements	Rec	2005	Identifies the security requirements for the management plane in telecommunication management. It focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the telecommunication infrastructure.
ITU-T SG 4	M.3016.2	Security for the management plane: Security services	Rec	2005	Identifies the security services for the management plane in Telecommunication management. It focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the Telecommunication infrastructure.
ITU-T SG 4	M.3016.3	Security for the management plane: Security mechanism	Rec	2005	Identifies the security mechanisms for the management plane in the Telecommunications management network. This Recommendation focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the Telecommunication infrastructure.
ITU-T SG 4	M.3016.4	Security for the management plane: Profile proforma	Rec	2005	Defines the Conformance Profile proforma for organizations using ITU-T Recs M.3016.1-M.3016.3 for specifying the telecommunications management plane requirements. By completing the proforma in this Recommendation, different profiles are specified.

ITU-T SG 4	M.3210.1	TMN management services for IMT-2000 security management (M.IMTSEC)	Rec	2001	Is one of the series of TMN Management Service Rec.s that provide description of management services, goals and context for management aspects of IMT-2000 networks. This Rec. describes a subset of Security Management services to provide Requirements and Analysis of the Security management and a profile for *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. This Rec. 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.
ITU-T SG 4	M.3320	MANAGEMENT REQUIREMENTS FRAMEWORK FOR THE TMN X INTERFACE	Rec	1997	Is part of a series dealing with the transfer of information for the management of telecommunication networks and services , and only some parts address security aspects. The purpose of this Rec. is to define a requirements framework for all functional, service and network-level requirements for the TMN exchange of information between Administrations.. This Rec. 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.This Rec. includes specifications of the security requirements of the TMN X interface.
ITU-T SG4	M.3400	TMN management functions	Rec	2000	Is one of a series of Rec.s 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 Rec. This Rec. includes descriptions of the security management function supported by the TMN.
ITU-T SG 4	Q.293	Intervals at which security measures are to be invoked	Rec	1988	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
ITU-T SG 4	Q.813	Security transformations application service element for remote operations service element (STASE-ROSE)	Rec	1998	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 Rec. describes an approach to the provisioning of security transformations that is implemented in the application layer and requires no security-specific functionality in any of the underlying OSI stack layers. This Rec. enhances TMN security by supporting security transformations for ROSE PDUs and exchange of related security information.
ITU-T SG 4	Q.815	Specification of a security module for whole message protection	Rec	2000	Specifies an optional security module to be used with Rec. Q.814, Specification of an Electronic Data Interchange Interactive Agent that provides security services for whole Protocol Data Units (PDUs). In particular, the security module supports *non-repudiation of origin and of receipt*, as well as whole *message integrity.*

ITU-T SG 4	Q.817	TMN PKI ~ Digital certificates and certificate revocation lists profiles	Rec	2001	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 Rec. is intended to promote interoperability among TMN elements that use Public Key Infrastructure (PKI) to support security-related functions. The purpose of this Rec. 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 Rec. does not specify how such functions should be implemented, with or without PKI.
ITU-T SG 15	G.808.1	Generic protection switching – Linear trail and subnetwork protection	Rec	2003	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 Rec.s.
ITU-T SG 15	G.841	Types and characteristics of SDH network protection architectures	Rec	1998	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).
ITU-T SG 15	G.842	Interworking of SDH network protection architectures	Rec	1997	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.
Security of television signals and services					
ITU-T SG 9	J.93	Requirements for conditional access in the secondary delivery of digital television or cable television systems	Rec	1998	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.
ITU-T SG 9	J.96 Amd 1	Technical Method for Ensuring Privacy in Long-Distance International MPEG-2 Television Transmission Conforming to Rec. J.89	Rec	2002	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.

ITU-T SG 9	J.112	Transmission systems for interactive cable television services	Rec	1998	This Rec. complements and extends the scope of J.83 "Digital multi-programme systems for television, sound and data services for cable distribution" to make provision for bidirectional data over coaxial and hybrid fibre-coax cables for interactive services. It also contains several annexes in recognition of different existing media environments.. Security requirements are established, the use of SP-DOCSS Data Over Cable Security System (DOCSS) Specification; SP-RSM Removable Security Module Specification and SP-BDS Baseline Data-Over-Cable Security Specification is recommended.
ITU-T SG 9	J.191	IP feature package to enhance cable modems	Rec	2004	Provides a set of IP-based features that may be added to a cable modem that will enable cable operators to provide an additional set of enhanced services to their customers including support for IPCablecom Quality of Service (QoS), enhanced security, additional management and provisioning features, and improved addressing and packet handling. These IP-based features reside in the logical element Portal Service (PS or just Portal). A Cable Modem that contains these enhanced features is an IP-enhanced Cable Modem (IPCM), and is an implementation of a J.190 HA device class. As described in Rec. J.190, the HA device class includes both Cable Modem functionality as well as Portal Services functionality. Chapter 11 security: defines the security interfaces, protocols and functional requirements needed to reliably deliver cable-based IP services in a secure environment to the PS. The purpose of any security technology is to protect value, whether a revenue stream, or a purchasable information asset of some type. Threats to this revenue stream exist when a user of the network perceives the value, expends effort and money, and invents a technique to get around making the necessary payments. Annex C: Security threats and preventative measures.
ITU-T- SG9	J.160	Architectural framework for the delivery of time-critical services over cable television networks using cable modems	Rec	2002	Provides the architectural framework that will enable cable television operators to provide time-critical services over their networks that have been enhanced to support cable modems. The security services available through 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).

ITU-T- SG9	J.170 (Rev)	IPCablecom security specification	Rec	2005	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.
ITU-T- SG9	J.191	IP feature to enhance cable modems	Rec	2004	Chapter 11 defines security interfaces, protocols and functional requirements to deliver cable-based IP services in a secure environment.
Facsimile					
ITU-T- SG 16	T.30	Procedures for document facsimile transmission in the GSTN	Rec	2005	Annex G provides procedures for secure G3 document facsimile transmission usig the HKM and HFX system, Annex H provides for security in facsimile G3 based on the *RSA algorithm*.
ITU-T- SG 16	T.36	Security capabilities for use with Group 3 facsimile terminals	Rec	1997	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*.
ITU-T- SG 16	T.503	A document application profile for the interchange of Group 4 facsimile documents	Rec	2000	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.
ITU-T- SG 16	T.563	Terminal Characteristics for Group 4 facsimile apparatus	Rec	1996	Defines the general aspects of Group 4 facsimile apparatus and the interface to the physical network.
ITU-T- 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	Rec	1994	Defines a Programming Communication Interface called “APPLI/COM”, which provides unified access to different communications services, such as telefax group 3 or other telematic services. This Rec. describes the structure and contents of messages and the way to exchange them between a Local Application (LA) and a Communication Application (CA). Any communication is preceded by a login process and terminated by a logout process, where both the processes facilitate the implementation of security schemes especially important on multi-user systems, and provide means to implement security mechanisms between the LA and the CA. This Rec. forms a high level API (Application Programming Interface), which gives powerful control and monitoring on the telecommunication activity to the application designers.
Mobile					
ITU-T SG 19	Q.1741.1	IMT-2000 references to release 1999 of GSM evolved UMTS core network with UTRAN access network	Rec	2002	Includes references to the 3GPP security specifications i.e. to *TS 21.133: Security Threats and Requirements, TS 33.102: Security Architecture, TS 33.103: Security Integration Guidelines, TS 33.105: Cryptographic Algorithm requirements, TS 33.106: Lawful interception requirements, TS 33.107: Lawful interception Architecture and Functions, TS 33.120: Security Objectives and Principles*

ITU-T SG 19	Q.1741.2	IMT-2000 references to release 4 of GSM evolved UMTS core network with UTRAN access network	Rec	2002	Includes references to the 3GPP security specifications as *TS 21.133: Security Threats and Requirements, TS 22.048: Security Mechanisms for the (U) SIM application toolkit, TS 22.101: Service aspects; Service principles, TS 33.102: Security Architecture, TS 33.103: Security Integration Guidelines, TS 33.105: Cryptographic Algorithm requirements, TS 33.106: Lawful interception requirements, TS 33.107: Lawful interception Architecture and Functions, TS 33.120: Security Objectives and Principles, TS 33.200: Network Domain Security – MAP, TS 35.205, .206, .207, and .208: Specification of the MILENAGE Algorithm Set*
ITU-T SG 19	Q.1741.3	IMT-2000 references to release 5 of GSM evolved UMTS core network with UTRAN access network	Rec	2003	Includes references to the 3GPP security specifications as *TS 22.101: Service aspects; Service principles, TS 33.102: Security Architecture, TS 33.106: Lawful interception requirements, TS 33.107: Lawful interception Architecture and Functions, TS 33.108: Handover interface for Lawful Interception (LI), TS 33.200: Network Domain Security – MAP, TS 33.203: Access security for IP-based services, TS 33.210: Security; Network Domain Security (NDS); IP network layer security, TS 35.205, .206, .207, .208 and .909: Specification of the MILENAGE Algorithm Set*
ITU-T SG 17	X.1121	Framework of secure technologies for mobile end-to-end data communication	Rec	2004	This Rec. shows where the security technologies realizing certain security function appear in the mobile end-to-end data communication model and provides a framework of security technologies for mobile end-to-end data communication.
ETSI	102 203	Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements	TR		
ETSI	102 204	Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface Specification	TS		
ETSI	102 206	Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework	TR		
ETSI	102 207	Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature	TS		
ETSI	102 071	Mobile Commerce (M-COMM); Requirements for Payment Methods for Mobile Commerce	TR		

ETSI	100 920 SMG 01	Digital cellular telecommunications system (Phase 2+); Security aspects	TS		
ETSI	100 929 SMG 03	Global System for Mobile communication (GSM) (Phase 2+); Security related network functions	TS		
ETSI	121 133 3GPP SA 3 (3GPP TS 21.133)	Universal Mobile Telecommunications System (UMTS); 3G security; Security threats and requirements	TS		
ETSI	133 102 3GPP SA 3 (3GPP TS 33.102)	Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture	TS		
ETSI	133 103 3GPP SA 3 (3GPP TS 33.103)	Universal Mobile Telecommunications System (UMTS); 3G Security; Integration Guidelines	TS		
ETSI	133 105 3GPP SA 3 (3GPP TS 33.105)	Universal Mobile Telecommunications System (UMTS); Cryptographic algorithm requirements	TS		
ETSI	133 120 3GPP SA 3 (3GPP TS33.120)	Universal Mobile Telecommunications System (UMTS); 3G Security; Security Principles and Objectives	TS		
ETSI	133 141 3GPP SA 3 (3GPP TS 33.141)	Universal Mobile Telecommunications System (UMTS); Presence service; Security	TS		

ETSI	133 200 3GPP SA 3 (3GPP TS 33.200)	Universal Mobile Telecommunications System (UMTS); 3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security	TS		
ETSI	133 203 3GPP SA 3 (3GPP TS 33.203)	Details and Download Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services	TS		
ETSI	133 210 3GPP SA 3 (3GPP TS 33.210)	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security	TS		
ETSI	133 220 3GPP SA 3 (3GPP TS 33.220)	Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture	TS		
ETSI	133 221 3GPP SA 3 (3GPP TS 33.221)	Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Support for subscriber certificates	TS		
ETSI	133 222 3GPP SA 3 (3GPP TS 33.222)	Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)	TS		

ETSI	133 234 3GPP SA 3 (3GPP TS 33.234)	Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security	TS		
ETSI	133 246 3GPP SA 3 (3GPP TS 33.246)	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)	TS		
ETSI	133 310 3GPP SA 3 (3GPP TS 33.310)	Universal Mobile Telecommunications System (UMTS); Network domain security; Authentication framework (NDS/AF)	TS		
ETSI	135 201 3GPP SA 3 (3GPP TS 35.201 version 6.0.0 Release 6)	Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	TS		
ETSI	135 202 3GPP SA 3 (3GPP TS 35.202)	Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	TS		
ETSI	135 203 3GPP SA 3 (3GPP TS 35.203)	Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	TS		

ETSI	135 204 3GPP SA 3 (3GPP TS 35.204)	Universal Mobile Telecommunications System 30 (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	TS		
ETSI	135 205 3GPP SA 3 (3GPP TS 35.205)	Universal Mobile Telecommunications System (UMTS); 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*; Document 1: General	TS		
ETSI	135 206 3GPP SA 3 (3GPP TS 35.206)	Universal Mobile Telecommunications System (UMTS); 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*; Document 2: Algorithm specification	TS		
ETSI	135 207 3GPP SA 3 (3GPP TS 35.207)	Universal Mobile Telecommunications System (UMTS); 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*; Document 3: Implementors' test data	TS		

ETSI	135 208 3GPP SA 3 (3GPP TS 35.208)	Universal Mobile Telecommunications System (UMTS); 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*; Document 4: Design conformance test data	TS		
ETSI	135 909 3GPP SA 3 (3GPP TR 35.909)	Universal Mobile Telecommunications System (UMTS); 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*; Document 5: Summary and results of design and evaluation	TR		
ETSI	141 033 3GPP SA 3 (3GPP TR 41.033)	Digital cellular telecommunications system (Phase 2+); Lawful Interception requirements for GSM	TR		
ETSI	142 033 3GPP SA 3 (3GPP TS 42.033)	Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 1	TS		
ETSI	143 020 3GPP SA 3 (3GPP TS 43.020)	Digital cellular telecommunications system (Phase 2+); Security-related network functions	TS		
ETSI	155 205 3GPP SA 3 (3GPP TS 55.205)	Digital cellular telecommunications system (Phase 2+); Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8	TS		

ETSI	3GPP TS 55.216	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 1: A5/3 and GEA3 specification	TS		
ETSI	3GPP TS 55.217	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 2: Implementors' test data	TS		
ETSI	3GPP TS 55.218	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 3: Design and conformance test data	TS		
ETSI	3GPP TR 55.919	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report	TR		
ETSI	122 016 (3GPP TS 22.016)	Technical Specification Group Services and System Aspects; International Mobile station Equipment Identities (IMEI)	TS		
ETSI	123 003	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Numbering, Addressing and Identification	TS		
ETSI	122 242 (3GPP TS 22.242)	Universal Mobile Telecommunications System (UMTS); Digital Rights Management (DRM); Stage 1	TS		
ETSI	100 929 (GSM 03.20)	Global System for Mobile communication (GSM) (Phase 2+); Security related network functions	TS		

ETSI	100 614	Digital cellular telecommunications system (Phase 2+)(GSM); Security management	TS		
Satellite security					
ETSI	102 287	Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); IP Interworking over satellite; Security aspects	TR		
ETSI	102 465	SES BSM; Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); General Security Architecture	TS		
ETSI	102 466	SES BSM; Details and Download Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Multicast Security Architecture	TS		
ETSI	101 376-3-9	GEO-Mobile Radio Interface Specifications; Part 3: Network specifications; Sub-part 9: Security related Network Functions; GMR-1 03.020	TS		
ETSI	101 377-2-3	SES GMR GEO-Mobile Radio Interface Specifications; Part 2: Service specifications; Sub-part 3: Security Aspects; GMR-2 02.009	TS		
ETSI	101 377-3-10	SES GMR GEO-Mobile Radio Interface Specifications; Part 3: Network specifications; Sub-part 10: Securityrelated Network Functions; GMR-2 03.020	TS		

ETSI	101 442-6	Satellite Earth Stations and Systems (SES); Satellite Component of UMTS/IMT-2000; Multimedia Broadcast/Multicast Services part 6: Security	TS		
Miscelaneous					
ITU-T SG15	Q.1531	UPT security requirements for service Set 1	Rec	2000	Specifies UPT security requirements for both user-to-network and internetwork communication applicable to UPT Service Set 1 as defined within Rec. F.851. This Rec. covers all aspects of security for UPT using DTMF accesses and out-band DSS 1 based user accesses.
ITU-T SG17	X.1141	Security Assertion Markup Language (SAML 2.0)	Rec	2005	SAML is an XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain. This Recommendation defines a protocol by which clients can request assertions from SAML authorities and get a response from them. In creating their responses, SAML authorities can use various sources of information, such as external policy stores and assertions that were received as input in requests. The Recommendation provides a comprehensive list of SAML profiles such Web Browser SSO profile and Single Logout Profiles to enable the wide adoption of SAML in the industry. Guidelines for authentication context and conformance are also provided. This Recommendation is technically equivalent and compatible with the OASIS SAML 2.0 standard.