APEC-TEL

INFORMATION SYSTEMS SECURITY

STANDARDS

HANDBOOK

FINAL DRAFT

Committee Representation

Natsira Amal	Universitas Indonesia, Indonesia
Mark Baddeley	Ministry of Defence,New Zealand
Jeimy Cano	Los Andes University, Colombia
Keen Chan	Infocomm Development Authority of Singapore, Singapore
Ted Fecteau	Ministry of Education, New Zealand
Jay Garden	Government Communications Security Bureau, New Zealand
Francis Goh	Infocomm Development Authority of Singapore, Singapore
Lech Janczewski	University of Auckland, New Zealand
Somnuk Keretho	National Electronics and Computer Technology Unit, Thailand
Frank March	Ministry of Economic Development, New Zealand
Andrew Mason	BSA Consulting Group, New Zealand
Colin Oliver	DCITA, Australia
Steve Orlowski	Chair of e-Security Task Group
Mike Pearson	State Services Commission, New Zealand
Nelson Procter	Standards New Zealand (ex Officio)
Joe Richardson	Department of State, USA
Malcolm Shore	CES Communications Ltd New Zealand
John Snare	Adacel Technologies Ltd., Australia
Kume Takashi	IT Security Policy Office, Japan
Miles Trent	Trent Consulting Ltd. New Zealand
Mas Wigranturo	State Ministry for Communication and Information, Indonesia
Richard Wilsher	the Zygma partnership, Great Britain
Jeni Wolfe-Wilson	Health Sector Payments and Administration, New Zealand

COPYRIGHT NOTICE

CONTENTS **PAGE**

FOREWORD

This publication has been prepared for APEC-Telecommunications and Information Working Group (APEC-TEL) by Standards New Zealand. It is based on the Standards New Zealand Miscellaneous Publication NZMP 6653:2000 Information Systems Security Standards Handbook

This publication is designed to provide IT and security professionals with an understanding of the major national and international standards relating to information systems security. It contains references to a wide range of IT security standards from all the major IT security standards arenas, with cross-references between standards where relevant.

The development of international standards is an ongoing process, and new security standards will continue to emerge. The content of this publication will be subject to regular review to ensure that all relevant standards are included.

The inclusion of any particular standard does not in any way reflect support for the standard, nor does omission represent any criticism of the standard.

APEC HANDBOOK

INFORMATION SYSTEMS
SECURITY STANDARDS HANDBOOK

1 SCOPE

1.1
This Handbook provides a single source reference document for information security industry users who wish to ascertain the appropriate Standard(s) or other documents available and applicable to their specific interest area.

2 INTRODUCTION TO SECURITY STANDARDS

2.1 The Standards

2.1.1
There are many sources of security standards and guidelines. In this publication, we have selected the main sources of such standards relating to the most common environments in which security is of significance. The established security standards from these sources have been grouped, where appropriate, to focus on specific areas of application.

2.1.2
The sources selected for this publication are:

(a) **ISO/IEC**. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) produce a wide range of IT standards and guidelines through their joint agency Joint Technical Committee No 1 (JTC1). JTC1 Sub-Committee 27 is responsible for the production of information security standards. Other Sub-Committees such as SC6 and SC21 also produce standards relevant to security. Output of JTC1 is indicated by the prefix “ISO/IEC” in this document.

(b) **CCITT**. The International Telegraph and Telephone Consultative Committee (CCITT) originated the X-series of standards, which make up a significant portion of the Open Systems Interconnect set of standards. These are also sometimes referred to by their parent body name, the International Telecommunications Union (ITU) of the United Nations

(c) **IETF**. The Internet Engineering Task Force produces standards necessary to ensure the inter-operability of components of the Internet. These standards are definitive within the Internet community, but are also in many cases used outside the Internet.

(d) **ANSI** The American National Standards Institute includes in its products a number of Standards covering a broad spectrum of security issues.

(e) **NIST**. The National Institute of Standards and Technology produce a wide range of guidelines on information technology for the US Government. A number of their publications have received widespread acceptance as standards for general use.

(f) **EESSI.** The European Electronic Signature Standardisation Initiative (EESSI). The European ICT Standards Board, with a mandate from the European Commission, launched an industry initiative bringing together industry and public authorities, experts and other market-players, in support of the European Directive on electronic signatures: the European Electronic Signature Standardization Initiative (EESSI). The initiative is open to all who wish to participate.

(g) **Other**. There are a number of standards included in this publication which come from other

sources but which have achieved significant recognition nationally and/or internationally. Included in this category, in particular, are documents published by standards bodies in individual countries, as well as by a number of vendor consortia and industry/business sector groupings

2.1.3
Standards are dynamic, and continue to evolve and be superseded. This publication will undergo regular review to ensure that new standards, once established, are included.

3 STRATEGIC STANDARDS

3.1 Philosophy

3.1.1 OECD Guidelines for the Security of Information Systems

The 24 member nations of the organization for Economic Cooperation and Development (OECD), on 26 November 1992 adopted the OECD Guidelines for the Security of Information. This publication details the nine principles to be adhered to in the deployment of information systems, and five strategies by which the principles may be applied.

3.1.2 OECD Guidelines for Cryptography Policy

The OECD Guidelines on Cryptography Policy provides a set of principles to be adhered to in the development of national policy on cryptography. The principles cover private use of cryptography, support for cryptographic research, and lawful access.

3.2 Management Frameworks

3.2.1 ISO/IEC 15408 *Common Criteria for Information Technology Security Evaluation*
This multi-part standard, the Common Criteria (CC) is provided for use as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience. The CC permit comparability between the results of independent IT security evaluations by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation.

3.2.1.1 ISO/IEC 15408-1: *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*
Part 1 is the introduction to the Common Criteria . It defines general concepts and principles of IT security evaluation and presents a general model of evaluation. Part 1 also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. In addition, the usefulness of each part of the CC is described in terms of each of the target audiences.

3.2.1.2 ISO/IEC 15408-2: *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements*
Part 2 establishes a set of security functional components as a standard way of expressing the security functional requirements for Targets of Evaluation (TOEs). Part 2 catalogues the set of functional components, families, and classes.

3.2.1.3 ISO/IEC 15408-3: *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements*

Part 3 establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs. Part 3 catalogues the set of assurance components, families, and classes. Part 3 also defines evaluation criteria for Protection Profiles (PPs) and Security Targets (STs) and presents evaluation assurance levels that define the predefined CC scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs).

3.2.1.4 ISO/IEC TR 13335: *Information technology – Guidelines for the management of IT security (GMITS)*

Government and commercial organizations rely heavily on the use of information to conduct their business activities. Loss of confidentiality, integrity, availability and also accountability, authenticity and reliability, of information and services, can have an adverse impact on organizations. Consequently, there is a critical need to protect information and to manage the security of information technology (IT) systems within an organization. This requirement to protect information is particularly environment because many organizations are internally and externally connected by networks of IT systems. IT Security management is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, and also accountability, authenticity and reliability, for information and services. The purpose of this TR is to provide guidance, not solutions, to specific security problems. The document is in 5 parts:

Part 1: Concepts and models for IT security
Part 2: Managing and planning IT security
Part 3: Techniques for the management of IT security
Part 4: Selection of safeguards
Part 5: Management guidance on network security

3.2.2 ISO/IEC 15292: *Information Technology -- Security Techniques - Protection profile registration procedures*

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. A package is defined as a reusable set of either functional or assurance components combined together to satisfy a set of identified security objectives. This document 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.

3.2.3 ISO/IEC 17799: *Information Security Management*

This document is a code of practice which sets out a series of controls for the security of information systems. The controls are grouped into ten sections: Security Policy, Security Organization, Asset Classification and Control, Personnel Security, Physical and Environmental Security, Computer and Network management, System Access Control, Systems Development and Maintenance, Business Continuity Planning, and Compliance.

> NOTE - This document is based on the BSI document 7799, which is presented in two parts. Not yet developed as an ISO/IEC Standard, Part 2, *Specification for information security management* is a customisable specification for information security management systems and can be used as the basis for a certification checklist.

3.2.4 IT Security Evaluation Criteria (ITSEC)

This publication of the European Commission describes a set of Harmonised Information Technology (IT) Security Evaluation Criteria, a common criteria formed through the harmonisation of the national security evaluation criteria of the Netherlands, the United Kingdom, Germany, and

France. The criteria provide an independent means of specifying, evaluating against, and comparing security in systems and products.

NOTE – The IT Security Evaluation Criteria (ITSEC) is listed, but has been largely overtaken by the ISO /IEC 15408 set, the Common Criteria for evaluation of security in IT systems. As the Common Criteria become accepted and matures through the ISO standards development process, it is envisaged that the ITSEC will be replaced by the Common Criteria standard.

3.3 Certification and Accreditation

An acknowledged international standard addressing this area has not yet been identified.

3.4 Risk Management and Assessment

3.4.1 AS/NZS 4360: *Risk Management*

This standard provides a generic guide for establishing and implementing the risk management process, which involves establishing context, identification, analysis, evaluation, treatment, monitoring and review and consultation and communication. It may be applied at every stage in the life of an activity, function, project or asset generated by any public, private or community enterprise or group.

3.4.2 SAA/SNZ HB 231: *Information Security Risk Management Guidelines*

This guide provides guidance for the establishment and implementation of a risk management process for information security risks. This guide is not intended to be a comprehensive schedule of information security threats and vulnerabilities. It is intended to serve as a single reference point describing an information security risk management process suitable for most situations encountered in industry and commerce and therefore can be applied by a wide range of organisations.

3.4.3 SAA/SNZ HB 240: *Guidelines for managing risk in outsourcing utilizing the AS/NZS 4360 process*

This guides provides guidance for managing risks, which arise when organisations outsource elements of their business. The Handbook uses the risk management model in AS/NZS 4360, and includes case studies and a checklist of important issues to address when outsourcing.

3.4.4 GAO/AIMD-00-33: *Information Security Risk Assessment – Practices of Leading Organisation*

This guide is intended to help federal managers implement an ongoing information security risk assessment process by providing examples, or case studies, of practical risk assessment procedures that have been successfully adopted by four organizations known for their efforts to implement good risk assessment practices. More importantly, it identifies, based on the case studies, factors that are important to the success of any assessment program, regardless of the specific methodology employed.

3.4.5 IT System Security Assessment:

A guide produced by the UK Department of Trade and Industry (DTI), which describes the parameters that need to be considered in order to understand the risk to an organization's information assets handled by its IT systems. Risk combines a number of elements including:

(a) the likelihood of an asset being subject to a security threat;
(b) the vulnerabilities of an IT system (or an organisation) which may be exploited by a threat;
(c) the impact on the business if a particular threat occurs.

There are many recognised techniques, of varying complexity, for performing risk analysis within an organisation, which are beyond the scope of these guidelines. The approach used by this

guidance is to encourage readers to consider a series of issues about the usage and environment of IT systems or subsystems using tables designed for this purpose. The reader is then directed to select 'values', from sets of tables, that most closely describe their IT environment. These values are then used to identify:

(a) the vulnerability of information assets;
(b) the trust that can be placed in the users of the IT systems;
(c) the impact of a breach of security relating to these assets.

3.4.6 MG-2: *A Guide to Security Risk Management for Information Technology System*
This guide produced by the Government of Canada, Communications Security Establishment (CSE,) provides guidance for security risk management for information technology (IT) systems, throughout the life cycle of IT systems. It is intended for use by a wide range of personnel, including managers of programs, systems, and projects; security officials; planners; and engineers. It is structured into two main parts: the first describes a general framework for security risk management and the second provides detailed guidance for implementation of the framework

3.4.7 MG-3: *A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems*
This guide produced by Government of Canada, Communications Security Establishment (CSE), provides additional guidance for system designers on the technical factors associated with performing risk assessments and selecting appropriate safeguards. It applies to both proposed and existing systems. The document is primarily intended for use by risk analysts and security engineers in the performance of risk assessments and safeguard selections. It may also be of value to system and project managers as a means of understanding these two processes.

3.4.8 NIST Spec Pub 800-30: *Risk Management Guide for Information Technology Systems*
This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organizations to better manage IT-related mission risks.

In addition, this guide provides information on the selection of cost-effective security controls. These controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store and carry this information.

3.4.9 OCTAVE (sm) Method:
Produced by the US Software Engineering Institute Carnegie Mellon University, the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) method defines the essential components of a systematic and context-driven information security risk evaluation. This is a self-directed approach that enables personnel involved in the risk assessment the context to understand the risks and to make informed decisions and tradeoffs when developing a protection strategy. OCTAVE uses a three-phase method and examines the organizational and technology issues to assemble a comprehensive picture of the information security needs of an enterprise. By adopting this approach, organizations can understand their current security posture and use it as a benchmark for improvement.

3.4.10 BSI PD3002: *Guide to BS7799 Risk Assessment and Risk Management*
This guide addresses the topic of risk assessment and risk management in the context of BS7799 ‘Code of Practice for Information Security Management,’ and in particular the development and certification of BS 7799 Information Management Systems (ISMSs). It aims at providing a common basis and understanding of the underlying concepts behind risk assessment and risk management, the terminology used, and the overall process of, and options for, assessing risks

and for managing the risks. This document should be useful to both those that are doing certification of ISMS, and those organizations whose ISMS is being certified, in providing a 'common language'.

3.4.11 Security Risk Management Guide:
Produced by the USA Federal Aviation Administration, this guide provides a logical process to assess and quantify risk, and provides management with cost-effective solutions to security risk reduction using available resources. This guide starts at program inception and is applied throughout the life cycle. It is designed to:

(a) Identify and quantify assets to be safeguarded;
(b) Measure the criticality of each asset by determining the impact of loss of each asset;
(c) Address the threat taxonomy that applies;
(d) Identify and quantify the vulnerabilities associated with each asset when matched with each identified threat, and
(e) Analyze the costs and benefits associated with risk mitigation

3.5 Control Objectives for Information and Related Technology (COBIT)

The Control Objectives for Information and Related Technology (COBIT) is a publication of the Information Systems Audit and Control Association which sets out the control objectives which the relevant management units should be imposing on each of several areas, including those related to security.

3.6 Business Continuity Planning

An acknowledged standard addressing this area has not yet been identified.

3.7 ISSA Guidelines for Information Valuation

3.7.1
These guidelines produced by the Information Systems Security Association present a method of establishing defensible values for targeted bodies of information. Once information value has been established, an information security program can be realistically evaluated to ensure it is commensurate with the value of the information being secured.

3.7.2
Information is assumed to have a value that is measurable in a practical sense. When it is not practical or necessary to value the information quantitatively in monetary terms, a qualitative technique may be employed. Typically, the development or replacement costs for a body of information may be assumed to reflect the minimum value of the information while the real value may be much greater. In this guideline, security practitioners are provided with concepts and rationale, and are guided through a series of steps that will allow them to select, from among several valuation techniques, the one best suited to their situation.

3.8 Incident reporting

While an acknowledged standard addressing this area has not yet been identified, WD 18044 described in 4.5.10, is expected to fulfill this function

3.9 Terminology

3.9.1 ISO/IEC 2382-8: *Information technology -Vocabulary Part 8: Security*
The purpose of this document is to provide definitions that are rigorous, uncomplicated and which can be understood by all concerned. The scope of each concept defined has been chosen to provide a definition that is suitable for general application. In those circumstances where a

restricted application is concerned, the definition may need to be more specific.

3.9.2 RFC 2828: *Internet Security Glossary*
This glossary provides a very comprehensive set of abbreviations, explanations and recommendations for use in information security technology. It is particularly oriented to Internet-based systems. (Refer to section 6).

4 INTERNATIONAL STANDARDS

International Standards for information security are developed by Joint Technical Committee No 1, (JTC1), a committee created jointly by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). Specifically it is Sub-committee No 27 within JTC1 which has the responsibility, though other sub-committees have also produced documents of relevance to this publication.

4.1 ISO/IEC Frameworks

4.1.1 ISO/IEC 7498-2: *Open Systems Interconnect (OSI) Security Model*

4.1.1.1
This part of ISO/IEC 7498 defines the general security related architectural elements which can be applied in an appropriate way when the security of communications is required. It establishes, within the framework of the Open Systems Interconnect (OSI) reference model, guidelines and constraints to improve the existing standards or develop new standards.

4.1.1.2
The standard defines the five security services of access control, authentication, data integrity, data confidentiality, and non-repudiation. It also identifies the eight security mechanisms of encipherment, digital signature, access control, data integrity, authentication exchange, traffic padding, routing control, and notarisation.

4.1.2 ISO/IEC 9160: *Physical Layer Interoperability Requirements*
This document is one of three standards making up the Lower Layers Security model (LLS) - see also ISO/IEC 10736 and ISO/IEC 11577. In addition, IEEE 802.10 is sometimes cited as a fourth LLS standard. ISO/IEC 9160 specifies interoperability and security related requirements for using encipherment at the physical layer of the Open Systems Interconnect reference model. It is intended to facilitate the interoperation of data encipherment equipment and protect against all forms of passive attack including traffic analysis.

4.1.3 ISO/IEC 9594-8: *Directory Authentication*
This is the ISO/IEC version of the CCITT X.509 standard. It covers a range of directory authentication functions, including in particular the specification of the security certificate and certificate extensions.

4.1.4 ISO/IEC 9797: *Message Authentication Codes (MACs)*
This international standard specifies a method of using a key and an n-bit block cipher algorithm to calculate an m-bit cryptographic check value. This method can be used as a data integrity mechanism to detect that data has not been altered in an unauthorized manner. The strength of the data integrity mechanism is dependent upon the key length and its secrecy, on the nature of the cryptographic algorithm, and on m, the length of the check value.

4.1.4.1 ISO/IEC 9797-1: *Part 1: Mechanism using a Cryptographic Check Function Employing a Block Cipher Algorithm.*

4.1.4.2 ISO/IEC 9797-2: *Part 2: Mechanism using a dedicated Hash Function.*

4.1.5 ISO/IEC 9798: *Entity Authentication*

This is a five part standard specifying an authentication model and general requirements and constraints for entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is the one that is claimed. An entity to be authenticated proves its identity by showing its knowledge of a secret. The mechanisms are defined as exchanges of information between entities and, where required, exchanges with a trusted third party. The standard comprises the following parts: General; Mechanisms using Symmetric Encipherment Algorithms; Entity Authentication using a Public Key Algorithm; Mechanisms using a Cryptographic Check Function; Mechanisms using Zero Knowledge Techniques.

4.1.5.1 ISO/IEC 9798-1: *Part 1: General Model.*

4.1.5.2 ISO/IEC 9798-2: *Part 2: Entity Authentication Mechanisms using a Symmetric Algorithm..*

4.1.5.3 ISO/IEC 9798-3: *Part 3: Entity Authentication Using a Public Key Algorithm.*

4.1.5.4 ISO/IEC 9798-4: *Part 4: Entity Authentication Using Cryptographic Check Function.*

4.1.5.5 ISO/IEC 9798-5: *Part 5: Entity Authentication Using Zero Knowledge Techniques.*

4.1.6 ISO/IEC 10164: *Audit*

Part eight of the Open Systems Interconnection: Systems Management standard defines the security audit trail function which may be used by an application process in a centralised or decentralised management environment to exchange information and commands for the purpose of systems management. The specification defines a set of notifications for security related events, a set of service primitives, the parameters passed in each primitive, the semantic description of each primitive, and conformance requirements.

4.1.7 ISO/IEC 10181: *Security Frameworks*

4.1.7.1

The Security Frameworks standard is promulgated in eight parts and addresses the application of security services in an Open Systems environment. The frameworks address both data elements and sequences of operations used to obtain specific security services, but not protocol elements. The frameworks address a broad field of information systems security, including OSI, ODP, Databases, and Distributed Applications, and refines and extends the security concepts in each of these models.

4.1.7.2

The eight parts of this standard are: Overview, Authentication, Access Control, Non-Repudiation, Integrity, Confidentiality, Audit, and Key Management. The frameworks have a number of common concepts, including security domains, security authorities, security policies, trust, and trusted third parties. The frameworks presented here are further detailed in separate standards

4.1.7.3

The various parts of this standard describe the basic concepts of the specific security service, identify the possible classes of mechanisms available to support the service, define the management and services needed for these mechanisms, and identify the functional requirement for protocols to support them. The specific mechanisms and protocol exchanges are not, themselves, specified.

4.1.8 ISO/IEC 10736: *Transport Layer Security Protocol (TLSP)*

The Transport Layer Security Protocol (TLSP) is the second of the three main ISO/IEC lower layer security protocols, located wholly within the Transport Layer which operates in conjunction

with the Transport Protocol Data Units (TPDUs) and the associated TPDU generation/processing procedures specified in ISO/IEC 8073 and ISO/IEC 8602 without any modification to formats and procedures. The protocol operates by encapsulating TPDUs between ends using the following mechanisms: security label, direction indicator, integrity check-value, encipherment, and encipherment padding.

4.1.9 ISO/IEC 10745: *Generic Upper Layers Security*

ISO/IEC 7498-2 defines the security related architectural elements which are appropriate for application when security protection is required in an open systems environment. This standard describes the selection, placement, and use of security services and mechanisms in the Application, Presentation, and Session layers of the OSI Reference Model. It provides a basis for the development of application-independent services and protocols for security in these layers, and the utilization of these services and protocols to fulfil the security requirements of a wide variety of applications.

4.1.10 ISO/IEC 11577: *Network Layer Security Protocol (NLSP)*

The Network Layer of the OSI model is a complex layer requiring many standards. The Network Layer Security Protocol (NLSP) is the third of the three lower layers security protocols, and is one of the network layer standards for security which can operate in either connection-oriented or connectionless mode. NLSP can be considered to be a sublayer which might be positioned in one of several different places within the Network Layer, and uses an encapsulation technique similar to that used by TLSP, with two additional features: an integrity sequence number, and a traffic padding field to support traffic flow security.

4.1.11 ISO/IEC 11770: *Key Management*

This three part standard identifies the objectives of key management and describes a general model on which key management mechanisms are based. It defines key management services and mechanisms and the management of key material throughout its life cycle. The standard is promulgated in the three parts: Framework; Mechanisms using Symmetric Techniques; and Mechanisms using Asymmetric Techniques.

4.1.11.1 ISO/IEC 11770: *Part 1 Framework*

4.1.11.2 ISO/IEC 11770: *Part 2 Mechanisms using symmetric techniques*

4.1.11.3 ISO/IEC 11770: *Part 3 Mechanisms using asymmetric techniques*

4.1.12 ISO/IEC 13888: Non-Repudiation

This standard describes the model for non-repudiation mechanisms providing evidence based on non-repudiation certificates generated using symmetric or asymmetric techniques. The standard provides non-repudiation mechanisms for evidence generation, transfer, storage, retrieval, verification, and dispute resolution.

4.1.12.1 ISO/IEC 13888-1: *Part 1 General model*

4.1.12.1 ISO/IEC 13888-2: *Part 2 Mechanisms using symmetric techniques*

4.1.12.1 ISO/IEC 13888-3: *Part 3 Mechanisms using asymmetric techniques*

4.1.13 ISO/IEC 8073: *Information technology – Open systems interconnection – Protocol for providing the connection-mode transport service*

4.1.14 ISO/IEC 8602: *Information technology – Protocol for providing the OSI connectionless-mode transport service*

4.1.15 ISO/IEC TR 15947 *Information Technology-Security techniques - Framework for intrusion detection*

Explains the role of intrusion detection in IT risk management. It seeks to establish common definitions for intrusion detection terms and concepts. The objective is to define a framework for detection of intrusions into IT systems. It seeks to establish common definitions for intrusion detection terms and concepts. It describes the methodologies and concepts and the relationships among them; it addresses possible orderings of intrusion detection tasks and related activities, and attempts to relate these tasks and processes to an organization's or enterprise's procedures to demonstrate the practical integration of intrusion detection within an organization or enterprise security policy.

4.1.16 ISO/IEC 15816 *Information Technology- Security techniques - Security Information Objects for access control*

The document 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.

4.1.17 ISO/IEC 15945 / ITU-T X.843*: Information technology - Security techniques - Specification of TTP services to support the application of digital signatures*

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. Those topics are mainly covered in TR 14516.

4.1.18 ISO/IEC 18014 *Information Technology- Security techniques – Time stamping services*

Defines time-stamping services that are provided using time-stamp tokens between the participating entities, the time-stamping mechanisms that produce independent tokens, (that is proofs of existence that can be verified one by one), and mechanisms based on the usage of several tokens that altogether provide the desired guarantees. This document is in 3 parts.

4.1.18.1 Part 1 serves as the introductory part for time-stamping. In this it 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.

4.1.18.2 Refer to the Section 4.5.13 for Parts 2 and 3 which are at Draft stage.

4.2 ISO/IEC Cryptographic mechanisms

4.2.1 ISO/IEC 9796 *Digital Signature Scheme giving Message Recovery*

A digital signature in electronic exchange of information is a counterpart to a handwritten signature in traditional mail, and is based upon a public key system. This standard is in two parts, one defining a digital signature scheme for messages of limited length, and the other for messages of at least 128 bits.

4.2.1.1 ISO/IEC 9796-2 *Integer factorisation based mechanisms*

4.2.1.2 ISO/IEC 9796-3 *Discrete logarithm based mechanisms*

4.2.2 ISO/IEC 10116: *Modes of Operation for an n-bit Block Cipher*

This standard establishes four defined modes of operation for the application of an n-bit block cipher algorithm. These modes are Electronic Codebook Mode (ECB), Cipher Block Chaining (CBC), Cipher Feedback Mode (CFB), and Output Feedback Mode (OFB).

4.2.3 ISO/IEC 10118: *Hash Functions*

This is a four part standard which specifies the operation of hash functions which are required in the authentication, integrity, and non-repudiation security services. The hash functions defined by ISO/IEC 10118 require the use of a secret key . The standard provides guidance on initialization and padding values and, in Part 2, the use of an n-bit block cipher to create the hash value. The third part of the standard specifies dedicated (specially designed) hash functions based on the iterative use of a round-function. Part 4 covers the creation of hash functions using modular arithmetic secure hashing techniques (MASH-1 and MASH-2).

4.2.3.1 ISO/IEC 10118-1: *Part 1 General*

4.2.3.2 ISO/IEC 10118-2: *Part 2 Hash functions using an n-bit cipher algorithm*

4.2.3.3 ISO/IEC 10118-3: *Part 3 Dedicated hash functions*

4.2.3.4 ISO/IEC 10118-4: *Part 4 Hash functions using modular arithmetic*

4.2.4 ISO/IEC TR 14516: *Guidelines for the use and management of Trusted Third Party services*

This is a guideline, which provides an overview of the basic duties of trusted third parties (TTPs), their role and their functions; guidelines to assist in the design, development, and operation of TTPs; guidance on the services provided by a TTP; and guidance regarding internetworking and mutual recognition of TTPs.

4.2.5 ISO/IEC 14888: *Digital Signatures with Appendix*

This is a three part standard defining the creation and verification of a digital signature using asymmetric cryptographic techniques. In this standard, the verification technique needs the message as part of input, and uses a hash function in the calculation of the message appendix. The standard is applicable to the data origin authentication, non-repudiation, and integrity of data security services.

4.2.5.1 ISO/IEC 14888: *Part 1 General*

4.2.5.2 ISO/IEC 14888: *Part 2 Identity based mechanisms*

4.2.6 ISO/IEC 8372: *Information processing - Modes of operation for a 64-bit block cipher algorithm*

Specifies four modes of operation for a 64-bit block cipher algorithm. These modes are Electronic codebook (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB), and Cipher Feedback (CFB). For some modes, padding may be required to insure that the input is of the necessary length. Padding techniques are not within the scope of this International Standard. Block cipher algorithms operate on blocks of data of fixed size but messages to be enciphered can be of any size. Four modes of operation for block cipher algorithms are widely used to cover most of the practical requirements for the use of encipherment in computer and network systems. The modes of operation as described in ANSI X3.106 and FIPS Publication 81 are a specific case of the modes specified in ISO/IEC 8372. The main difference lies in the use if arbitrary 64-bit block cipher algorithms in the case of ISO 8372.

4.2.7 ISO/IEC 15946: *Information Technology - Security Techniques – Cryptographic techniques based on elliptic curves*

Specifies public-key cryptographic techniques based on elliptic curves. They include the establishment of keys for secret-key systems, and digital signature mechanisms. Refer to the Section 4.5 for a description of Part 4, currently in Draft form.

4.2.7.1 *Part 1 General*

Describes the mathematical background and general techniques necessary for implementing any of the mechanisms described in other parts of ISO/IEC 15946. The scope of this standard is restricted to cryptographic techniques based on elliptic curves defined over finite fields of prime power order (including the special cases of prime order and characteristic two). The representation of elements of the underlying finite field (i.e. which basis is used) is outside the scope of this standard.

4.2.7.2 *Part 2 Digital Signatures*

This international standard describes mechanisms for digital signatures based on elliptic curves. In particular, it describes techniques for:

- digital signatures with appendix, based on elliptic curves, and
- digital signatures giving message recovery, based on elliptic curves.

4.2.7.3 *Part 3 Key establishment*

This part of ISO/IEC 15946 specifically addresses the use of elliptic curve public-key techniques to (a) Establish a shared secret key between two entities A and B by key agreement. In a secret key agreement mechanism the secret key is the result of a data exchange between the two entities A and B. Neither of them can predetermine the value of the shared key. and (b) Establish a shared secret key between two entities A and B by key transport. In a secret key transport mechanism the secret key is chosen by one entity A and is transferred to another entity B, suitably protected by asymmetric techniques.

4.3 ISO/IEC Banking

4.3.1 ISO/IEC 8583: *Banking - Financial Transaction Card originated Messages - Interchange Message Specifications*

This standard covers the requirements for interchange of EFTPOS transactions, including the cryptographic mechanisms.

4.3.2 ISO/IEC 8730: *Banking - Requirements for Message Authentication (Wholesale)*

This standard specifies methods to be used for protecting the authenticity of wholesale financial messages by means of a message authentication code. The whole or part of a message may be protected.

4.3.3 ISO/IEC 8731: *Banking - Approved Algorithms for Message Authentication*

Two algorithms which may be used to generate message authentication codes are described in this standard, each promulgated as a separate part. They are: the Data Encryption Algorithm (DEA); and a special purpose algorithm designed for high speed message authentication.

4.3.4 ISO/IEC 8732: *Banking - Key Management (Wholesale)*

This standard specifies methods for the management of keying material used for the encipherment, decipherment, and authentication of messages exchanged in the course of wholesale financial transactions.

4.3.5 ISO/IEC 9564: *Banking - Personal Identification Number Management and Security*

4.3.5.1
This standard specifies the minimum security measures required for effective PIN management and, in a second part, the algorithms approved for the encipherment of PINs.

4.3.5.2
The standard provides a means of interchanging PIN data and specifies the rules related to the approval of PIN encipherment algorithms. It is applicable to institutions responsible for implementing techniques for the management and protection of the PIN for bank card originated transactions.

4.3.6 ISO/IEC 9807: *Banking and Financial Services - Requirements for Message Authentication (Retail)*

4.3.6.1
This standard specifies the procedures to be used for protecting the integrity of retail banking messages and for verifying that the messages originated from an authorized source. It also describes the method by which algorithms are approved for use for the authentication of retail banking messages.

4.3.6.2
The standard includes an annex which lists the algorithms approved for the calculation of a message authentication code and the procedures necessary to prevent exhaustive key determination. A method of generation of pseudo-random keys is also given.

4.3.7 ISO/IEC 9992: *Financial Transaction Cards - Messages between the Integrated Circuit Card and the Card Accepting Device*

This standard, promulgated in two parts, details the functions required for financial interchange, the structure and types of messages between the integrated circuit card and the card accepting device, and the identification of data elements which may or shall be used during exchanges. It also details the logical structure of files and records used in messages and how data elements are mapped into those messages.

4.3.8 ISO/IEC 10126: *Banking - Procedures for Message Encipherment (Wholesale)*

This two part standard defines procedures for the cryptographic protection of financial messages across any communications architecture, including store-and-forward and telex environments, and both public and private networks. The standard also includes a description of the Data Encryption Algorithm (DEA).

4.3.9 ISO/IEC 10202: *Financial Transaction Cards - Security Architectures of Financial Transaction Systems using Integrated Circuit Cards*

4.3.9.1
This eight part standard specifies techniques for the protection of integrated circuit cards used in financial transactions, through the whole of life from their manufacture and issue to card termination. The life cycle and the minimum levels of security required for interchange are described, and security options given.

4.3.9.2
The standard includes eight parts: Card Life cycle; Transaction Process; Cryptographic Key relationships; Secure Application Modules; Use of Algorithms; Cardholder Verification; Key management; and general Principles and Overview.

4.3.10 ISO/IEC 11131: *Banking - Financial Institution Sign-On Authentication*

This standard addresses three types of authentication between entities requesting access and entities capable of granting access: authentication via personal authentication information such as a password; authentication of a user via a user unique key; and authentication of a node via a node unique key.

4.3.11 ISO/IEC 11166: *Banking - Key Management by means of Asymmetric Algorithms*

This two part standard specifies methods for the management of keying material used for the encipherment, decipherment, and authentication of wholesale banking messages. It also specifies the requirements for control of the distribution and recovery of keying material. The standard specifies the RSA algorithm for encipherment and digital signature.

4.3.12 ISO/IEC 11568: *Banking - Key Management (Retail)*

4.3.12.1

This standard specifies the principles for the management of keys used in cipher systems implemented within the retail banking environment. The retail banking environment involves the interface between a card accepting device and an acquirer and between an acquirer and a card issuer. The standard applies to key management within symmetric and asymmetric cipher systems.

4.3.12.2

This standard is promulgated in 6 parts: Introduction to Key Management; Key Management Techniques for Symmetric Ciphers; Key Management Life Cycle for Symmetric Ciphers; Key Management Techniques using Public Key Cryptography; Key Life Cycle for Public Key Cryptosystems; and Key Management Schemes.

4.3.13 ISO/IEC 13491: *Secure Cryptographic Devices*

This standard states the requirements concerning both the operational characteristics of secure cryptographic devices, and the management of such devices throughout all stages of their life cycle. It also provides a means of verifying compliance with those requirements.

4.3.14 ISO/IEC 13492: *Key Management Related Data Elements (Retail)*

4.3.14.1

This standard specifies a key management related data element that may be necessary to be conveyed in electronically transmitted messages within the retail banking environment, where this environment involves the communications between a card accepting device and an acquirer and between an acquirer and a card issuer.

4.3.14.2

When ISO/IEC 8583 is used, the key management related data element defined within this standard is transmitted in ISO/IEC 8583 bit P-53 (Security related Control Information) to convey information about keys used for the current transaction and is transmitted in ISO/IEC 8583 bit S-96 (Key Management Data) to convey information about keys used for future transportation of key management related data to ISO/IEC 8583.

4.3.15 ISO/IEC 13569: *Banking and Financial Services - Information Security Guidelines for Banking*

This document presents an information security programme structure together with a guideline which defines accepted prudent business practice. Adoption of this guideline will result in a more uniformly secure banking system. Recognizing that information security demands can vary

greatly from institution to institution, or from application to application, flexibility was built into this document. Where appropriate, this document references and is consistent with existing standards.

4.4 ISO/IEC - Other

4.4.1 ISO/IEC 9735: EDI

ISO/IEC 9735: Electronic Data Interchange for administration, commerce, and transport (EDIFACT) is a seven part standard specifying the rules at the application level for structuring data in the interchange of electronic messages. There are three parts relevant to security: Part 5, Security Rules for Batch EDI for Authenticity, Integrity, and Non-repudiation; Part 6 Secure Authentication and Acknowledgment Message (AUTACK); and Part 7 Security Rules for Batch EDI for confidentiality.

4.4.2 ISO/IEC 9979: *Procedures for the Registration of Cryptographic Algorithms*

This standard provides the procedures to be followed and the information required for the submission of specific cryptographic algorithms for inclusion on the ISO/IEC Cryptographic Algorithms register. Registration provides the opportunity to establish a global ISO/IEC code for the algorithm but does not infer any form of ISO approval or endorsement of the algorithm. Refer to http://www.iso-register.com

4.5 ISO/IEC Projects at Draft Stage

4.5.1 CD 15946-4: *Information Technology - Security Techniques - Cryptographic techniques based on elliptic curves - Part 4: Digital signatures with message recovery*

This part of ISO/IEC 15946 specifically addresses the digital signatures giving message recovery based on elliptic curves to: (a) Provide the digital signatures giving message recovery with each type of redundancy: natural redundancy, added redundancy, or both and (b) Specify the general model for digital signatures giving partial or total message recovery aiming at reducing storage and transmission overhead.

4.5.2 CD 18014-3: *Information Technology – Security Techniques –Time Stamping Services: Part 3 Mechanisms producing linked tokens*

4.5.3 CD 18031: *Information Technology – Security Techniques –Random bit generation*

This standard specifies the main elements and security requirements of a random bit generator that are necessary for cryptographic applications. This standard includes:

(a) the description of the main elements required for a true (non-deterministic) random bit generator;
(b) the description of the main elements required for a pseudo-random (deterministic) bit generator;
(c) the description of a cryptographically secure random bit generator; characteristics of each; and
(d) security requirements.

4.5.4 CD 18032: *Information Technology – Security Techniques –Prime number generation*

4.5.5 CD 18033: *Information Technology – Security Techniques –Encryption Algorithms*

The primary purpose of encryption (or encipherment) techniques is to protect the confidentiality of stored or transmitted data. An encryption algorithm is applied to data (often called plaintext or cleartext), with the result being encrypted data (or ciphertext); this process is known as

encryption. The encryption algorithm should be designed so that the ciphertext yields no information about the plaintext except, perhaps, its length. Proposed as a four part document

4.5.5.1 CD 18033-1: *Encryption Algorithms Part 1: General*
The primary purpose of encryption (or encipherment) techniques is to protect the confidentiality of stored or transmitted data. An encryption algorithm is applied to data (often called plaintext or cleartext), with the result being encrypted data (or ciphertext); this process is known as encryption. The encryption algorithm should be designed so that the ciphertext yields no information about the plaintext except, perhaps, its length. Every encryption algorithm shall also provide for a decryption process, which shall transform ciphertext back to the original plain text. This part is general in nature, and provides definitions that apply in subsequent parts. 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.

4.5.5.2 WD 18033-2: Encryption Algorithms *Part 2: Asymmetric ciphers*
This standard 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 encrypt a message using this symmetric key.

4.5.5.3 WD18033-3: *Encryption Algorithms Part 3: Symmetric ciphers*
This part of ISO/IEC 18033 describes the specifications of block ciphers. These algorithms satisfies the requirements described in the Part 1 of this standard

4.5.5.4 WD18033-4: *Encryption Algorithms Part 4: Stream ciphers*

4.5.6 WD 18055: *Information Security - Security Techniques - Methodology for IT Security Evaluation*

4.5.7 PDTR 15446: *Information Security - Security Techniques - Guide for production of protection profiles and security targets*
Intended to provide the guidance necessary to support the development of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with the standard for Information Technology Security Evaluation. The objective is to provide a general guidance body of material, with annexes which provide guidance for specific product types, e.g. firewalls or relational databases. A guidance document is required to ensure that PPs and STs are developed in an efficient and consistent manner.

4.5.8 PDTR 15443: *Information Security - Security Techniques -A framework for IT assurance*
This draft Technical Report presents a variety of assurance methods, and to guide the IT Security Professional in the selection of an appropriate assurance method (or combination of methods) to achieve confidence that a given IT security product, system, service, process or environmental factor satisfies its stated security assurance requirements. This report examines assurance methods and approaches proposed by various types of organisations whether they are approved or de-facto standards.

4.5.8.1 PDTR 15443: *Part 1 Overview and framework*

4.5.8.2 PDTR 15443: *Part 2 Assurance methods*

4.5.8.3 PDTR 15443: *Part 3 Analysis of assurance methods*

4.5.9 WD 18028: *Information Security - Security Techniques – Network Security*

The general objectives of 18028 are to extend the security management guidelines provided in ISO/IEC TR 13335 - Guidelines for the Management of IT Security (GMITS) - by detailing the specific operations and mechanisms needed to implement network security safeguards and controls in a wider range of network environments, providing a bridge between general IT security management issues and network security technical implementations. The first edition of 18028 is expected to contain 4 parts. Part 1 is an overview of Network Security, covering management, models and policy, providing enough information for the standard to be useful on its own, whilst also providing linkage to the GMITS series. The remaining parts provide detailed guidance on the selection and implementation of security safeguards and controls in specific network environments:

(a) Securing Inter-network connections using Security Gateways.
(b) Securing Inter-network connections using Virtual Private Networks (VPN)s.
(c) Securing Remote Access connections to Networks.

4.5.10 WD 18044: *Information Security - Security Techniques –Information Security Incident Management*

This Technical Report (TR) type 3 provides advice and guidance on information security incident management for information security managers, and information system managers. Proper information security incident management requires appropriate planning and preparation, which has technical, organizational and procedural aspects. If any responses are to be effective, it is essential to develop comprehensive documentation of an information security incident (and weakness) reporting and handling scheme, along with its related procedures, processes and support tools. Further, the benefits must be clear and accepted by all concerned, otherwise information security incident management will not be successful. In addition, activity must be in line with the information security incident (and weakness) management policy, that should be covered in corporate, and individual system, service and network, information security policies.

4.5.11 NP 18045: *Information Security - Security Techniques – Methodology for IT security evaluation (MITSE)*

ISO/IEC 15408 Evaluation Criteria for IT Security specifies assurance requirements in its part 3. There is a need for a supporting document that details the minimum actions to be performed by the evaluators referenced. This proposed Technical Report 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. The Technical Report is intended to provide some support for the international recognition of evaluation results. This Technical Report is primarily aimed at those who are involved in the evaluation of Targets Of Evaluation (TOEs), Protection Profiles (PPs) and Security Targets (STs), and those who are responsible for defining and monitoring the application of the methodology for such evaluations. In addition the Technical Report is also intended to be useful to developers of PPs, STs and of TOEs that are to evaluated.

4.5.12 FDIS 7064 *Data processing - Check character systems*

This revision of ISO/IEC 7064:1983 specifies a set of check character systems capable of protecting strings against errors which occur when people copy or key data. The strings may be of fixed or variable length and may have character sets which are:

(a) numeric (10 digits: 0 to 9);
(b) alphabetic (26 letters: A to Z);
(c) alphanumeric (letters and digits).

Embedded spaces and special characters are ignored. This document specifies conformance requirements for products described as generating check characters or checking strings using the

systems given. It is for use in information interchange between organizations; it is also strongly recommended as good practice for internal information systems.

4.5.13 FDIS 18014- 2 *Information Security - Security Techniques – Time stamping services Part 2 Mechanisms producing independent tokens*

Defines time-stamping mechanisms that produce independent tokens, that is, proofs of existence that can be verified one by one.

4.5.13.1 CD 18014-3 *Information Security - Security Techniques – Time stamping services Part 3 Mechanisms producing linked tokens -*

Defines the additional data types that support the implementation of time-stamping mechanisms producing linked tokens. It also defines the linking, aggregation and publishing operations in time-stamping mechanisms producing linked tokens, as well as the related protocols. It defines two encapsulation methods for the resulting time-stamping data, using the data types defined in ISO/IEC 18014-1.

4.5.14 NP 21091: *Health Informatics - Directory Services for Security,Communications, and Identification of Professionals and Patients*

The Healthcare Directory and Certificate Registry is intended to support the communication and security requirements of healthcare providers in the conduct of clinical and administrative functions. Healthcare requires extensive encryption and access control requirements for the disclosure and transport of all confidential health information. In support of the Healthcare public key infrastructure, Healthcare will make available a registry of certificates including business and professional information necessary to conduct healthcare transactions. This information necessarily includes identification of individual roles within the healthcare system as can only be identified by the respective healthcare organizations. As such, the registration and management functions must be extensible, and potentially distributed throughout the healthcare community.

4.5.15 ISO/TC215 N266: *Health informatics – Security requirements for archiving and backup*

This two-part ISO Technical Specification (ISO/TS) describes the functional requirements for the following security services necessary for ensuring protection in the long-term digital archival of electronic health records: data integrity, origin authentication, data confidentiality and availability. The standard may define requirements for data structures and syntax, including the management of versions of referenced coding systems and other terminological systems; however, this standard will not define the format of the stored records. Requirements for a supporting public-key infrastructure for the verification of digital signatures should be included. Access conditions and possible methods for access, including the expressed consent by the data subject, could also be defined.

5 INTERNATIONAL TELEGRAPH AND TELEPHONE CONSULTATIVE COMMITTEE (CCITT) OF THE INTERNATIONAL TELECOMMUNICATIONS UNION (ITU)

5.1 X.500 Directory Standards

5.1.1 X.509: Directory Authentication

5.1.1.1

The X.509: Directory Authentication Framework standard defines three basic security services that can be used by all application layer OSI services: simple authentication, strong authentication, and digital signatures. Simple authentication is based on either the use of name and password (in the clear) or a security token consisting of the user name, password, a random

number, and a timestamp protected by a one way hash.

5.1.1.2

Strong authentication is based on asymmetric encryption techniques, and digital signatures are used to ensure data integrity by the use of asymmetric encryption on a message digest or hash value. X.509 has been adopted by ISO/IEC as ISO/IEC 9594-8, but is better known by its CCITT/ITU title.

5.2 X.700/800 Security Standards

5.2.1

The CCITT/ITU issue under their own cover, a number of the OSI architecture and ISO/IEC security standards which are also described in section 4. These include:

(a) Recommendation X.740: Information technology - Open Systems Interconnection - Systems management: Security audit trail function

(b) Recommendation X.741: Information technology - Open Systems Interconnection - Systems management: Objects and attributes for access control

(c) Recommendation X.800: Security architecture for Open Systems Interconnection for CCITT applications

(d) Recommendation X.802: Information technology - Lower layers security model

(e) Recommendation X.803: Information technology - Open Systems Interconnection - Upper layers security model

(f) Recommendation X.810: Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview

(g) Recommendation X.811: Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework

(h) Recommendation X.812: Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework

(i) Recommendation X.813: Information technology - Open Systems Interconnection - Security frameworks in open systems: Non-repudiation framework

(j) Recommendation X.814: Information technology - Open Systems Interconnection - Security frameworks for open systems: Confidentiality framework

(k) Recommendation X.815: Information technology - Open Systems Interconnection - Security frameworks for open systems: Integrity frameworks

(l) Recommendation X.816: Information technology - Open Systems Interconnection - Security frameworks for open systems: Security audit and alarms framework

(m) Recommendation X.830: Information technology - Open Systems Interconnection - Generic upper layers security: Overview, models and notation

(n) Recommendation X.831: Information technology - Open Systems Interconnection - Generic upper layers security: Security Exchange Service Element (SESE) service definition 20

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

(p) Recommendation X.833: Information technology - Open Systems Interconnection - Generic

upper layers security: Protecting transfer syntax specification

(q) Recommendation X.834: Information technology - Open systems interconnection - Generic upper layers security: Security exchange service element (SESE) protocol implementation conformance statement (PICS) pro forma

(r) Recommendation X.835: Information technology - Open Systems Interconnection - Generic upper layers security: Protecting transfer syntax Protocol Implementation Conformance Statement (PICS) pro forma

6 INTERNET RELATED

(Available from www.rfc-editor.org)

6.1 Request for comments

6.1.1 RFC 1153: *Digest Message Format*

6.1.1.1

In the mid-70s, moderators of high traffic volume mailing lists developed a digest message format to enclose several messages into one composite message for redistribution to the mailing list addressees. This format reduces the mailer load in proportion to the number of messages contained within a digest message, and conserves network bandwidth by reducing the size of the headers of the enclosed messages.

6.1.1.2

This RFC documents the de facto standard digest message format to be used in creating and separating digest messages. It is not meant to supersede nor replace the generic message encapsulation format described in RFC 934. It merely documents a particular message encapsulation format that existed well before RFC 934 was published and continues to be the format of choice for digest messages.

6.1.2 RFC 1281: *Guidelines for the Secure Operation of the Internet*

The purpose of this document is to provide a set of guidelines to aid in the secure operation of the Internet. During its history, the Internet has grown significantly and is now quite diverse. Its participants include government institutions and agencies, academic and research institutions, commercial network and electronic mail carriers, non-profit research centers and an increasing array of industrial organizations who are primarily users of the technology. Despite this dramatic growth, the system is still operated on a purely collaborative basis. Each participating network takes responsibility for its own operation. Service providers, private network operators, users and vendors all cooperate to keep the system functioning.

6.1.3 RFC 1319: *The MD2 Message-Digest Algorithm*

This document describes the MD2 message-digest algorithm. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit “fingerprint” or “message digest” of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest. The MD2 algorithm is intended for digital signature applications, where a large file must be “compressed” in a secure manner before being signed with a private (secret) key under a public-key cryptosystem such as RSA

6.1.4 RFC 1320: *The MD4 Message-Digest Algorithm*

6.1.4.1
This document describes the MD4 message-digest algorithm. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit “fingerprint” or “message digest” of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest. The MD4 algorithm is intended for digital signature applications, where a large file must be “compressed” in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

6.1.4.2
The MD4 algorithm is designed to be quite fast on 32-bit machines. In addition, the MD4 algorithm does not require any large substitution tables; the algorithm can be coded quite compactly.

6.1.5 RFC 1321: *The MD5 Message-Digest Algorithm*

6.1.5.1
This document describes the MD5 message-digest algorithm. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit “fingerprint” or “message digest” of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be “compressed” in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

6.1.5.2
The MD5 algorithm is designed to be quite fast on 32-bit machines. In addition, the MD5 algorithm does not require any large substitution tables; the algorithm can be coded quite compactly. The MD5 algorithm is an extension of the MD4 message-digest algorithm. MD5 is slightly slower than MD4, but is more “conservative” in design. MD5 was designed because MD4 was being adopted for use more quickly than justified by the existing critical review; because MD4 was designed to be exceptionally fast, it is “at the edge” in terms of risking successful cryptanalytic attack. MD5 backs off a bit, giving up a little in speed for a much greater likelihood of ultimate security.

6.1.6 RFC 1352: *SNMP Security Protocols*

6.1.6.1
The Simple Network Management Protocol (SNMP) specification allows for the protection of network management operations by a variety of security protocols. The SNMP administrative model provides a framework for securing SNMP network management. In the context of that framework, this memo defines protocols to support the following three security services: data integrity, data origin authentication, and data confidentiality.

6.1.6.2
In the SNMP model, each party is, by definition, associated with a single authentication protocol. The authentication protocol provides a mechanism by which SNMP management communications transmitted by the party may be reliably identified as having originated from that party. The authentication protocol defined in this memo also reliably determines that the message received is the message that was sent.

6.1.6.3
Similarly, each SNMP party is, by definition, associated with a single privacy protocol. The privacy protocol provides a mechanism by which SNMP management communications transmitted to said party are protected from disclosure. The privacy protocol in this memo specifies that only authenticated messages may be protected from disclosure. The two protocols described are the Digest Authentication Protocol and the Symmetric Privacy Protocol. Both protocols described here require the sharing of secret information between the originator of a message and its recipient. The protocol specifications assume the existence of the necessary secrets. The selection of such secrets and their secure distribution to appropriate parties may be accomplished by a variety of strategies. One such strategy is presented.

6.1.7 RFC 1355: *Privacy and Accuracy Issues in Network Information Center Databases*

6.1.7.1
This document provides a set of guidelines for the administration and operation of public Network Information Center (NIC) databases. The purpose is to formalise procedures for the responsible handling of the personal and organizational information maintained by NICs in publicly accessible databases, and to improve the accuracy and accessibility of such data where appropriate.

6.1.7.2
The purpose of this document is to consider the privacy and accuracy issues that result from many NIC databases being publicly accessible. This document considers only generic concerns about such systems; it intentionally does not make recommendations for specific databases on the Internet. Clearly, it is the responsibility of each NIC to determine what procedures should apply for each of its databases. The document discusses the obligations a NIC that maintains such a database has towards those about whom data appears in the database. These obligations apply to database entries that contain information that is publicly accessible to Internet users.

6.1.8 RFC 1411: *Telnet Authentication: Kerberos Version 4*
This standard defines an experimental authentication mechanism for use across the Internet.

6.1.9 RFC 1412: *Telnet Authentication: SPX*
This standard defines an experimental authentication mechanism for use across the Internet.

6.1.10 RFC 1413: *Identification Protocol*

6.1.10.1
The Identification Protocol provides a means to determine the identity of a user of a particular TCP connection. Given a TCP port number pair, it returns a character string which identifies the owner of that connection on the server's system.

6.1.10.2
The Identification Protocol was formerly called the Authentication Server Protocol. It has been renamed to better reflect its function. This is a connection based application on TCP. A server listens for TCP connections on TCP port 113 (decimal). Once a connection is established, the server reads a line of data which specifies the connection of interest. If it exists, the system dependent user identifier of the connection of interest is sent as the reply. The server may then either shut the connection down or it may continue to read/respond to multiple queries.

6.1.11 RFC 1414: *Identification MIB*
The Identification MIB defines a uniform set of objects useful for identifying users associated with TCP connections. End-systems which support TCP may, at their option, implement this MIB.

6.1.12 RFC 1416: *Telnet Authentication Option*

6.1.12.1

The purpose of the AUTHENTICATION option is to provide a framework for the passing of authentication information through the TELNET session. This means that: 1) the users password will not be sent in clear text across the network, and 2) if the front end TELNET process has the appropriate authentication information, it can automatically send the information, and the user will not have to type any password.

6.1.12.2

It is intended that the AUTHENTICATION option be general enough that it can be used to pass information for any authentication system. However, the ability to negotiate a common authentication mechanism between client and server is a feature of the authentication option that should be used with caution. When the negotiation is performed, no authentication has yet occurred. Therefore, each system has no way of knowing whether or not it is talking to the system it intends. An intruder could attempt to negotiate the use of an authentication system which is either weak, or already compromised by the intruder.

6.1.13 RFC 1421: *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures*

6.1.13.1

This document defines message encryption and authentication procedures, in order to provide privacy-enhanced mail (PEM) services for electronic mail (RFC-822 textual mail environment) transfer in the Internet. It is one member of a related set of four standards (RFC 1421-1424). The procedures defined in this document are compatible with a wide range of key management approaches, including both symmetric (secret-key) and asymmetric (public-key) approaches for encryption of data encrypting keys. Use of symmetric cryptography for message text encryption and/or integrity check computation is anticipated.

6.1.13.2

Privacy enhancement services (confidentiality, authentication, message integrity assurance, and non-repudiation of origin) are offered through the use of end-to-end cryptography between originator and recipient processes at or above the User Agent level. No special processing requirements are imposed on the Message Transfer System at end points or at intermediate relay sites. This approach allows privacy enhancement facilities to be incorporated selectively on a site-by-site or user-by-user basis without impact on other Internet entities. Interoperability among heterogeneous components and mail transport facilities is supported.

6.1.14 RFC 1422: *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management*

This is one of a series of documents defining privacy enhancement mechanisms for electronic mail transferred using Internet mail protocols. The key management architecture described in this document is compatible with the authentication framework described in CCITT 1988 X.509. This document goes beyond X.509 by establishing procedures and conventions for a key management infrastructure for use with Privacy Enhanced Mail (PEM) and with other protocols, from both the TCP/IP and OSI suites, in the future. The infrastructure specified in this document establishes a single root for all certification within the Internet, the Internet Policy Registration Authority (IPRA), beneath which exist Policy Certification Authorities and Certification Authorities.

6.1.15 RFC 1423: *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers*

This document provides definitions, formats, references, and citations for cryptographic

algorithms, usage modes, and associated identifiers and parameters used in support of Privacy Enhanced Mail (PEM) in the Internet community. It is intended to become one member of the set of related PEM RFCs. This document is organized into four primary sections, dealing with message encryption algorithms, message integrity check algorithms, symmetric key management algorithms, and asymmetric key management algorithms (including both asymmetric encryption and asymmetric signature algorithms).

6.1.16 RFC 1424: *Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services*

This document describes three types of service in support of Internet Privacy-Enhanced Mail (PEM): key certification, certificate-revocation list (CRL) storage, and CRL retrieval. Such services are among those required of an RFC 1422 certification authority. Other services such as certificate revocation and certificate retrieval are left to the certification authority to define, although they may be based on the services described in this document.

6.1.17 RFC 1446: *Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)*

6.1.17.1

The authentication protocol provides a mechanism by which SNMPv2 management communications transmitted by the party may be reliably identified as having originated from that party. The authentication protocol defined in this memo also reliably determines that the message received is the message that was sent.

6.1.17.2

The privacy protocol provides a mechanism by which SNMPv2 management communications transmitted to said party are protected from disclosure. The privacy protocol in this memo specifies that only authenticated messages may be protected from disclosure.

6.1.17.3 The RFC defines two authentication protocols: the Digest Authentication Protocol and the Symmetric Privacy Protocol. Both protocols described here require the sharing of secret information between the originator of a message and its recipient. The protocol specifications assume the existence of the necessary secrets. The RFC provides a strategy for selection of such secrets and their secure distribution to appropriate parties.

6.1.18 RFC 1455: *Physical Link Security Type of Service*

This RFC documents an experimental protocol providing a Type of Service (TOS) to request maximum physical link security. This is an addition to the types of service enumerated in RFC 1349: Type of Service in the Internet Protocol Suite. The new TOS requests the network to provide what protection it can against surreptitious observation by outside agents of traffic so labelled. The purpose is protection against traffic analysis and as an additional possible level of data confidentiality. This TOS is consistent with all other defined types of service for IP version 4 in that it is based on link level characteristics and will not provide any particular guaranteed level of service.

6.1.19 RFC 1457: *Security Label Framework for the Internet*

This memo presents a security labelling framework for the Internet. The framework is intended to help protocol designers determine what, if any, security labelling should be supported by their protocols. The framework should also help network architects determine whether or not a particular collection of protocols fulfil their security labelling requirements. The Open Systems Interconnection Reference Model provides the structure for the presentation.

6.1.20 RFC 1507: *DASS Distributed Authentication Security Service*

6.1.20.1

The goal of authentication is to reliably learn the name of the originator of a message or request. The classic way by which people authenticate to computers (and by which computers authenticate to one another) is by supplying a password. There are a number of problems with existing password based schemes which DASS attempts to solve. The goal of DASS is to provide authentication services in a distributed environment which are both more secure (more difficult for a bad guy to impersonate a good guy) and easier to use than existing mechanisms.

6.1.20.2

DASS uses cryptographic mechanisms to provide “strong, mutual” authentication. Mutual authentication means that the two parties communicating each reliably learn the name of the other. Strong authentication means that in the exchange neither obtains any information that it could use to impersonate the other to a third party. This can’t be done with passwords alone. Mutual authentication can be done with passwords by having a “sign” and a “counter-sign” which the two parties must utter to assure one another of their identities. But whichever party speaks first reveals information which can be used by the second (unauthenticated) party to impersonate it. Longer sequences (often seen in spy movies) cannot solve the problem in general. Further, anyone who can eavesdrop on the conversation can impersonate either party in a subsequent conversation (unless passwords are only good once). Cryptography provides a means whereby one can prove knowledge of a secret without revealing it. People cannot execute cryptographic algorithms in their heads, and thus cannot strongly authenticate to computers directly. DASS lays the groundwork for “smart cards”: microcomputers sealed in credit cards which when activated by a PIN will strongly authenticate to a computer. Until smart cards are available, the first link from a user to a DASS node remains vulnerable to eavesdropping. DASS mechanisms are constructed so that after the initial authentication, smart card or password based authentication looks the same.

6.1.20.3

DASS supports the concept of global identity and network login. A user is assigned a name from a global namespace and that name will be recognized by any node in the network. (In some cases, a resource may be configured as accessible only by a particular user acting through a particular node. That is an access control decision, and it is supported by DASS, but the user is still known by his global identity). From a practical point of view, this means that a user can have a single password (or smart card) which can be used on all systems which allow him access and access control mechanisms can conveniently give access to a user through any computer the user happens to be logged into. Because a single user secret is good on all systems, it should never be necessary for a user to enter a password other than at initial login. Because cryptographic mechanisms are used, the password should never appear on the network beyond the initial login node.

6.1.21 *RFC 1508: Generic Security Service Application Program Interface*

The Generic Security Service Application Program Interface (GSS-API) definition provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments. This specification defines GSS-API services and primitives at a level independent of underlying mechanism and programming language environment, and is to be complemented by other, related specifications:

(a) Documents defining specific parameter bindings for particular language environments
(b) Documents defining token formats, protocols, and procedures to be implemented in order to realise GSS-API services atop particular security mechanisms

6.1.22 RFC 1509: *Generic Security Service API : C-bindings*

6.1.22.1

This document specifies C language bindings for the Generic Security Service Application Program Interface (GSS-API), which is described at a language-independent conceptual level in other documents.

6.1.22.2

The Generic Security Service Application Programming Interface (GSS-API) provides security services to its callers, and is intended for implementation atop alternative underlying cryptographic mechanisms. Typically, GSS-API callers will be application protocols into which security enhancements are integrated through invocation of services provided by the GSS-API. The GSS-API allows a caller application to authenticate a principal identity associated with a peer application, to delegate rights to a peer, and to apply security services such as confidentiality and integrity on a per-message basis.

6.1.23 RFC 1510: *The Kerberos Network Authentication Service (V5)*

6.1.23.1

The Kerberos model is based in part on Needham and Schroeder's trusted third-party authentication protocol and on modifications suggested by Denning and Sacco. The original design and implementation of Kerberos Versions 1 through 4 was the work of two former Project Athena staff members, Steve Miller of Digital Equipment Corporation and Clifford Neuman (now at the Information Sciences Institute of the University of Southern California), along with Jerome Saltzer, Technical Director of Project Athena, and Jeffrey Schiller, MIT Campus Network Manager. Many other members of Project Athena have also contributed to the work on Kerberos. Version 4 is publicly available, and has seen wide use across the Internet.

6.1.23.2

Version 5 (described in this document) has evolved from Version 4 based on new requirements and desires for features not available in Version 4.

6.1.24 RFC 1544: *The Content-MD5 Header Field*

6.1.24.1

Despite all of the mechanisms provided by MIME which attempt to protect data from being damaged in the course of email transport, it is still desirable to have a mechanism for verifying that the data, once decoded, are intact. For this reason, this memo defines the use of an optional header field, Content-MD5, which may be used as a message integrity check (MIC), to verify that the decoded data are the same data that were initially sent.

6.1.24.2

MD5 is an algorithm for computing a 128 bit "digest" of arbitrary-length data, with a high degree of confidence that any alterations in the data will be reflected in alterations in the digest. This memo specifies how the algorithm may be used as an integrity check for MIME mail.

6.1.25 RFC 1734: *POP3 AUTHentication command*

This document describes the optional AUTH command, for indicating an authentication mechanism to the server, performing an authentication protocol exchange, and optionally negotiating a protection mechanism for subsequent protocol interactions. The authentication and protection mechanisms used by the POP3 AUTH command are those used by IMAP4.

6.1.26 RFC 1750: *Randomness Recommendations*

6.1.26.1

Security systems today are built on increasingly strong cryptographic algorithms that foil pattern analysis attempts. However, the security of these systems is dependent on generating secret quantities for passwords, cryptographic keys, and similar quantities. The use of pseudo-random processes to generate secret quantities can result in pseudo-security. The sophisticated attacker of these security systems may find it easier to reproduce the environment that produced the secret quantities, searching the resulting small set of possibilities, than to locate the quantities in the whole of the number space.

6.1.26.2

Choosing random quantities to foil a resourceful and motivated adversary is surprisingly difficult. This paper points out many pitfalls in using traditional pseudo-random number generation techniques for choosing such quantities. It recommends the use of truly random hardware techniques and shows that the existing hardware on many systems can be used for this purpose. It provides suggestions to ameliorate the problem when a hardware solution is not available. And it gives examples of how large such quantities need to be for some particular applications.

6.1.27 RFC 1760: *The S/KEY One-Time Password System*

6.1.27.1

One form of attack on computing system connected to the Internet is eavesdropping on network connections to obtain login id's and passwords of legitimate users. The captured login id and password are, at a later time, used to gain access to the system. The S/KEY One-Time Password system is designed to counter this type of attack, called a replay attack.

6.1.27.2

With the S/KEY system, only a single use password ever crosses the network. The user's secret pass-phrase never crosses the network at any time, including during login or when executing other commands requiring authentication such as the UNIX commands passwd or su. Thus, it is not vulnerable to eavesdropping/replay attacks. Added security is provided by the property that no secret information need be stored on any system, including the host being protected.

6.1.27.3

The S/KEY system protects against external passive attacks against the authentication subsystem. It does not prevent a network eavesdropper from gaining access to private information, and does not provide protection against "inside jobs" or against active attacks where the potential intruder is able to intercept and modify the packet stream.

6.1.28 RFC 1824: *The Exponential Security System TESS*

This informational RFC describes the basic mechanisms and functions of an identity based system for the secure authenticated exchange of cryptographic keys, the generation of signatures, and the authentic distribution of public keys.

6.1.29 RFC 1828: *IP Authentication using Keyed MD5*

The Authentication Header (AH) [RFC-1826] provides integrity and authentication for IP datagrams. This specification describes the AH use of keys with Message Digest 5 (MD5) [RFC-1321]. All implementations that claim conformance or compliance with the Authentication Header specification MUST implement this keyed MD5 mechanism. This document assumes that the reader is familiar with the related document "Security Architecture for the Internet Protocol" [RFC-1825], which defines the overall security plan for IP, and provides important background for this specification.

6.1.30 RFC 1829: *The ESP DES-CBC Transform*

6.1.30.1
The Encapsulating Security Payload (ESP) [RFC-1827] provides confidentiality for IP datagrams by encrypting the payload data to be protected. This specification describes the ESP use of the Cipher Block Chaining (CBC) mode of the US Data Encryption Standard (DES) algorithm.

6.1.30.2
All implementations that claim conformance or compliance with the Encapsulating Security Payload specification must implement this DES-CBC transform.

6.1.30.3
This document assumes that the reader is familiar with the related document “Security Architecture for the Internet Protocol” [RFC-1825], which defines the overall security plan for IP, and provides important background for this specification.

6.1.31 RFC 1847: *Security Multiparts for MIME*

6.1.31.1
This standard defines a framework within which security services may be applied to MIME body parts. MIME, an acronym for “Multipurpose Internet Mail Extensions”, defines the format of the contents of Internet mail messages and provides for multi-part textual and non-textual message bodies. The new content types are subtypes of multipart: signed and encrypted.

6.1.31.2
A MIME security component will contain two body parts: one for the protected data and one for the control information necessary to remove the protection. The type and contents of the control information body parts are determined by the value of the protocol parameter of the enclosing multipart/signed or multipart/encrypted content type, which is required to be present. By registering new values for the required protocol parameter, the framework is easily extended to accommodate a variety of protocols.

6.1.32 RFC 1848: *MIME Object Security Services (MOSS)*

MIME Object Security Services (MOSS) define a protocol that uses the multipart/signed and multipart/encrypted framework [7] to apply digital signature and encryption services to MIME objects. The services are offered through the use of end-to-end cryptography between an originator and a recipient at the application layer. Asymmetric (public key) cryptography is used in support of the digital signature service and encryption key management. Symmetric (secret key) cryptography is used in support of the encryption service. The procedures are intended to be compatible with a wide range of public key management approaches, including both ad hoc and certificate-based schemes. Mechanisms are provided to support many public key management approaches.

6.1.33 RFC 1910: *User-based Security Model for SNMPv2*

6.1.33.1
A management system contains: several (potentially many) nodes, each with a processing entity, termed an agent, which has access to management instrumentation; at least one management station; and, a management protocol, used to convey management information between the agents and management stations. Operations of the protocol are carried out under an administrative framework which defines authentication, authorization, access control, and privacy policies.

6.1.33.2
Management stations execute management applications which monitor and control managed elements. Managed elements are devices such as hosts, routers, terminal servers, etc., which are monitored and controlled via access to their management information.

6.1.33.3
The Administrative Infrastructure for SNMPv2 document [1] defines an administrative framework which realises effective management in a variety of configurations and environments. In this administrative framework, a security model defines the mechanisms used to achieve an administratively-defined level of security for protocol interactions. This document defines the security model for this administrative framework.

6.1.33.4
This administrative framework includes the provision of an access control model. The enforcement of access rights requires the means to identify the entity on whose behalf a request is generated. This SNMPv2 security model identifies an entity on whose behalf an SNMPv2 message is generated as a “user”.

6.1.33.5
This memo defines an Experimental Protocol for the Internet community but is not an Internet standard per se.

6.1.34 RFC 1929: *Username/Password Authentication for SOCKS V5*
The protocol specification for SOCKS Version 5 specifies a generalised framework for the use of arbitrary authentication protocols in the initial socks connection setup. This document describes one of those protocols, as it fits into the SOCKS Version 5 authentication “sub-negotiation”.

6.1.35 RFC 1961: *GSS-API Authentication Method for SOCKS Version 5*

6.1.35.1
The protocol specification for SOCKS Version 5 specifies a generalised framework for the use of arbitrary authentication protocols in the initial SOCKS connection setup. This document provides the specification for the SOCKS V5 GSS-API authentication protocol, and defines a GSS-API-based encapsulation for provision of integrity, authentication and optional confidentiality.

6.1.35.2
GSS-API provides an abstract interface which provides security services for use in distributed applications, but isolates callers from specific security mechanisms and implementations. GSS-API peers achieve interoperability by establishing a common security mechanism for security context establishment - either through administrative action, or through negotiation. GSS-API is specified in RFCs 1508 and 1509. This specification is intended for use with implementations of GSS-API, and the emerging GSS-API V2 specification.

6.1.35.3
The approach for use of GSS-API in SOCKS V5 is to authenticate the client and server by successfully establishing a GSS-API security context - such that the GSS-API encapsulates any negotiation protocol for mechanism selection, and the agreement of security service options. The GSS-API enables the context initiator to know what security services the target supports for the chosen mechanism. The required level of protection is then agreed by negotiation. The GSS-API per-message protection calls are subsequently used to encapsulate any further TCP and UDP traffic between client and server.

6.1.36 RFC 1964: *The Kerberos Version 5 GSS-API Mechanism*
This document discusses protocol-visible characteristics of the GSS-API mechanism to be

implemented on top of Kerberos V5 security technology per RFC-1508 and RFC-1510; it defines elements of protocol for interoperability and is independent of language bindings per RFC-1509. This specification is subject to ongoing experimentation, testing, and evolution and is not currently defined as a proposed standard RFC. Tokens transferred between GSS-API peers (for security context management and per-message protection purposes) are defined. The data elements exchanged between a GSS-API endpoint implementation and the Kerberos KDC are not specific to GSS-API usage and are therefore defined within RFC-1510 rather than within this specification.

6.1.37 RFC 1968: *The PPP Encryption Control Protocol (ECP)*

The Point-to-Point Protocol (PPP) [1] provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP also defines an extensible Link Control Protocol. This document defines a method for negotiating data encryption over PPP links.

6.1.38 RFC 1991: *PGP Message Exchange Formats*

PGP (Pretty Good Privacy) uses a combination of public-key and conventional encryption to provide security services for electronic mail messages and data files. These services include confidentiality and digital signature. PGP is widely used throughout the global computer community. This document describes the format of “PGP files”, i.e., messages that have been encrypted and/or signed with PGP. This document describes the message exchange formats used in versions 2.x of PGP. Specifically, versions 2.6 and 2.7 conform to this specification. Version 2.3 conforms to this specification with minor differences.

6.1.39 RFC 1994: *PPP Challenge Handshake Authentication Protocol (CHAP)*

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP also defines an extensible Link Control Protocol, which allows negotiation of an Authentication Protocol for authenticating its peer before allowing Network Layer protocols to transmit over the link. This document defines a method for Authentication using PPP, which uses a random Challenge, with a cryptographically hashed Response which depends upon the Challenge and a secret key.

6.1.40 RFC 2015: *MIME Security with Pretty Good Privacy (PGP)*

This document describes how Pretty Good Privacy (PGP) can be used to provide privacy and authentication using the Multipurpose Internet Mail Extensions (MIME) security content types described in RFC1847. Three new content types for implementing security and privacy with PGP are described: application/pgp-encrypted, application/pgp-signature and application/pgp-keys.

6.1.41 RFC 2025: *The Simple Public-Key GSS-API Mechanism (SPKM)*

6.1.41.1

The SPKM is a GSS-API Mechanism providing authentication, key establishment, data integrity, and data confidentiality in an on-line distributed application environment using a public-key infrastructure. Because it conforms to the interface defined by RFC1508, SPKM can be used as a drop-in replacement by any application which makes use of security services through GSS-API calls (for example, any application which already uses the Kerberos GSS-API for security). The use of a public-key infrastructure allows digital signatures supporting non-repudiation to be employed for message exchanges, and provides other benefits such as scalability to large user populations.

6.1.41.2

The tokens defined in SPKM are intended to be used by application programs according to the

GSS API “operational paradigm”. A typical GSS-API caller is itself a communications protocol [or is an application program which uses a communications protocol], calling on GSS-API in order to protect its communications with authentication, integrity, and/or confidentiality security services. A GSS-API caller accepts tokens provided to it by its local GSS-API implementation and transfers the tokens to a peer on a remote system; that peer passes the received tokens to its local GSS-API implementation for processing.

6.1.41.3

This document defines two separate GSS-API mechanisms, SPKM-1 and SPKM-2, whose primary difference is that SPKM-2 requires the presence of secure timestamps for the purpose of replay detection during context establishment and SPKM-1 does not. This allows greater flexibility for applications since secure timestamps cannot always be guaranteed to be available in a given environment.

6.1.42 RFC 2040: *The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms*

This document defines four ciphers with enough detail to ensure interoperability between different implementations. The first cipher is the raw RC5 block cipher. The RC5 cipher takes a fixed size input block and produces a fixed sized output block using a transformation that depends on a key. The second cipher, RC5-CBC, is the Cipher Block Chaining (CBC) mode for RC5. It can process messages whose length is a multiple of the RC5 block size. The third cipher, RC5-CBC-Pad, handles plaintext of any length, though the ciphertext will be longer than the plaintext by at most the size of a single RC5 block. The RC5-CTS cipher is the Cipher Text Stealing mode of RC5, which handles plaintext of any length and the ciphertext length matches the plaintext length.

6.1.43 RFC 2065: *Domain Name Security Extensions*

6.1.43.1

This document describes extensions of the Domain Name System (DNS) protocol to support DNS security and public key distribution. The document provides an overview of the extensions and the key distribution, data origin authentication, and transaction and request security they provide.

6.1.43.2

The document discusses the KEY resource record, its structure, use in DNS responses, and file representation for the public keys of entities named in the DNS and are used for key distribution. It also describes the SIG digital signature resource record, its structure, use in DNS responses, and file representation used to authenticate other resource records in the DNS and optionally to authenticate DNS transactions and requests. It also discusses the NXT resource record and its use in DNS responses. The NXT RR permits authenticated denial in the DNS of the existence of a name or of a particular type for an existing name.

6.1.43.3

The document describes how a resolver can be configured with a starting key or keys and proceed to securely resolve DNS requests. Interactions between resolvers and servers are discussed for all combinations of security aware and security non-aware. Two additional query header bits are defined for signalling between resolvers and servers. It also reviews a variety of operational considerations including key generation, lifetime, and storage and levels of conformance for resolvers and servers.

6.1.44 RFC 2069: *An Extension to HTTP: Digest Access Authentication*

The HTTP 1.0 protocol includes specification for a Basic Access Authentication scheme. However, this scheme is not considered to be a secure method of user authentication, as the

user name and password are passed over the network in an unencrypted form. RFC 2069 specifies a new authentication scheme for inclusion in HTTP v1.1 and future protocols, referred to as “Digest Access Authentication”. The Digest Access Authentication scheme is not intended to be a complete answer to the need for security in the World Wide Web, rather provides a weak access authentication method which avoids the most serious flaws of Basic authentication. Like Basic Access Authentication, the Digest scheme is based on a simple challenge-response paradigm. The Digest scheme challenges using a nonce value. A valid response contains a checksum (by default the MD5 checksum) of the username, the password, the given nonce value, the HTTP method, and the requested URI. In this way, the password is never sent in the clear. Just as with the Basic scheme, the username and password must be prearranged in some fashion which is not addressed by this document.

6.1.45 RFC 2078: *Generic Security Service Application Program Interface, Version 2*

The Generic Security Service Application Program Interface (GSS-API), as defined in RFC-1508, provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments. RFC 2078 revises RFC-1508, making specific, incremental changes in response to implementation experience and liaison requests. It is intended, therefore, that this memo will become the basis for subsequent progression of the GSS-API specification on the standards track. RFC 2078 is rendered obsolete by RFC- 2735 and FRC-2743

6.1.46 RFC 2082: *RIP-MD5 Authentication*

6.1.46.1

The increasing use of the Internet has resulted in the need for improved authentication of routing information. RIP-2 provides for unauthenticated service (as in classical RIP), or password authentication. Both are vulnerable to passive attacks currently widespread in the Internet. Well-understood security issues exist in routing protocols. Clear text passwords, currently specified for use with RIP-2, are no longer considered sufficient.

6.1.46.2

If authentication is disabled, then only simple misconfigurations are detected. Simple passwords transmitted in the clear are of little use in providing access control as a hostile process can simply intercept the password and use it to penetrate the network.

6.1.46.3

RIP-2 uses an authentication algorithm, as was originally proposed for SNMP Version 2, augmented by a sequence number. The standard authentication algorithm for RIP-2 is keyed MD5, but the mechanism is intended to be algorithm-independent. While this mechanism is not unbreakable (no known mechanism is), it provides a greatly enhanced probability that a system being attacked will detect and ignore hostile messages. The output of the authentication algorithm, rather than the secret RIP-2 Authentication Key, is transmitted and is a one-way function of a message and a secret RIP-2 Authentication Key. This RIP-2 Authentication Key is never sent over the network in the clear, thus providing protection against the passive attacks now commonplace in the Internet.

6.1.46.4

In this way, protection is afforded against forgery or message modification. It is possible to replay a message until the sequence number changes, but the sequence number makes replay in the long term less of an issue. The mechanism does not afford confidentiality, since messages stay in the clear; however, the mechanism is also exportable from most countries, which test a privacy algorithm would fail.

6.1.46.5
Keyed MD5 is also being used for OSPF cryptographic authentication, and is therefore present in routers already, as is some form of password management. A similar approach has been standardised for use in IP-layer authentication.

6.1.47 RFC 2084: *Considerations for Web Transaction Security*

6.1.47.1
The use of the HyperText Transport Protocol for commercial services and personal or private data necessitates the development of secure versions that include privacy and authentication services. Such services may be provided as extensions to HTTP, or as encapsulating security protocols. This RFC reviews the security requirements for all such enhancements to HTTP under the generic term Web Transaction Security (WTS).

6.1.47.2
WTS is an enhancement to an object transport protocol. As such, it does not provide independent certification of documents or other data objects outside of the scope of the transfer of said objects. In addition, security at the WTS layer is independent of and orthogonal to security services provided at underlying network layers. It is envisioned that WTS may coexist in a single transaction with such mechanisms, each providing security services at the appropriate level, with at worst some redundancy of service.

6.1.47.3
WTS defines the following services: confidentiality of the HTTP request and/or response; data origin authentication and data integrity of the HTTP request and/or response; non-repudiability of origin for the request and/or response; transmission freshness of request and/or response; ease of integration with other features of HTTP; and support of multiple mechanisms for the above services.

6.1.47.4
Confidentiality is required for both requests and responses. Because the identity of the object being requested is potentially sensitive, the URI of the request should be confidential; this is particularly critical in the common case of form data or other user input being passed in the URI.

6.1.47.5
HTTP needs to be able to authenticate the gatewayed services to the client and vice-versa. It should support the authentication of the HTTP server or gatewayed services regardless of intermediary proxy or caching servers. To allow user privacy, WTS must support service authentication with user anonymity. Because the identity of the object being requested is potentially sensitive, service authentication should occur before any part of the request, including the URI of the requested object, is passed. In cases where the authentication process depends on the URI (or other header data) of the request, such as gatewayed services, the minimum necessary information to identify the entity to be authenticated should be passed.

6.1.47.6
The WTS will need to provide assurance of the integrity of the HTTP transaction, including the HTTP headers and data objects of both client requests and server responses.

6.1.48 RFC 2085: *HMAC-MD5 IP Authentication with Replay Prevention*

The Authentication Header provides integrity and authentication for IP datagrams. The transform specified in this document uses a keyed-MD5 mechanism known as HMAC-MD5. The mechanism uses the (key-less) MD5 hash function which produces a message digest. When combined with an AH Key, authentication data is produced. This value is placed in the Authentication Data field of the AH. This value is also the basis for the data integrity service

offered by the AH protocol. To provide protection against replay attacks, a Replay Prevention field is included as a transform option. This field is used to help prevent attacks in which a message is stored and re-used later, replacing or repeating the original. The Security Parameters Index is used to determine whether this option is included in the AH.

6.1.49 RFC 2104: *HMAC - Keyed Hashing for Message Authentication*

Providing a way to check the integrity of information transmitted over or stored in an unreliable medium is a prime necessity in the world of open computing and communications. Mechanisms that provide such integrity check based on a secret key are usually called “message authentication codes” (MAC). Typically, message authentication codes are used between two parties that share a secret key in order to validate information transmitted between these parties. RFC 2104 presents a message authentication mechanism based on cryptographic hash functions called HMAC. HMAC can be used in combination with any iterated cryptographic hash function. MD5 and SHA-1 are examples of such hash functions. HMAC also uses a secret key for calculation and verification of the message authentication values.

6.1.50 RFC 2137: *Secure Domain Name System Dynamic Update*

Domain Name System (DNS) protocol extensions have been defined to authenticate the data in DNS and provide key distribution services. DNS Dynamic Update operations have also been defined, but without a detailed description of security for the update operation. This memo describes how to use DNSSEC digital signatures covering requests and data to secure updates and restrict updates to those authorized to perform them as indicated by the updater’s possession of cryptographic keys.

6.1.51 RFC 2138: *Remote Authentication Dial In User Service (RADIUS)*

6.1.51.1

Managing dispersed serial line and modem pools for large numbers of users can create the need for significant administrative support. Since modem pools are by definition a link to the outside world, they require careful attention to security, authorization and accounting. This can be best achieved by managing a single “database” of users, which allows for authentication (verifying user name and password) as well as configuration information detailing the type of service to deliver to the user (for example, SLIP, PPP, telnet, rlogin). This document specifies a remote authentication dial in user service.

6.1.51.2

A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

6.1.51.3

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an insecure network could determine a user’s password.

6.1.51.4

The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the user name and original password given by the user, it can support PPP PAP or CHAP,

UNIX login, and other authentication mechanisms.

6.1.52 RFC 2144: *The CAST-128 Encryption Algorithm*

There is a need in the Internet community for an unencumbered encryption algorithm with a range of key sizes that can provide security for a variety of cryptographic applications and protocols. This document describes an existing algorithm that can be used to satisfy this requirement. Included are a description of the cipher and the key scheduling algorithm, the s-boxes, and a set of test vectors.

6.1.53 RFC 2154: *OSPF with Digital Signatures*

This memo describes the extensions to OSPF required to add digital signature authentication to Link State data, and to provide a certification mechanism for router data. Added LSA processing and key management is detailed. A method for migration from, or co- existence with, standard OSPF V2 is described.

6.1.54 RFC 2179: *Network Security For Trade Shows*

This document is designed to assist vendors and other participants in trade shows, such as Networld+Interop, in designing effective protection against network and system attacks by unauthorized individuals. Generally, it has been observed that many system administrators and trade show coordinators tend to overlook the importance of system security at trade shows and such systems are at least as prone to attack as office-based platforms. This document is not intended to replace the multitudes of comprehensive books on the subject of Internet security. Rather, its purpose is to provide a checklist-style collection of frequently overlooked, simple ways to minimize the chance of a costly attack.

6.1.55 RFC 2195: *IMAP/POP AUTHorize Extension for Simple Challenge/Response*

6.1.55.1

Existing proposed standards specify an AUTHENTICATE mechanism for the IMAP4 protocol and a parallel AUTH mechanism for the POP3 protocol. The AUTHENTICATE mechanism is intended to be extensible; the four methods specified in IMAP-AUTH are all fairly powerful and require some security infrastructure to support. The base POP3 specification also contains a lightweight challenge-response mechanism called APOP. APOP is associated with most of the risks associated with such protocols: in particular, it requires that both the client and server machines have access to the shared secret in cleartext form.

6.1.55.2

The Challenge-Response Authentication Mechanism (CRAM) offers a method for avoiding such cleartext storage while retaining the algorithmic simplicity of APOP in using only MD5, though in a “keyed” method. At present, IMAP lacks any facility corresponding to APOP. The only alternative to the strong mechanisms identified in IMAP-AUTH is a presumably cleartext username and password, supported through the LOGIN command in IMAP. RFC 2195 describes a simple challenge-response mechanism, similar to APOP and PPP CHAP that can be used with IMAP (and, in principle, with POP3). This mechanism also has the advantage over some possible alternatives of not requiring that the server maintain information about email “logins” on a per-login basis. While mechanisms that do require such per-login history records may offer enhanced security, protocols such as IMAP, which may have several connections between a given client and server open more or less simultaneous, may make their implementation particularly challenging.

6.1.56 RFC 2196: *Site Security Handbook*

This document is a first attempt at providing Internet users guidance on how to deal with security issues in the Internet. As such, this document is necessarily incomplete. There are some clear shortfalls; for example, this document focuses mostly on resources available in the United States. In the spirit of the Internet's "Request for Comments" series of notes, we encourage feedback from users of this handbook. In particular, those who utilize this document to craft their own policies and procedures. This handbook is meant to be a starting place for further research and should be viewed as a useful resource, but not the final authority. Different organizations and jurisdictions will have different resources and rules. Talk to your local organizations, consult an informed lawyer, or consult with local and national law enforcement. These groups can help fill in the gaps that this document cannot hope to cover.

6.1.57 RFC 2203: *RPCSEC_GSS Protocol Specification*

This memo describes an ONC/RPC security flavor that allows RPC protocols to access the Generic Security Services Application Programming Interface.

6.1.58 RFC 2228: *FTP Security Extensions*

This document defines extensions to the FTP specification STD 9, RFC 959, "FILE TRANSFER PROTOCOL (FTP)" (October 1985). These extensions provide strong authentication, integrity, and confidentiality on both the control and data channels with the introduction of new optional commands, replies, and file transfer encodings. The following new optional commands are introduced in this specification: AUTH (Authentication/Security Mechanism), ADAT (Authentication/Security Data), PROT (Data Channel Protection Level), PBSZ (Protection Buffer Size), CCC (Clear Command Channel), MIC (Integrity Protected Command), CONF (Confidentiality Protected Command), and ENC (Privacy Protected Command). A new class of reply types (6yz) is also introduced for protected replies. None of the above commands are required to be implemented, but interdependencies exist. These dependencies are documented with the commands.

6.1.59 RFC 2230: *Key Exchange Delegation Record for the DNS*

This standard describes a mechanism whereby authorization for one node to act as key exchanger for a second node is delegated and made available via the Secure DNS. This mechanism is intended to be used only with the Secure DNS. It can be used with several security services. For example, a system seeking to use IPSec to protect IP packets for a given destination can use this mechanism to determine the set of authorized remote key exchanger systems for that destination.

6.1.60 RFC 2245: *Anonymous SASL Mechanism*

It is common practice on the Internet 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 optional trace information, such as an email address, as the password. As plaintext login commands are not permitted in new IETF protocols, a new way to provide anonymous login is needed within the context of the SASL framework.

6.1.61 RFC 2267: *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

A number of Denial of Service (DoS) attacks which have employed forged source addresses have proven to be a troublesome issue for Internet Service Providers and the Internet community overall. This paper discusses a simple, effective, and straightforward method for using ingress traffic filtering to prohibit DoS attacks which use forged IP addresses to be propagated from

'behind' an Internet Service Provider's (ISP) aggregation point.

6.1.62 RFC 2268: *A Description of the RC2(r) Encryption Algorithm*

This memo describes a conventional (secret-key) block encryption algorithm, called RC2, which may be considered as a proposal for a DES replacement. The input and output block sizes are 64 bits each. The key size is variable, from one byte up to 128 bytes, although the current implementation uses eight bytes. The algorithm is designed to be easy to implement on 16-bit microprocessors. On an IBM AT, the encryption runs about twice as fast as DES (assuming that key expansion has been done).

6.1.63 RFC 2274: *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*

This document describes the User-based Security Model (USM) for 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 MIB for remotely monitoring/managing the configuration parameters for this Security Model.

6.1.64 RFC 2275: *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

This document describes the View-based Access Control Model for use in the SNMP architecture. It defines the Elements of Procedure for controlling access to management information. This document also includes a MIB for remotely managing the configuration parameters for the View-based Access Control Model.

6.1.65 RFC 2284: *PPP Extensible Authentication Protocol (EAP)*

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP also defines an extensible Link Control Protocol, which allows negotiation of an Authentication Protocol for authenticating its peer before allowing Network Layer protocols to transmit over the link. This document defines the PPP Extensible Authentication Protocol.

6.1.66 RFC 2286: *Test Cases for HMAC-RIPEMD160 and HMAC-RIPEMD128*

This document provides two sets of test cases for HMAC-RIPEMD160 and HMAC-RIPEMD128, respectively. HMAC-RIPEMD160 and HMAC-RIPEMD128 are two constructs of the HMAC message authentication function using the RIPEMD-160 and RIPEMD-128 hash functions. The test cases and results provided in this document are meant to be used as a conformance test for HMAC-RIPEMD160 and HMAC-RIPEMD128 implementations.

6.1.67 RFC 2289: *A One-Time Password System*

6.1.67.1

This document describes a one-time password authentication system (OTP). The system provides authentication for system access (login) and other applications requiring authentication that is secure against passive attacks based on replaying captured reusable passwords. OTP evolved from the S/KEY One-Time Password System described by Bellcore.

6.1.67.2

One form of attack on networked computing systems is eavesdropping on network connections to obtain authentication information such as the login IDs and passwords of legitimate users. Once this information is captured, it can be used at a later time to gain access to the system. One-time password systems are designed to counter this type of attack, called a "replay attack".

6.1.67.3
The authentication system described in this document uses a secret pass-phrase to generate a sequence of one-time (single use) passwords. With this system, the user's secret pass-phrase never needs to cross the network at any time such as during authentication or during pass-phrase changes. Thus, it is not vulnerable to replay attacks. Added security is provided by the property that no secret information need be stored on any system, including the server being protected.

6.1.67.4
The OTP system protects against external passive attacks against the authentication subsystem. It does not prevent a network eavesdropper from gaining access to private information and does not provide protection against either "social engineering" or active attacks.

6.1.68 RFC 2311: *S/MIME Version 2 Message Specification*

6.1.68.1
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). S/MIME can be used by traditional mail user agents (MUAs) to add cryptographic security services to mail that is sent, and to interpret cryptographic security services in mail that is received.

6.1.68.2
S/MIME is not restricted to mail; it can be used with any transport mechanism that transports MIME data, such as HTTP. As such, S/MIME takes advantage of the object-based features of MIME and allows secure messages to be exchanged in mixed-transport systems. Further, S/MIME can be used in automated message transfer agents that use cryptographic security services that do not require any human intervention, such as the signing of software-generated documents and the encryption of FAX messages sent over the Internet.

6.1.69 RFC 2312: *S/MIME Version 2 Certificate Handling*

S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a method to send and receive secure MIME messages. In order to validate the keys of a message sent to it, an S/MIME agent needs to certify that the key is valid. This memo describes the mechanisms S/MIME uses to create and validate keys using certificates. This specification is compatible with PKCS #7 in that it uses the data types defined by PKCS #7. It also inherits all the varieties of architectures for certificate-based key management supported by PKCS #7. In order to handle S/MIME certificates, a developer has to follow specifications in this memo, as well as some of the following specifications: "PKCS #1: RSA Encryption", "PKCS #7: Cryptographic Message Syntax", and "PKCS #10: Certification Request Syntax".

6.1.70 RFC 2314: *PKCS 10: Certification Request Syntax Version 1.5*

6.1.70.1
A certification request consists of a distinguished name, a public key, and optionally a set of attributes, collectively signed by the entity requesting certification. Certification requests are sent to a certification authority, who transforms the request to an X.509 public-key certificate, or a PKCS #6 extended certificate. (In what form the certification authority returns the newly signed certificate is outside the scope of this document. A PKCS #7 message is one possibility.)

6.1.70.2
The intention of including a set of attributes is twofold: to provide other information about a given

entity, such as the postal address to which the signed certificate should be returned if electronic mail is not available, or a "challenge password" by which the entity may later request certificate revocation; and to provide attributes for a PKCS #6 extended certificate. A non-exhaustive list of attributes is given in PKCS #9. Certification authorities may also require non-electronic forms of request and may return non-electronic replies.

6.1.70.3

It is expected that descriptions of such forms, which are outside the scope of this document, will be available from the certification authority. The preliminary intended application of this document is to support PKCS #7 cryptographic messages, but is expected that other applications will be developed.

6.1.71 RFC 2315: *PKCS 7: Cryptographic Message Syntax Version 1.5*

This document describes a general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes. The syntax admits recursion so that, for example, one envelope can be nested inside another, or one party can sign some previously enveloped digital data. It also allows arbitrary attributes, such as signing time, to be authenticated along with the content of a message, and provides for other attributes such as countersignatures to be associated with a signature. A degenerate case of the syntax provides a means for disseminating certificates and certificate-revocation lists.

6.1.72 RFC 2316: *Report of the IAB Security Architecture Workshop*

On 3-5 March 1997, the IAB held a security architecture workshop at Bell Labs in Murray Hill, NJ. This document reports on the outcomes of that workshop.

6.1.73 RFC 2350: *Expectations for Computer Security Incident Response*

The purpose of this document is to express the general Internet community's expectations of Computer Security Incident Response Teams (CSIRTs). It is not possible to define a set of requirements that would be appropriate for all teams, but it is possible and helpful to list and describe the general set of topics and issues which are of concern and interest to constituent communities. CSIRT constituents have a legitimate need and right to fully understand the policies and procedures of 'their' Computer Security Incident Response Team. One way to support this understanding is to supply detailed information which users may consider, in the form of a formal template completed by the CSIRT. An outline of such a template and a filled in example are provided.

6.1.74 RFC 2356: *Sun's SKIP Firewall Traversal for Mobile IP*

The Mobile IP specification establishes the mechanisms that enable a mobile host to maintain and use the same IP address as it changes its point of attachment to the network. Mobility implies higher security risks than static operation, because the traffic may at times take unforeseen network paths with unknown or unpredictable security characteristics. The Mobile IP specification makes no provisions for securing data traffic. The mechanisms described in this document allow a mobile node out on a public sector of the internet to negotiate access past a SKIP firewall, and construct a secure channel into its home network. In addition to securing traffic, our mechanisms allow a mobile node to roam into regions that (1) impose ingress filtering, and (2) use a different address space.

6.1.75 RFC 2367: *PF_KEY Key Management API, Version 2*

A generic key management API that can be used not only for IP Security but also for other network security services is presented in this document. Version 1 of this API was implemented

inside 4.4-Lite BSD as part of the U. S. Naval Research Laboratory's freely distributable and usable IPv6 and IPsec implementation. It is documented here for the benefit of others who might also adopt and use the API, thus providing increased portability of key management applications (e.g. a manual keying application, an ISAKMP daemon, a GKMP daemon, a Photuris daemon, or a SKIP certificate discovery protocol daemon).

6.1.76 RFC 2401: *Security Architecture for the Internet Protocol*

The goal of the IPSec architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments. This memo specifies the base architecture for IPsec compliant systems, the security services offered by the IPsec protocols, and how these services can be employed in the IP environment. The following fundamental components of the IPsec security architecture are discussed in terms of their underlying, required functionality: Security Protocols — Authentication Header (AH) and Encapsulating Security Payload (ESP); Security Associations — what they are and how they work, how they are managed, associated processing; Key Management — manual and automatic (The Internet Key Exchange (IKE)); and algorithms for authentication and encryption.

6.1.77 RFC 2402: *IP Authentication Header (AH)*

The Authentication Header is a mechanism for providing strong integrity and authentication for IP datagrams. It might also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed. For example, use of an asymmetric digital signature algorithm, such as RSA, could provide non-repudiation. Confidentiality, and protection from traffic analysis are not provided by the Authentication Header. Users desiring confidentiality should consider using the IP Encapsulating Security Protocol (ESP) either in lieu of, or in conjunction with the Authentication Header. This document assumes the reader has previously read the related IP Security Architecture document which defines the overall security architecture for IP and provides important background information for this specification.

6.1.78 RFC 2403: *The Use of HMAC-MD5-96 within ESP and AH*

This memo describes the use of the HMAC algorithm in conjunction with the MD5 algorithm as an authentication mechanism within the revised IPSEC Encapsulating Security Payload and the revised IPSEC Authentication Header. HMAC with MD5 provides data origin authentication and integrity protection.

6.1.79 RFC 2404: *The Use of HMAC-SHA-1-96 within ESP and AH*

This memo describes the use of the HMAC algorithm in conjunction with the SHA-1 algorithm (FIPS-180-1) as an authentication mechanism within the revised IPSEC Encapsulating Security Payload and the revised IPSEC Authentication Header. HMAC with SHA-1 provides data origin authentication and integrity protection.

6.1.80 RFC 2405: *The ESP DES-CBC Cipher Algorithm With Explicit IV*

This document describes the use of the DES Cipher algorithm in Cipher Block Chaining Mode, with an explicit IV, as a confidentiality mechanism within the context of the IPSec Encapsulating Security Payload.

6.1.81 RFC 2406: *IP Encapsulating Security Payload (ESP)*

ESP is a mechanism for providing integrity and confidentiality to IP datagrams. It may also provide authentication, depending on which algorithm and algorithm mode are used. Non-repudiation and protection from traffic analysis are not provided by ESP. The IP Authentication Header (AH) can provide non-repudiation if used with certain authentication algorithms. The IP

Authentication Header can be used in conjunction with ESP to provide authentication, and can on its own provide integrity and authentication without confidentiality. This document assumes that the reader is familiar with the related document “IP Security Architecture”, which defines the overall Internet-layer security architecture for IPv4 and IPv6 and provides important background for this specification.

6.1.82 RFC 2407: *The Internet IP Security Domain of Interpretation for ISAKMP*
The Internet Security Association and Key Management Protocol (ISAKMP) defines a framework for security association management and cryptographic key establishment for the Internet. This framework consists of defined exchanges, payloads, and processing guidelines that occur within a given Domain of Interpretation (DOI). This document defines the Internet IP Security DOI (IPSEC DOI), which instantiates ISAKMP for use with IP when IP uses ISAKMP to negotiate security associations.

6.1.83 RFC 2408: *Internet Security Association and Key Management Protocol (ISAKMP)*
This memo describes a protocol utilizing security concepts necessary for establishing Security Associations (SA) and cryptographic keys in an Internet environment. A Security Association protocol that negotiates, establishes, modifies and deletes Security Associations and their attributes is required for an evolving Internet, where there will be numerous security mechanisms and several options for each security mechanism. The key management protocol must be robust in order to handle public key generation for the Internet community at large and private key requirements for those private networks with that requirement. The Internet Security Association and Key Management Protocol (ISAKMP) defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques, and threat mitigation (e.g. denial of service and replay attacks). All of these are necessary to establish and maintain secure communications (via IP Security Service or any other security protocol) in an Internet environment.

6.1.84 RFC 2409: *The Internet Key Exchange (IKE)*
ISAKMP provides a framework for authentication and key exchange but does not define them. It is designed to be key exchange independant; that is, it is designed to support many different key exchanges. Oakley describes a series of key exchanges -- called “modes”-- and details the services provided by each (e.g. perfect forward secrecy for keys, identity protection, and authentication). SKEME describes a versatile key exchange technique which provides anonymity, repudiability, and quick key refreshment. This document describes a protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI.

6.1.85 *RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec*
This memo defines the NULL encryption algorithm and its use with the IPsec Encapsulating Security Payload (ESP). NULL does nothing to alter plaintext data. In fact, NULL, by itself, does nothing. NULL provides the means for ESP to provide authentication and integrity without confidentiality.

6.1.86 RFC 2411: *IP Security Document Roadmap*
The IPsec protocol suite is used to provide privacy and authentication services at the IP layer. Several documents are used to describe this protocol suite. The interrelationship and organization of the various documents covering the IPsec protocol are discussed here. An explanation of what to find in which document, and what to include in new Encryption Algorithm and Authentication Algorithm documents are described.

6.1.87 RFC 2412: *The OAKLEY Key Determination Protocol*

This document describes a protocol, named OAKLEY, by which two authenticated parties can agree on secure and secret keying material. The basic mechanism is the Diffie-Hellman key exchange algorithm. The OAKLEY protocol supports Perfect Forward Secrecy, compatibility with the ISAKMP protocol for managing security associations, user-defined abstract group structures for use with the Diffie-Hellman algorithm, key updates, and incorporation of keys distributed via out-of-band mechanisms.

6.1.88 RFC 2419: *The PPP DES Encryption Protocol (DESE)*

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. The PPP Encryption Control Protocol (ECP) defined in RFC 1968 provides a method to negotiate and utilize encryption protocols over PPP encapsulated links. This document provides specific details for the use of the DES standard for encrypting PPP encapsulated packets.

6.1.89 RFC 2420: *The PPP Triple-DES Encryption Protocol (3DESE)*

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. The PPP Encryption Control Protocol (ECP) provides a method to negotiate and utilize encryption protocols over PPP encapsulated links. This document provides specific details for the use of the Triple-DES standard (3DES) for encrypting PPP encapsulated packets.

6.1.90 RFC 2437: *PKCS #1: RSA Cryptography Specifications Version 2.0*

This document provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering the following aspects: cryptographic primitives, encryption schemes, signature schemes with appendix, and ASN.1 syntax for representing keys and for identifying the schemes. The recommendations are intended for general application within computer and communications systems, and as such include a fair amount of flexibility. It is expected that application standards based on these specifications may include additional constraints. The recommendations are intended to be compatible with draft standards currently being developed by the ANSI X9F1 and IEEE P1363 working groups.

6.1.91 RFC 2440: *OpenPGP Message Format*

This document is maintained in order to publish all necessary information needed to develop interoperable applications based on the OpenPGP format. It is not a step-by-step cookbook for writing an application. It describes only the format and methods needed to read, check, generate, and write conforming packets crossing any network. It does not deal with storage and implementation questions. It does however, discuss implementation issues necessary to avoid security flaws. 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.

6.1.92 *RFC 2444:* *The One-Time-Password SASL Mechanism*

6.1.92.1

This document describes a method for adding authentication support to connection-based protocols. To use this specification, a protocol includes a command for identifying and authenticating a user to a server and for optionally negotiating protection of subsequent protocol interactions. If its use is negotiated, a security layer is inserted between the protocol and the

connection. This document describes how a protocol specifies such a command, defines several mechanisms for use by the command, and defines the protocol used for carrying a negotiated security layer over the connection.

6.1.92.2

The One Time Password (OTP) provides a useful authentication mechanism for situations where there is limited client or server trust. Currently, OTP is added to protocols in an ad-hoc fashion with heuristic parsing. This specification defines an OTP SASL mechanism so it can be easily and formally integrated into many application protocols

6.1.93 RFC 2451: *The ESP CBC-Mode Cipher Algorithms*

This document describes how to use CBC-mode cipher algorithms with the IPSec ESP (Encapsulating Security Payload) Protocol. It not only clearly states how to use certain cipher algorithms, but also how to use all CBC-mode cipher algorithms.

6.1.94 RFC 2459: *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*

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.

6.1.95 RFC 2478: *The Simple and Protected GSS-API Negotiation Mechanism*

This document specifies a Security Negotiation Mechanism for the Generic Security Service Application Program Interface (GSS-API). The GSS-API provides a generic interface which can be layered atop different security mechanisms such that if communicating peers acquire GSS-API credentials for the same security mechanism, then a security context may be established between them (subject to policy). The Simple and Protected GSS-API Negotiation Mechanism defined in this standard is a pseudo-security mechanism, represented by the object identifier iso.org.dod.internet.security.mechanism.snego(1.3.6.1.5.5.2) which enables GSS-API peers to determine in-band whether their credentials share common GSS-API security mechanism(s), and if so, to invoke normal security context establishment for a selected common security mechanism. This is most useful for applications that are based on GSS-API implementations which support multiple security mechanisms. This allows to negotiate different security mechanisms, different options within a given security mechanism or different options from several security mechanisms.

6.1.96 RFC 2479: *Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)*

The IDUP-GSS-API extends the GSS-API for applications requiring protection of a generic data unit (such as a file or message) in a way which is independent of the protection of any other data unit and independent of any concurrent contact with designated “receivers” of the data unit. Thus, it is suitable for applications such as secure electronic mail where data needs to be protected without any on-line connection with the intended recipient(s) of that data. The protection offered by IDUP includes services such as data origin authentication with data integrity, data confidentiality with data integrity, and support for non-repudiation services. Subsequent to being

protected, the data unit can be transferred to the recipient(s) - or to an archive - perhaps to be processed ("unprotected") only days or years later.

6.1.97 RFC 2480: *Gateways and MIME Security Multiparts*
This document examines the problems associated with use of MIME security multiparts and gateways to non-MIME environments. A set of requirements for gateway behavior are defined which provide facilities necessary to properly accomodate the transfer of security multiparts through gateways.

6.1.98 RFC 2487: *SMTP Service Extension for Secure SMTP over TLS*
This document describes an extension to the SMTP service that allows an SMTP server and client to use transport-layer security to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers.

6.1.99 RFC 2504: *Users' Security Handbook*
The Users' Security Handbook is the companion to the Site Security Handbook (SSH). It is intended to provide users with the information they need to help keep their networks and systems secure.

6.1.100 RFC 2505: *Anti-Spam Recommendations for SMTP MTAs*

6.1.100.1
This memo gives a number of implementation recommendations for SMTP, MTAs (Mail Transfer Agents, e.g. sendmail) to make them more capable of reducing the impact of spam. The intent is that these recommendations will help clean up the spam situation, if applied on enough SMTP MTAs on the Internet, and that they should be used as guidelines for the various MTA vendors. We are fully aware that this is not the final solution, but if these recommendations were included, and used, on all Internet SMTP MTAs, things would improve considerably and give time to design a more long term solution.

6.1.100.2
The Future Work section suggests some ideas that may be part of such a long term solution. It might, though, very well be the case that the ultimate solution is social, political, or legal, rather than technical in nature. The implementor should be aware of the increased risk of denial of service attacks that several of the proposed methods might lead to. For example, increased number of queries to DNS servers and increased size of logfiles might both lead to overloaded systems and system crashes during an attack. A brief summary of this memo is: (a) Stop unauthorized mail relaying; (b) Spammers then have to operate in the open; deal with them; (c) Design a mail system that can handle spam.

6.1.101 RFC 2510: *Internet X.509 Public Key Infrastructure Certificate Management Protocols*
This document describes the Internet X.509 Public Key Infrastructure (PKI) Certificate Management Protocols. Protocol messages are defined for all relevant aspects of certificate creation and management. Note that "certificate" in this document refers to an X.509v3 Certificate.

6.1.102 RFC 2511: *Internet X.509 Certificate Request Message Format*
This document describes the Certificate Request Message Format (CRMF). This syntax is used to convey a request for a certificate to a Certification Authority, possibly via a Registration Authority, for the purposes of X.509 certificate production. The request will typically include a

public key and associated registration information.

6.1.103 RFC 2521: *ICMP Security Failures Messages*
This document specifies ICMP messages for indicating failures when using IP Security Protocols (AH and ESP).

6.1.104 RFC 2528: *Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates*
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.

6.1.105 RFC 2535: *Domain Name System Security Extensions*
Extensions to the Domain Name System (DNS) are described that provide data integrity and authentication to security aware resolvers and applications through the use of cryptographic digital signatures. These digital signatures are included in secured zones as resource records. Security can also be provided through non-security aware DNS servers in some cases. The extensions provide for the storage of authenticated public keys in the DNS. This storage of keys can support general public key distribution services as well as DNS security. The stored keys enable security aware resolvers to learn the authenticating key of zones in addition to those for which they are initially configured. Keys associated with DNS names can be retrieved to support other protocols. Provision is made for a variety of key types and algorithms. In addition, the security extensions provide for the optional authentication of DNS protocol transactions and requests.

6.1.106 RFC 2536: *DSA KEYs and SIGs in the Domain Name System (DNS)*
A standard method for storing US Government Digital Signature Algorithm keys and signatures in the Domain Name System is described which utilizes DNS KEY and SIG resource records.

6.1.107 RFC 2537: *RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)*
A standard method for storing RSA keys and RSA/MD5 based signatures in the Domain Name System is described which utilizes DNS KEY and SIG resource records.

6.1.108 RFC 2538: *Storing Certificates in the Domain Name System (DNS)*
Cryptographic public keys are frequently published and their authenticity demonstrated by certificates. A CERT resource record is defined so that such certificates and related certificate revocation lists can be stored in the Domain Name System.

6.1.109 RFC 2539: *Storage of Diffie-Hellman Keys in the Domain Name System (DNS)*
A standard method for storing Diffie-Hellman keys in the Domain Name System is described which utilizes DNS KEY resource records.

6.1.110 RFC 2541: *DNS Security Operational Considerations*
Secure DNS is based on cryptographic techniques. A necessary part of the strength of these techniques is careful attention to the operational aspects of key and signature generation, lifetime, size, and storage. In addition, special attention must be paid to the security of the high level zones, particularly the root zone. This document discusses these operational aspects for keys and signatures used in connection with the KEY and SIG DNS resource records.

6.1.111 RFC 2559: Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2

This memo describes a syntax for embedding S-HTTP negotiation parameters in HTML documents. S-HTTP, as described by RFC 2660, contains the concept of negotiation headers which reflect the potential receiver of a message's preferences as to which crypto- graphic enhancements should be applied to the message. This document describes a syntax for binding these negotiation parameters to HTML anchors.

6.1.112 RFC 2560: *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*

This memo describes a syntax for securing messages sent using the Hypertext Transfer Protocol (HTTP), which forms the basis for the World Wide Web. Secure HTTP (S-HTTP) provides independently applicable security services for transaction confidentiality, authenticity/integrity and non-repudiability of origin. The protocol emphasizes maximum flexibility in choice of key management mechanisms, security policies and cryptographic algorithms by supporting option negotiation between parties for each transaction.

6.1.113 RFC 2574: *User-based Security Model (USM) for SNMPv3*

This document describes the User-based Security Model (USM) for SNMP version 3 for use in the SNMP architecture [RFC2571]. It defines the Elements of Procedure for providing SNMP message level security. This document also includes a MIB for remotely monitoring/managing the configuration parameters for this Security Model.

6.1.114 RFC 2575: *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

This document describes the View-based Access Control Model for use in the SNMP architecture [RFC2571]. It defines the Elements of Procedure for controlling access to management information. This document also includes a MIB for remotely managing the configuration parameters for the View-based Access Control Model.

6.1.115 RFC 2577: *FTP Security Considerations*

The specification for the File Transfer Protocol (FTP) contains a number of mechanisms that can be used to compromise network security. The FTP specification allows a client to instruct a server to transfer files to a third machine. This third-party mechanism, known as proxy FTP, causes a well known security problem. The FTP specification also allows an unlimited number of attempts at entering a user's password. This allows brute force "password guessing" attacks. This document provides suggestions for system administrators and those implementing FTP servers that will decrease the security problems associated with FTP.

6.1.116 RFC 2585: *Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP*

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. Additional mechanisms addressing PKIX operational requirements are specified in separate documents.

6.1.117 RFC 2587: *Internet X.509 Public Key Infrastructure LDAPv2 Schema*

The schema defined in this document is a minimal schema to support PKIX in an LDAPv2 environment, as defined in RFC 2559. Only PKIX- specific components are specified here. LDAP

servers, acting as PKIX repositories should support the auxiliary object classes defined in this specification and integrate this schema specification with the generic and other application-specific schemas as appropriate, depending on the services to be supplied by that server.

6.1.118 RFC 2588: *IP Multicast and Firewalls*
Many organizations use a firewall computer that acts as a security gateway between the public Internet and their private, internal 'intranet'. In this document, we discuss the issues surrounding the traversal of IP multicast traffic across a firewall, and describe possible ways in which a firewall can implement and control this traversal. We also explain why some firewall mechanisms - such as SOCKS - that were designed specifically for unicast traffic, are less appropriate for multicast.

6.1.119 RFC 2595: *Using TLS with IMAP, POP3 and ACAP*
This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. The TLS protocol (formerly known as SSL) provides a way to secure an application protocol from tampering and eavesdropping. The option of using such security is desirable for IMAP, POP and ACAP due to common connection eavesdropping and hijacking attacks [AUTH].

6.1.120 RFC 2612: *The CAST-256 Encryption Algorithm*
There is always a desire in the Internet community for unencumbered encryption algorithms with a range of key sizes that can provide security for a variety of cryptographic applications and protocols. This document describes an existing algorithm that can be used to satisfy this requirement. Included are a description of the cipher and the key scheduling algorithm, the s-boxes, and a set of test vectors

6.1.121 RFC 2617: *HTTP Authentication: Basic and Digest Access Authentication*
"HTTP/1.0", includes the specification for a Basic Access Authentication scheme. This scheme is not considered to be a secure method of user authentication (unless used in conjunction with some external secure system such as SSL [5]), as the user name and password are passed over the network as cleartext. This document also provides the specification for HTTP's authentication framework, the original Basic authentication scheme and a scheme based on cryptographic hashes, referred to as "Digest Access Authentication". It is therefore also intended to serve as a replacement for RFC 2069 [6].

6.1.122 RFC 2618: *RADIUS Authentication Client MIB*
This memo defines a set of extensions which instrument RADIUS authentication client functions. These extensions represent a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. Using these extensions IP-based management stations can manage RADIUS authentication clients.

6.1.123 RFC 2619: *RADIUS Authentication Server MIB*
This memo defines a set of extensions which instrument RADIUS authentication server functions. These extensions represent a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. Using these extensions IP-based management stations can manage RADIUS authentication servers.

6.1.124 RFC 2620: *RADIUS Accounting Client MIB*
This memo defines a set of extensions which instrument RADIUS accounting client functions. These extensions represent a portion of the Management Information Base (MIB) for use with

network management protocols in the Internet community. Using these extensions IP-based management stations can manage RADIUS accounting clients.

6.1.125 RFC 2621: *RADIUS Accounting Server MIB*
This memo defines a set of extensions which instrument RADIUS accounting server functions. These extensions represent a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. Using these extensions IP-based management stations can manage RADIUS accounting servers.

6.1.126 RFC 2623: *NFS Version 2 and Version 3 Security Issues and the NFS Protocol's Use of RPCSEC_GSS and Kerberos V5*
This memorandum clarifies various security issues involving the NFS protocol (Version 2 and Version 3 only) and then describes how the Version 2 and Version 3 of the NFS protocol use the RPCSEC_GSS security flavor protocol and Kerberos V5. This memorandum is provided so that people can write compatible implementations.

6.1.127 RFC 2627: *Key Management for Multicast: Issues and Architectures*
This report contains a discussion of the difficult problem of key management for multicast communication sessions. It focuses on two main areas of concern with respect to key management, which are, initializing the multicast group with a common net key and rekeying the multicast group. A rekey may be necessary upon the compromise of a user or for other reasons (e.g., periodic rekey). In particular, this report identifies a technique which allows for secure compromise recovery, while also being robust against collusion of excluded users. This is one important feature of multicast key management which has not been addressed in detail by most other multicast key management proposals [1,2,4]. The benefits of this proposed technique are that it minimizes the number of transmissions required to rekey the multicast group and it imposes minimal storage requirements on the multicast group.

6.1.128 RFC 2628: *Simple Cryptographic Program Interface (Crypto API)*
This document describes a simple Application Program Interface to cryptographic functions. The main purpose of such an interface is to separate cryptographic libraries from internet applications, thus allowing an independent development of both. It can be used in various internet applications such as [IPsec], [ISAKMP], [IKE], [TLS].

6.1.129 RFC 2630: *Cryptographic Message Syntax*
This document describes the Cryptographic Message Syntax. This syntax is used to digitally sign, digest, authenticate, or encrypt arbitrary messages. The Cryptographic Message Syntax is derived from PKCS #7 version 1.5 as specified in RFC 2315 [PKCS#7]. Wherever possible, backward compatibility is preserved; however, changes were necessary to accommodate attribute certificate transfer and key agreement techniques for key management.

6.1.130 RFC 2631: *Diffie-Hellman Key Agreement Method*
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.

6.1.131 RFC 2632: *S/MIME Version 3 Certificate Handling*
S/MIME (Secure/Multipurpose Internet Mail Extensions), described in [SMIME-MSG], provides a method to send and receive secure MIME messages. Before using a public key to provide security services, the S/MIME agent MUST certify that the public key is valid. S/MIME agents MUST use PKIX certificates to validate public keys as described in the Internet X.509 Public Key Infrastructure (PKIX) Certificate and CRL Profile [KEYM]. S/MIME agents MUST meet the certificate processing requirements documented in this document in addition to those stated in [KEYM]. This specification is compatible with the Cryptographic Message Syntax [CMS] in that it uses the data types defined by CMS. It also inherits all the varieties of architectures for certificate-based key management supported by CMS.

6.1.132 RFC 2633: *S/MIME Version 3 Message Specification*
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).

6.1.133 RFC 2634: *Enhanced Security Services for S/MIME*
This document describes four optional security service extensions for S/MIME. The services are: - signed receipts - security labels - secure mailing lists - signing certificates The first three of these services provide functionality that is similar to the Message Security Protocol [MSP4], but are useful in many other environments, particularly business and finance. Signing certificates are useful in any environment where certificates might be transmitted with signed messages. The services described here are extensions to S/MIME version 3 ([MSG] and [CERT]), and some of them can also be added to S/MIME version 2 [SMIME2]. The extensions described here will not cause an S/MIME version 3 recipient to be unable to read messages from an S/MIME version 2 sender. However, some of the extensions will cause messages created by an S/MIME version 3 sender to be unreadable by an S/MIME version 2 recipient. This document describes both the procedures and the attributes needed for the four services. Note that some of the attributes described in this document are quite useful in other contexts and should be considered when extending S/MIME or other CMS applications.

6.1.134 RFC 2637: *Point-to-Point Tunneling Protocol*
This document specifies a protocol which allows the Point to Point Protocol (PPP) to be tunneled through an IP network. PPTP does not specify any changes to the PPP protocol but rather describes a new vehicle for carrying PPP. A client-server architecture is defined in order to decouple functions which exist in current Network Access Servers (NAS) and support Virtual Private Networks (VPNs). The PPTP Network Server (PNS) is envisioned to run on a general purpose operating system while the client, referred to as a PPTP Access Concentrator (PAC) operates on a dial access platform. PPTP specifies a call-control and management protocol which allows the server to control access for dial-in circuit switched calls originating from a PSTN or ISDN or to initiate outbound circuit-

6.1.35 RFC 2642: *Cabletron's VLS Protocol Specification*
The Virtual LAN Link State Protocol (VLSP) is part of the InterSwitch Message Protocol (ISMP) which provides interswitch communication between switches running Cabletron's SecureFast VLAN (SFVLAN) product. VLSP is used to determine and maintain a fully connected mesh topology graph of the switch fabric. Each switch maintains an identical database describing the topology. Call-originating switches use the topology database to determine the path over which to

route a call connection. VLSP provides support for equal-cost multipath routing, and recalculates routes quickly in the face of topological changes, utilizing a minimum of routing protocol traffic.

6.1.136 RFC 2643: *Cabletron's SecureFast VLAN Operational Model*
Cabletron's SecureFast VLAN (SFVLAN) product implements a distributed connection-oriented switching protocol that provides fast forwarding of data packets at the MAC layer. The product uses the concept of virtual LANs (VLANs) to determine the validity of call connection requests and to scope the broadcast of certain flooded messages.

6.1.137 RFC 2647: *Benchmarking Terminology for Firewall Performance*
This document defines terms used in measuring the performance of firewalls. It extends the terminology already used for benchmarking routers and switches with definitions specific to firewalls. Forwarding rate and connection-oriented measurements are the primary metrics used in this document.

6.1.138 RFC 2659: *Security Extensions For HTML*
This memo describes a syntax for embedding S-HTTP negotiation parameters in HTML documents. S-HTTP, as described by RFC 2660, contains the concept of negotiation headers which reflect the potential receiver of a message's preferences as to which crypto- graphic enhancements should be applied to the message. This document describes a syntax for binding these negotiation parameters to HTML anchors.

6.1.139 RFC 2660: *The Secure HyperText Transfer Protocol*
This memo describes a syntax for securing messages sent using the Hypertext Transfer Protocol (HTTP), which forms the basis for the World Wide Web. Secure HTTP (S-HTTP) provides independently applicable security services for transaction confidentiality, authenticity/integrity and non-repudiability of origin. The protocol emphasizes maximum flexibility in choice of key management mechanisms, security policies and cryptographic algorithms by supporting option negotiation between parties for each transaction.

6.1.140 RFC 2661: *Layer Two Tunneling Protocol "L2TP"*
This document describes the Layer Two Tunneling Protocol (L2TP). STD 51, RFC 1661 specifies multi-protocol access via PPP [RFC1661]. L2TP facilitates the tunneling of PPP packets across an intervening network in a way that is as transparent as possible to both end-users and applications.

6.1.141 RFC 2667: *IP Tunnel MIB*
This memo defines a Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects used for managing tunnels of any type over IPv4 networks. Extension MIBs may be designed for managing protocol-specific objects. Likewise, extension MIBs may be designed for managing security-specific objects. This MIB does not support tunnels over non-IPv4 networks (including IPv6 networks). Management of such tunnels may be supported by other MIBs.

6.1.142 RFC 2685: *Virtual Private Networks Identifier*
Virtual Private IP networks may span multiple Autonomous Systems or Service Providers. There is a requirement for the use of a globally unique VPN identifier in order to be able to refer to a particular VPN (see section 6.1.1 of [1]). This document proposes a format for a globally unique VPN identifier.

6.1.143 RFC 2692: *SPKI Requirements*
The IETF Simple Public Key Infrastructure [SPKI] Working Group is tasked with producing a certificate structure and operating procedure to meet the needs of the Internet community for trust management in as easy, simple and extensible a way as possible. The SPKI Working Group first established a list of things one might want to do with certificates (attached at the end of this document), and then summarized that list of desires into requirements. This document presents that summary of requirements.

6.1.144 RFC 2693: *SPKI Certificate Theory*
The SPKI Working Group has developed a standard form for digital certificates whose main purpose is authorization rather than authentication. These structures bind either names or explicit authorizations to keys or other objects. The binding to a key can be directly to an explicit key, or indirectly through the hash of the key or a name for it. The name and authorization structures can be used separately or together. We use S-expressions as the standard format for these certificates and define a canonical form for those S-expressions. As part of this development, a mechanism for deriving authorization decisions from a mixture of certificate types was developed and is presented in this document. This document gives the theory behind SPKI certificates and ACLs without going into technical detail about those structures or their uses.

6.1.145 RFC 2695: *Authentication Mechanisms for ONC RPC*
This document describes two authentication mechanisms created by Sun Microsystems that are commonly used in conjunction with the ONC Remote Procedure Call (ONC RPC Version 2) protocol. WARNING The DH authentication as defined in Section 2 in this document refers to the authentication mechanism with flavor AUTH_DH currently implemented in ONC RPC. It uses the underlying Diffie-Hellman algorithm for key exchange. The DH authentication defined in this document is flawed due to the selection of a small prime for the BASE field (Section 2.5). To avoid the flaw a new DH authentication mechanism could be defined with a larger prime. However, the new DH authentication would not be interoperable with the existing DH authentication.

6.1.146 RFC 2704: *The KeyNote Trust-Management System Version 2*
This memo describes version 2 of the KeyNote trust-management system. It specifies the syntax and semantics of KeyNote `assertions', describes `action attribute' processing, and outlines the application architecture into which a KeyNote implementation can be fit. The KeyNote architecture and language are useful as building blocks for the trust management aspects of a variety of Internet protocols and services.

6.1.147 RFC 2709: *Security Model with Tunnel-mode IPsec for NAT Domains*
There are a variety of NAT flavors, as described in [Ref 1]. Of the domains supported by NATs, only Realm-Specific IP clients are able to pursue end-to-end IPsec secure sessions. However, all flavors of NAT are capable of offering tunnel-mode IPsec security to private domain hosts peering with nodes in external realm. This document describes a security model by which tunnel-mode IPsec security can be architected on NAT devices. A section is devoted to describing how security policies may be transparently communicated to IKE (for automated KEY exchange) during Quick Mode. Also outlined are applications that can benefit from the Security Model described.

6.1.48 RFC 2712: *Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)*
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. 1. Abstract This document proposes the addition of new cipher suites to the TLS protocol [1] to support Kerberos-based authentication. Kerberos credentials are used to achieve mutual authentication and to establish a master secret which is subsequently used to secure client-server communication.

6.1.149 RFC 2716: *PPP EAP TLS Authentication Protocol*

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP also defines an extensible Link Control Protocol (LCP), which can be used to negotiate authentication methods, as well as an Encryption Control Protocol (ECP), used to negotiate data encryption over PPP links, and a Compression Control Protocol (CCP), used to negotiate compression methods. The Extensible Authentication Protocol (EAP) is a PPP extension that provides support for additional authentication methods within PPP. Transport Level Security (TLS) provides for mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. This document describes how EAP-TLS, which includes support for fragmentation and reassembly, provides for these TLS mechanisms within EAP.

6.1.150 RFC 2725: *Routing Policy System Security*

The RIPE database specifications and RPSL language define languages used as the basis for representing information in a routing policy system. A repository for routing policy system information is known as a routing registry. A routing registry provides a means of exchanging information needed to address many issues of importance to the operation of the Internet. The implementation and deployment of a routing policy system must maintain some degree of integrity to be of any operational use. This document addresses the need to assure integrity of the data by providing an authentication and authorization model.

6.1.151 RFC 2726: *PGP Authentication for RIPE Database Updates*

This document presents the proposal for a stronger authentication method of the updates of the RIPE database based on digital signatures. The proposal tries to be as general as possible as far as digital signing methods are concerned, however, it concentrates mainly on PGP, as the first method to be implemented. The proposal is the result of the discussions within the RIPE DBSEC Task Force.

6.1.152 RFC 2735: *NHRP Support for Virtual Private Networks*

The Generic Security Service Application Program Interface (GSS-API), Version 2, as defined in [RFC-2078], provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments. This specification defines GSS-API services and primitives at a level independent of underlying mechanism and programming language environment, and is to be complemented by other, related specifications: documents defining specific parameter bindings for particular language environments documents defining token formats, protocols, and procedures to be implemented in order to realize GSS-API services atop particular security mechanisms This memo obsoletes [RFC-2078], making specific, incremental changes in response to implementation experience and liaison requests. It is intended, therefore, that this memo or a successor version thereto will become the basis for subsequent progression of the GSS-API specification on the standards track.

6.1.153 RFC 2743: *Generic Security Service Application Program Interface Version 2, Update 1*
The Generic Security Service Application Program Interface (GSS-API), Version 2, as defined in [RFC-2078, but see RFC 2735], provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments. This specification defines GSS-API services and primitives at a level independent of underlying mechanism and programming language environment, and is to be complemented by other, related specifications: documents defining specific parameter bindings for particular language environments documents defining token formats, protocols, and procedures to be implemented in order to realize GSS-API services atop particular security mechanisms This memo obsoletes [RFC-2078], making specific, incremental changes in response to implementation experience and liaison requests. It is intended, therefore, that this memo or a successor version thereto will become the basis for subsequent progression of the GSS-API specification on the standards track.

6.1.154 RFC 2744: *Generic Security Service API Version 2 : C-bindings*
This document specifies C language bindings for Version 2, Update 1 of the Generic Security Service Application Program Interface (GSS- API), which is described at a language-independent conceptual level in RFC-2743 [GSSAPI]. It obsoletes RFC-1509, making specific incremental changes in response to implementation experience and liaison requests. It is intended, therefore, that this memo or a successor version thereof will become the basis for subsequent progression of the GSS-API specification on the standards track. The Generic Security Service Application Programming Interface provides security services to its callers, and is intended for implementation atop a variety of underlying cryptographic mechanisms. Typically, GSS-API callers will be application protocols into which security enhancements are integrated through invocation of services provided by the GSS-API. The GSS-API allows a caller application to authenticate a principal identity associated with a peer application, to delegate rights to a peer, and to apply security services such as confidentiality and integrity on a per-message basis.

6.1.155 RFC 2746: *RSVP Operation Over IP Tunnels*
This document describes an approach for providing RSVP protocol services over IP tunnels. We briefly describe the problem, the characteristics of possible solutions, and the design goals of our approach. We then present the details of an implementation which meets our design goals. IP-in-IP "tunnels" have become a widespread mechanism to transport datagrams in the Internet. Typically, a tunnel is used to route packets through portions of the network which do not directly implement the desired service (e.g. IPv6), or to augment and modify the behavior of the deployed routing architecture (e.g. multicast routing, mobile IP, Virtual Private Net).

6.1.156 RFC 2747: *RSVP Cryptographic Authentication*
This document describes the format and use of RSVP's INTEGRITY object to provide hop-by-hop integrity and authentication of RSVP messages. The Resource ReSerVation Protocol RSVP [1] is a protocol for setting up distributed state in routers and hosts, and in particular for reserving resources to implement integrated service. RSVP allows particular users to obtain preferential access to network resources, under the control of an admission control mechanism. Permission to make a reservation will depend both upon the availability of the requested resources along the path of the data, and upon satisfaction of policy rules.

6.1.157 RFC 2749: *COPS usage for RSVP*
The Common Open Policy Service (COPS) protocol is a query response protocol used to exchange policy information between a network policy server and a set of clients [COPS]. COPS is being developed within the RSVP Admission Policy Working Group (RAP WG) of the IETF,

primarily for use as a mechanism for providing policy-based admission control over requests for network resources [RAP]. This document is based on and assumes prior knowledge of the RAP framework [RAP] and the basic COPS [COPS] protocol. It provides specific usage directives for using COPS in outsourcing policy control decisions by RSVP clients (PEPs) to policy servers (PDPs).

6.1.158 RFC 2750: *RSVP Extensions for Policy Control*

This memo presents a set of extensions for supporting generic policy based admission control in RSVP. It should be perceived as an extension to the RSVP functional specifications [RSVP] These extensions include the standard format of POLICY_DATA objects, and a description of RSVP's handling of policy events. This document does not advocate particular policy control mechanisms; however, a Router/Server Policy Protocol description for these extensions can be found in [RAP, COPS, COPS-RSVP].

6.1.159 RFC 2752: *Identity Representation for RSVP*

This document describes the representation of identity information in POLICY_DATA object [POL-EXT] for supporting policy based admission control in RSVP. The goal of identity representation is to allow a process on a system to securely identify the owner and the application of the communicating process (e.g. user id) and convey this information in RSVP messages (PATH or RESV) in a secure manner. We describe the encoding of identities as RSVP policy element. We describe the processing rules to generate identity policy elements for multicast merged flows. Subsequently, we describe representations of user identities for Kerberos and Public Key based user authentication mechanisms. In summary we describe the use of this identity information in an operational setting.

6.1.160 RFC 2755: *Security Negotiation for WebNFS*

This document describes a protocol for a WebNFS client [RFC2054] to negotiate the desired security mechanism with a WebNFS server [RFC2055] before the WebNFS client falls back to the MOUNT v3 protocol [RFC1813]. This document is provided so that people can write compatible implementations.

6.1.161 RFC 2764: *A Framework for IP Based Virtual Private Net*

This document defines a method to encrypt a file transfer using the FTP specification STD 9, RFC 959, "File Transfer Protocol (FTP)", (October 1985) [3] and RFC 2228, "FTP Security Extensions" (October 1997) [1]. This method will use the Key Exchange Algorithm (KEA) to give mutual authentication and establish the data encryption keys. SKIPJACK is used to encrypt file data and the FTP command channel.

6.1.162 RFC 2773: *Encryption using KEA and SKIPJACK*

This document defines a method to encrypt a file transfer using the FTP specification STD 9, RFC 959, "File Transfer Protocol (FTP)", (October 1985) [3] and RFC 2228, "FTP Security Extensions" (October 1997) [1]. This method will use the Key Exchange Algorithm (KEA) to give mutual authentication and establish the data encryption keys. SKIPJACK is used to encrypt file data and the FTP command channel.

6.1.163 RFC 2786: *Diffie-Helman USM Key Management Information Base and Textual Convention*

This memo defines an experimental portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines a textual convention for doing Diffie-Helman key agreement key exchanges and a set of objects which

extend the usmUserTable to permit the use of a DH key exchange in addition to the key change method described in [12]. In otherwords, this MIB adds the possibility of forward secrecy to the USM model. It also defines a set of objects that can be used to kick start security on an SNMPv3 agent when the out of band path is authenticated, but not necessarily private or confidential. The KeyChange textual convention described in [12] permits secure key changes, but has the property that if a third-party has knowledge of the original key (e.g. if the agent was manufactured with a standard default key) and could capture all SNMP exchanges, the third-party would know the new key. The Diffie-Helman key change described here

6.1.164 RFC 2792: *DSA and RSA Key and Signature Encoding for the KeyNote Trust Management System*

This memo describes RSA and DSA key and signature encoding, and binary key encoding for version 2 of the KeyNote trust-management system. 1. Introduction KeyNote is a simple and flexible trust-management system designed to work well for a variety of large- and small-scale Internet-based applications. It provides a single, unified language for both local policies and credentials. KeyNote policies and credentials, called `assertions', contain predicates that describe the trusted actions permitted by the holders of specific public keys. KeyNote assertions are essentially small, highly-structured programs. A signed assertion, which can be sent over an untrusted network, is also called a `credential assertion'. Credential assertions, which also serve the role of certificates, have the same syntax as policy assertions but are also signed by the principal delegating the trust. For more details on KeyNote, see [BFIK99]. This document assumes reader familiarity with the KeyNote system.

6.1.165 RFC 2797: *Certificate Management Messages over CMS*

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. A small number of additional services are defined to supplement the core certificate request service. Throughout this specification the term CMS is used to refer to both [CMS] and [PKCS7]. For both signedData and envelopedData, CMS is a superset of the PKCS7. In general, the use of PKCS7 in this document is aligned to the Cryptographic Message Syntax [CMS] that provides a superset of the PKCS7 syntax. The term CMC refers to this specification.

6.1.166 RFC 2802: *Digital Signatures for the v1.0 Internet Open Trading Protocol (IOTP)*

A syntax and procedures are described for the computation and verification of digital signatures for use within Version 1.0 of the Internet Open Trading Protocol (IOTP).

6.1.167 RFC 2807: *XML Signature Requirements*

This document lists the design principles, scope, and requirements for the XML Digital Signature specification. It includes requirements as they relate to the signature syntax, data model, format, cryptographic processing, and external requirements and coordination.

6.1.168 RFC 2808: *The SecurID(r) SASL Mechanism*

SecurID is a hardware token card product (or software emulation thereof) produced by RSA Security Inc., which is used for end-user authentication. This document defines a SASL [RFC2222] authentication mechanism using these tokens, thereby providing a means for such tokens to be used in SASL environments. This mechanism is only for authentication, and has no effect on the protocol encoding and is not designed to provide integrity or confidentiality

services. This memo assumes the reader has basic familiarity with the SecurID token, its associated authentication protocol and SASL.

6.1.169 RFC 2809: *Implementation of L2TP Compulsory Tunneling via RADIUS*
This document discusses implementation issues arising in the provisioning of compulsory tunneling in dial-up networks using the L2TP protocol. This provisioning can be accomplished via the integration of RADIUS and tunneling protocols. Implementation issues encountered with other tunneling protocols are left to separate documents.

6.1.170 RFC 2817: *Upgrading to TLS Within HTTP/1.1*
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. Since HTTP/1.1 [1] defines Upgrade as a hop-by-hop mechanism, this memo also documents the HTTP CONNECT method for establishing end-to-end tunnels across HTTP proxies. Finally, this memo establishes new IANA registries for public HTTP status codes, as well as public or private Upgrade product tokens.

6.1.171 RFC 2818: *HTTP Over TLS*
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. A companion document describes a method for using HTTP/TLS over the same port as normal HTTP [RFC2817].

6.1.172 RFC 2820: *Access Control Requirements for LDAP*
This document describes the fundamental requirements of an access control list (ACL) model for the Lightweight Directory Application Protocol (LDAP) directory service. It is intended to be a gathering place for access control requirements needed to provide authorized access to and interoperability between directories.

6.1.173 RFC 2827: *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*
Recent occurrences of various Denial of Service (DoS) attacks which have employed forged source addresses have proven to be a troublesome issue for Internet Service Providers and the Internet community overall. This paper discusses a simple, effective, and straightforward method for using ingress traffic filtering to prohibit DoS attacks which use forged IP addresses to be propagated from 'behind' an Internet Service Provider's (ISP) aggregation point.

6.1.174 RFC 2828: *Internet Security Glossary*
This Glossary (191 pages of definitions and 13 pages of references) provides abbreviations, explanations, and recommendations for use of information system security terminology. The intent is to improve the comprehensibility of writing that deals with Internet security, particularly Internet Standards documents (ISDs). To avoid confusion, ISDs should use the same term or definition whenever the same concept is mentioned. To improve international understanding, ISDs should use terms in their plainest, dictionary sense. ISDs should use terms established in standards documents and other well-founded publications and should avoid substituting private or newly made-up terms. ISDs should avoid terms that are proprietary or otherwise favor a particular

vendor, or that create a bias toward a particular security technology or mechanism versus other, competing techniques that already exist or might be developed in the future.

6.1.175 RFC 2829: *Authentication Methods for LDAP*
This document specifies particular combinations of security mechanisms which are required and recommended in LDAP [1] implementations.

6.1.176 RFC 2830: *Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security*
This document defines the "Start Transport Layer Security (TLS) Operation" for LDAP [LDAPv3, TLS]. This operation provides for TLS establishment in an LDAP association and is defined in terms of an LDAP extended request.

6.1.177 RFC 2831: *Using Digest Authentication as a SASL Mechanism*
This specification defines how HTTP Digest Authentication [Digest] can be used as a SASL [RFC 2222] mechanism for any protocol that has a SASL profile. It is intended both as an improvement over CRAM-MD5 [RFC 2195] and as a convenient way to support a single authentication mechanism for web, mail, LDAP, and other protocols.

6.1.178 RFC 2845: *Secret Key Transaction Authentication for DNS (TSIG)*
This protocol allows for transaction level authentication using shared secrets and one way hashing. It can be used to authenticate dynamic updates as coming from an approved client, or to authenticate responses as coming from an approved recursive name server. No provision has been made here for distributing the shared secrets; it is expected that a network administrator will statically configure name servers and clients using some out of band mechanism such as sneaker-net until a secure automated mechanism for key distribution is available.

6.1.179 RFC 2847: *LIPKEY - A Low Infrastructure Public Key Mechanism Using SPKM*
This memorandum describes a method whereby one can use GSS-API [RFC2078] to supply a secure channel between a client and server, authenticating the client with a password, and a server with a public key certificate. As such, it is analogous to the common low infrastructure usage of the Transport Layer Security (TLS) protocol [RFC2246]. The method leverages the existing Simple Public Key Mechanism (SPKM) [RFC2025], and is specified as a separate GSS-API mechanism (LIPKEY) layered above SPKM.

6.1.180 RFC 2853: *Generic Security Service API Version 2*
The Generic Security Services Application Program Interface (GSS-API) offers application programmers uniform access to security services atop a variety of underlying cryptographic mechanisms. This document specifies the Java bindings for GSS-API which is described at a language independent conceptual level in RFC 2743 [GSSAPIv2-UPDATE]. The GSS-API allows a caller application to authenticate a principal identity, to delegate rights to a peer, and to apply security services such as confidentiality and integrity on a per-message basis. Examples of security mechanisms defined for GSS-API are The Simple Public-Key GSS-API Mechanism [SPKM] and The Kerberos Version 5 GSS-API Mechanism [KERBV5].

6.1.181 RFC 2865: *Remote Authentication Dial In User Service (RADIUS)*
This memo specifies new textual conventions for additional high capacity data types, intended for SNMP implementations which already support the Counter64 data type. The definitions contained in this document represent a short term solution which may be deprecated in the future.

6.1.182 RFC 2866: *RADIUS Accounting*
This document describes a protocol for carrying accounting information between a Network Access Server and a shared Accounting Server. This memo documents the RADIUS Accounting protocol. The early deployment of RADIUS Accounting was done using UDP port number 1646, which conflicts with the "sa-msg-port" service. The officially assigned port number for RADIUS Accounting is 1813.

6.1.183 RFC 2867: *RADIUS Accounting Modifications for Tunnel Protocol Support*
This document defines new RADIUS accounting Attributes and new values for the existing Acct-Status-Type Attribute [1] designed to support the provision of compulsory tunnelling in dial-up networks. Specification of Requirements. Many applications of tunnelling protocols such as PPTP [5] and L2TP [4] involve dial-up network access. Some, such as the provision of secure access to corporate intranets via the Internet, are characterized by voluntary tunnelling: the tunnel is created at the request of the user for a specific purpose. Other applications involve compulsory tunnelling: the tunnel is created without any action from the user and without allowing the user any choice in the matter, as a service of the Internet service provider (ISP).

6.1.184 RFC 2868: *RADIUS Attributes for Tunnel Protocol Support*
This document defines a set of RADIUS attributes designed to support the provision of compulsory tunnelling in dial-up networks. Many applications of tunnelling protocols such as L2TP involve dial-up network access. Some, such as the provision of access to corporate intranets via the Internet, are characterized by voluntary tunnelling: the tunnel is created at the request of the user for a specific purpose. Other applications involve compulsory tunnelling: the tunnel is created without any action from the user and without allowing the user any choice in the matter. In order to provide this functionality, new RADIUS attributes are needed to carry the tunnelling information from the RADIUS server to the tunnel end points; this document defines those attributes.

6.1.185 RFC 2869: *RADIUS Extensions*
This document describes additional attributes for carrying authentication, authorization and accounting information between a Network Access Server (NAS) and a shared Accounting Server using the Remote Authentication Dial In User Service (RADIUS) protocol described in RFC 2865 [1] and RFC 2866 [2].

6.1.186 RFC 2875: *Diffie-Hellman Proof-of-Possession Algorithms*
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.

6.1.187 RFC 2876: *Use of the KEA and SKIPJACK Algorithms in CMS*
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.

6.1.188 RFC 2888: *Secure Remote Access with L2TP*
This document is intended to provide methodology for the benchmarking of local area network (LAN) switching devices. It extends the methodology already defined for benchmarking network interconnecting devices in RFC 2544 [3] to switching devices. This RFC primarily deals with devices which switch frames at the Medium Access Control (MAC) layer. It provides a

methodology for benchmarking switching devices, forwarding performance, congestion control, latency, address handling and filtering. In addition to defining the tests, this document also describes specific formats for reporting the results of the tests.

6.1.189 RFC 2898 PKCS #5: *Password-Based Cryptography Specification Version 2.0*
This memo represents a republication of PKCS #5 v2.0 from RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, and change control is retained within the PKCS process. The body of this document, except for the security considerations section, is taken directly from that specification. This document provides recommendations for the implementation of password-based cryptography, covering key derivation functions, encryption schemes, message-authentication schemes, and ASN.1 syntax identifying the techniques. The recommendations are intended for general application within computer and communications systems, and as such include a fair amount of flexibility. They are particularly intended for the protection of sensitive information such as private keys, as in PKCS #8 [25]. It is expected that application standards and implementation profiles based on these specifications may include additional constraints.

6.1.190 RFC 2917: *A Core MPLS IP VPN Architecture*
This memo presents an approach for building core Virtual Private Network (VPN) services in a service provider's MPLS backbone. This approach uses Multiprotocol Label Switching (MPLS) running in the backbone to provide premium services in addition to best effort services. The central vision is for the service provider to provide a virtual router service to their customers. The keystones of this architecture are ease of configuration, user security, network security, dynamic neighbor discovery, scaling and the use of existing routing protocols as they exist today without any modifications.

6.1.191 RFC 2930: *Secret Key Establishment for DNS (TKEY RR)*
[RFC 2845] provides a means of authenticating Domain Name System (DNS) queries and responses using shared secret keys via the Transaction Signature (TSIG) resource record (RR). However, it provides no mechanism for setting up such keys other than manual exchange. This document describes a Transaction Key (TKEY) RR that can be used in a number of different modes to establish shared secret keys between a DNS resolver and server.

6.1.192 RFC 2941: *Telnet Authentication Option*
This document describes the authentication option to the telnet protocol as a generic method for negotiating an authentication type and mode including whether encryption should be used and if credentials should be forwarded. While this document summarizes currently utilized commands and types it does not define a specific authentication type. Separate documents are to be published defining each authentication type. This document updates a previous specification of the telnet authentication option, RFC 1416, so that it can be used to securely enable the telnet encryption option.

6.1.193 RFC 2942: *Telnet Authentication: Kerberos Version 5*
This document describes how Kerberos Version 5 [1] is used with the telnet protocol. It describes an telnet authentication suboption to be used with the telnet authentication option [2]. This mechanism can also used to provide keying material to provide data confidentiality services in conjunction with the telnet encryption option [3].

6.1.194 RFC 2943: *TELNET Authentication Using DSA*
This document defines a telnet authentication mechanism using the Digital Signature Algorithm (DSA) [FIPS186]. It relies on the Telnet Authentication Option [RFC2941].

6.1.195 RFC 2944: *Telnet Authentication: SRP*
This document specifies an authentication scheme for the Telnet protocol under the framework described in [RFC2941], using the Secure Remote Password Protocol (SRP) authentication mechanism. The specific mechanism, SRP-SHA1, is described in [RFC2945].

6.1.196 RFC 2945: *The SRP Authentication and Key Exchange System*
This document describes a cryptographically strong network authentication mechanism known as the Secure Remote Password (SRP) protocol. This mechanism is suitable for negotiating secure connections using a user-supplied password, while eliminating the security problems traditionally associated with reusable passwords. This system also performs a secure key exchange in the process of authentication, allowing security layers (privacy and/or integrity protection) to be enabled during the session. Trusted key servers and certificate infrastructures are not required, and clients are not required to store or manage any long-term keys. SRP offers both security and deployment advantages over existing challenge-response techniques, making it an ideal drop-in replacement where secure password authentication is needed.

6.1.197 RFC 2946: *Telnet Data Encryption Option*
This document describes the telnet encryption option as a generic method of providing data confidentiality services for the telnet data stream. While this document summarizes currently utilized encryption types and codes, it does not define a specific encryption algorithm. Separate documents are to be published defining implementations of this option for each encryption algorithm.

6.1.198 RFC 2947: *Telnet Encryption: DES3 64 bit Cipher Feedback*
This document specifies how to use the Triple-DES (data encryption standard) encryption algorithm in cipher feedback mode with the telnet encryption option.

6.1.199 RFC 2948: *Telnet Encryption: DES3 64 bit Output Feedback*
This document specifies how to use the Triple-DES (data encryption standard) encryption algorithm in output feedback mode with the telnet encryption option.

6.1.200 RFC 2949: *Telnet Encryption: CAST-128 64 bit Output Feedback*
This document specifies how to use the CAST-128 encryption algorithm in output feedback mode with the telnet encryption option. Two key sizes are defined: 40 bit and 128 bit.

6.1.201 RFC 2950: *Telnet Encryption: CAST-128 64 bit Cipher Feedback*
This document specifies how to use the CAST-128 encryption algorithm in cipher feedback mode with the telnet encryption option. Two key sizes are defined: 40 bit and 128 bit.

6.1.202 RFC 2951: *TELNET Authentication Using KEA and SKIPJACK*
This document defines a method to authenticate TELNET using the Key Exchange Algorithm (KEA), and encryption of the TELNET stream using SKIPJACK. Two encryption modes are specified; one provides data integrity and the other does not. The method relies on the TELNET Authentication Option.

6.1.203 RFC 2952: *Telnet Encryption: DES 64 bit Cipher Feedback*
This document specifies how to use the DES encryption algorithm in cipher feedback mode with the telnet encryption option.

6.1.204 RFC 2953: *Telnet Encryption: DES 64 bit Output Feedback*
This document specifies how to use the data encryption standard (DES) encryption algorithm in output feedback mode with the telnet encryption option.

6.1.205 RFC 2977: *Mobile IP Authentication, Authorization, and Accounting Requirements*
The Mobile IP and Authentication, Authorization, Accounting (AAA) working groups are currently looking at defining the requirements for Authentication, Authorization, and Accounting. This document contains the requirements which would have to be supported by a AAA service to aid in providing Mobile IP services.

6.1.206 RFC 2979: *Behaviour of and Requirements for Internet Firewalls*
This memo defines behavioural characteristics of and interoperability requirements for Internet firewalls. While most of these things may seem obvious, current firewall behaviour is often either unspecified or under-specified and this lack of specificity often causes problems in practice. This requirement is intended to be a necessary first step in making the behaviour of firewalls more consistent across implementations and in line with accepted IP protocol practices.

6.1.207 RFC 2984: *Use of the CAST-128 Encryption Algorithm in CMS*
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

6.1.208 RFC 2994: *A Description of the MISTY1 Encryption Algorithm*
This document describes a secret-key cryptosystem MISTY1, which is block cipher with a 128-bit key, a 64-bit block and a variable number of rounds. It documents the algorithm description including key scheduling part and data randomizing part.

6.1.209 RFC 3007: *Secure Domain Name System (DNS) Dynamic Update*
This document proposes a method for performing secure Domain Name System (DNS) dynamic updates. The method described here is intended to be flexible and useful while requiring as few changes to the protocol as possible. The authentication of the dynamic update message is separate from later DNSSEC validation of the data. Secure communication based on authenticated requests and transactions is used to provide authorization.

6.1.210 RFC 3008: *Domain Name System Security (DNSSEC) Signing Authority*
This document proposes a revised model of Domain Name System Security (DNSSEC) Signing Authority. The revised model is designed to clarify earlier documents and add additional restrictions to simplify the secure resolution process. Specifically, this affects the authorization of keys to sign sets of records.

6.1.211 RFC 3013: *Recommended Internet Service Provider Security Services and Procedures*
The purpose of this document is to express what the engineering community as represented by the IETF expects of Internet Service Providers (ISPs) with respect to security. It is not the intent of this document to define a set of requirements that would be appropriate for all ISPs, but rather to raise awareness among ISPs of the community's expectations, and to provide the community with a framework for discussion of security expectations with current and prospective service providers.

6.1.212 RFC 3029: *Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols*

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. Useful Data Validation and Certification Server responsibilities in a PKI are to assert the validity of signed documents, public key certificates, and the possession or existence of data. Assertions created by this protocol are called Data Validation Certificates (DVC). We give examples of how to use the Data Validation and Certification Server to extend the lifetime of a signature beyond key expiry or revocation and to query the Data Validation and Certification Server regarding the status of a public key certificate. The document includes a complete example of a time stamping transaction.

6.1.213 RFC 3039: *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*

This document forms a certificate profile for Qualified Certificates, based on RFC 2459, for use in the Internet. The term Qualified Certificate is used to describe a certificate with a certain qualified status within applicable governing law. Further, Qualified Certificates are issued exclusively to physical persons. The goal of this document is to define a general syntax independent of local legal requirements. The profile is however designed to allow further profiling in order to meet specific local needs. It is important to note that the profile does not define any legal requirements for Qualified Certificates.

6.1.214 RFC 3053: *IPv6 Tunnel Broker*

The IPv6 global Internet as of today uses a lot of tunnels over the existing IPv4 infrastructure. Those tunnels are difficult to configure and maintain in a large scale environment. The 6bone has proven that large sites and Internet Service Providers (ISPs) can do it, but this process is too complex for the isolated end user who already has an IPv4 connection and would like to enter the IPv6 world. The motivation for the development of the tunnel broker model is to help early IPv6 adopters to hook up to an existing IPv6 network (e.g., the 6bone) and to get stable, permanent IPv6 addresses and DNS names. The concept of the tunnel broker was first presented at Orlando's IETF in December 1998. Two implementations were demonstrated during the Grenoble IPng & NGtrans interim meeting in February 1999.

6.1.215 RFC 3058: *Use of the IDEA Encryption Algorithm in CMS*

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.

6.1.216 RFC 3077: *A Link-Layer Tunneling Mechanism for Unidirectional Links*

This document describes a mechanism to emulate full bidirectional connectivity between all nodes that are directly connected by a unidirectional link. The "receiver" uses a link-layer tunneling mechanism to forward datagrams to "feeds" over a separate bidirectional IP (Internet Protocol) network. As it is implemented at the link-layer, protocols in addition to IP may also be supported by this mechanism.

6.1.217 RFC 3078: *Microsoft Point-To-Point Encryption (MPPE) Protocol*

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. The PPP Compression Control Protocol provides a method to

negotiate and utilize compression protocols over PPP encapsulated links. This document describes the use of the Microsoft Point to Point Encryption (MPPE) to enhance the confidentiality of PPP-encapsulated packets.

6.1.218 RFC 3090: *DNS Security Extension Clarification on Zone Status*
The definition of a secured zone is presented, clarifying and updating sections of RFC 2535. RFC 2535 defines a zone to be secured based on a per algorithm basis, e.g., a zone can be secured with RSA keys, and not secured with DSA keys. This document changes this to define a zone to be secured or not secured regardless of the key algorithm used (or not used). To further simplify the determination of a zone's status, "experimentally secure" status is deprecated.

6.1.219 RFC 3093: *Firewall Enhancement Protocol (FEP)*
Internet Transparency via the end-to-end architecture of the Internet has allowed vast innovation of new technologies and services [1]. However, recent developments in Firewall technology have altered this model and have been shown to inhibit innovation. We propose the Firewall enhancement Protocol (FEP) to allow innovation, without violating the security model of a Firewall. With no cooperation from a firewall operator, the FEP allows ANY application to traverse a Firewall. Our methodology is to layer any application layer Transmission Control Protocol/User Datagram Protocol (TCP/UDP) packets over the HyperText Transfer Protocol (HTTP) protocol, since HTTP packets are typically able to transit Firewalls. This scheme does not violate the actual security usefulness of a Firewall, since Firewalls are designed to thwart attacks from the outside and to ignore threats from within. The use of FEP is compatible with the current Firewall security model because it requires cooperation from a host inside the Firewall. FEP allows the best of both worlds: the security of a firewall, and transparent tunnelling thought the firewall.

6.1.220 RFC 3097: *RSVP Cryptographic Authentication -- Updated Message Type Value*
This memo resolves a duplication in the assignment of RSVP Message Types, by changing the Message Types assigned by RFC 2747 to Challenge and Integrity Response messages.

6.1.221 RFC 3110: *RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS***)**
This document describes how to produce RSA/SHA1 SIG resource records (RRs) in Section 3 and, so as to completely replace RFC 2537, describes how to produce RSA KEY RRs in Section 2. Since the adoption of a Proposed Standard for RSA signatures in the DNS (Domain Name Space), advances in hashing have been made. A new DNS signature algorithm is defined to make these advances available in SIG RRs. The use of the previously specified weaker mechanism is deprecated. The algorithm number of the RSA KEY RR is changed to correspond to this new SIG algorithm. No other changes are made to DNS security.

6.1.222 RFC 3112: *LDAP Authentication Password Schema*
his document describes schema in support of user/password authentication in a LDAP (Lightweight Directory Access Protocol) directory including the authPassword attribute type. This attribute type holds values derived from the user's password(s) (commonly using cryptographic strength one-way hash). authPassword is intended to used instead of userPassword.

6.1.223 RFC 3118: *Authentication for DHCP Messages*
This document defines a new Dynamic Host Configuration Protocol (DHCP) option through which authorization tickets can be easily generated and newly attached hosts with proper authorization can be automatically configured from an authenticated DHCP server. DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. In some

situations, network administrators may wish to constrain the allocation of addresses to authorized hosts. Additionally, some network administrators may wish to provide for authentication of the source and contents of DHCP messages.

6.1.224 RFC 3125: *Electronic Signature Policies*
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. To allow for the automatic processing of an electronic signature another part of the signature policy specifies the electronic rules for the creation and validation of the electronic signature in a computer processable form. In the current document the format of the signature policy is defined using ASN.1. The contents of this document is based on the signature policy defined in ETSI TS 101 733 V.1.2.2 (2000-12) Copyright (C). Individual copies of this ETSI deliverable can be downloaded from http://www.etsi.org.

6.1.225 RFC 3126: *Electronic Signature Formats for long term electronic signatures*
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). The format can be considered as an extension to RFC 2630 and RFC 2634, where, when appropriate additional signed and unsigned attributes have been defined. The contents of this Informational RFC is technically equivalent to ETSI TS 101 733 V.1.2.2. The ETSI TS is under the ETSI Copyright (C). Individual copies of this ETSI deliverable can be downloaded from http://www.etsi.org

6.1.226 RFC 3127: *Authentication, Authorization, and Accounting: Protocol Evaluation*
This memo represents the process and findings of the Authentication, Authorization, and Accounting Working Group (AAA WG) panel evaluating protocols proposed against the AAA Network Access Requirements, RFC 2989. Due to time constraints of this report, this document is not as fully polished as it might have been desired. But it remains mostly in this state to document the results as presented.

6.1.227 RFC 3128: *Protection Against a Variant of the Tiny Fragment Attack (RFC 1858*
This document discusses how RFC 1858 compliant filters can be vulnerable to a variant of the "Tiny Fragment Attack" described in section 3.1 of the RFC. This document describes the attack and recommends corrective action.

6.1.228 RFC 3129: *Requirements for Kerberized Internet Negotiation of Keys*
The goal of this document is to produce a streamlined, fast, easily managed, and cryptographically sound protocol without requiring public key.

6.1.229 RFC 3156: *MIME Security with OpenPGP*
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.

6.1.230 RFC 3157: *Securely Available Credentials - Requirements*
This document describes requirements to be placed on Securely Available Credentials (SACRED) protocols. "Credentials" are information that can be used to establish the identity of an entity, or help that entity communicate securely. Credentials include such things as private

keys, trusted roots, tickets, or the private part of a Personal Security Environment (PSE) [RFC2510] - that is, information used in secure communication on the Internet. Credentials are used to support various Internet protocols, e.g., S/MIME, IPSec and TLS.

6.1.231 RFC 3161: *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*
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.

6.1.232 RFC 3162: *RADIUS and IPv6*
This document specifies the operation of RADIUS (Remote Authentication Dial In User Service) when run over IPv6 as well as the RADIUS attributes used to support IPv6 network access.

6.1.232 RFC 3163: *ISO/IEC 9798-3 Authentication SASL Mechanism*
This document defines a SASL (Simple Authentication and Security Layer) authentication mechanism based on ISO/IEC 9798-3 and FIPS PUB 196 entity authentication.

6.1.233 RFC 3174: *US Secure Hash Algorithm 1 (SHA1)*
The purpose of this document is to make the SHA-1 (Secure Hash Algorithm 1) hash algorithm conveniently available to the Internet community. The United States of America has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard. Most of the text herein was taken by the authors from FIPS 180-1. Only the C code implementation is "original".

6.1.234 RFC 3183: *Domain Security Services using S/MIME*
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'.

6.1.235 RFC 3185; *Reuse of CMS Content Encryption Keys*
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.

6.1.236 RFC 3193: *Securing L2TP using IPsec*
This document discusses how L2TP (Layer Two Tunnelling Protocol) may utilize IPsec to provide for tunnel authentication, privacy protection, integrity checking and replay protection. Both the voluntary and compulsory tunnelling cases are discussed.

6.1.237 RFC 3207: *SMTP Service Extension for Secure SMTP over Transport Layer Security*
This document describes an extension to the SMTP (Simple Mail Transfer Protocol) service that allows an SMTP server and client to use TLS (Transport Layer Security) to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers.

6.1.238 RFC 3211: *Password based encryption for CMS*
This document provides a method of encrypting data using user-supplied passwords and, by extension, any form of variable-length keying material which is not necessarily an algorithm-

specific fixed-format key. The Cryptographic Message Syntax data format does not currently contain any provisions for password-based data encryption.

6.1.239 RFC 3217: *Triple-DES and RC2 Key Wrapping*
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.

6.1.240 RFC 3218: *Preventing the Million Message Attack on Cryptographic Message Syntax*.
When data is encrypted using RSA it must be padded out to the length of the modulus -- typically 512 to 2048 bits. The most popular technique for doing this is described in [PKCS-1-v1.5]. However, in 1998 Bleichenbacher described an adaptive chosen ciphertext attack on SSL. This attack, called the Million Message Attack (MMA), allowed the recovery of a single PKCS-1 encrypted block, provided that the attacker could convince the receiver to act as a particular kind of oracle. The MMA is also possible against Cryptographic Message Syntax (CMS). Mail list agents are the most likely CMS implementations to be targets for the MMA, since mail list agents are automated servers that automatically respond to a large number of messages. This document describes a strategy for resisting such attacks.

6.1.241 RFC 3227: *Guidelines for Evidence Collection and Archiving*
A "security incident" as defined in the "Internet Security Glossary",RFC 2828, is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident. If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

6.1.242 RFC 3244: *Microsoft Windows 2000 Kerberos Change Password and Set Pass*word *Protocols*
This memo specifies Microsoft's Windows 2000 Kerberos change password and set password protocols. The Windows 2000 Kerberos change password protocol interoperates with the original Kerberos change password protocol. Change password is a request reply protocol that includes a KRB_PRIV message that contains the new password for the user.

6.1.243 RFC 3278: *Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)*.
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.

6.2 Other Internet Related

6.2.1 S/MIME

6.2.1.1
This document describes a protocol for adding cryptographic signature and/or encryption services to Internet MIME (RFC 1521) messages. MIME provides a general structure for the content type

of Internet mail messages and allows extensions for new content type applications. Therefore, this draft defines application/x-pkcs7-mime which specifies that a MIME body part has been cryptographically enhanced according to PKCS #7. This draft also defines application/x-pkcs10 for use in submitting a certification request.

6.2.1.2

This specification is compatible with PKCS #7 in that it uses the data types defined by PKCS #7. It also inherits all the varieties of architectures for certificate-based key management supported by PKCS #7. This document discusses the use of multipart/signed and application/x-pkcs7-signature, which can be used to display the "clear text" of a signed message for the benefit of readers using an e-mail system with no security services.

6.2.2 SSL

The Secure Sockets Layer standard defines how an application operating in the Microsoft Windows environment can access security and communications services in a connection-oriented mode. The SSL protocol provides the ability to invoke encipherment and digital signature.

7 AMERICAN NATIONAL STANDARDS INSTITUTE

7.1 X9 Standards

7.1.1 ANSI X9.9: *Financial Industry Message Authentication Code (Wholesale)*

This standard provides details of the generation of a message authentication code using the DES encryption algorithm in the wholesale finance sector.

7.1.2 ANSI X9.17: *Financial Industry Key Management (Wholsesale)*

This standard provides details of the key management required for the use of the DES encryption system in the wholesale finance sector. This standard is equivalent to ISO/IEC 8732.

7.1.3 ANSI X9.19: *Financial Industry Message Authentication Code (Retail)*

This standard provides details of the generation of a message authentication code using the DES encryption algorithm in the retail finance sector.

7.1.4 ANSI X9.23: *Data Encryption Standard (Wholesale)*

This standard provides details of the encipherment of financial transactions using the DES algorithm.

7.1.5 ANSI X9.24: *Financial Industry Key Management (Retail)*

This standard provides details of the key management required for the use of the DES encryption system in the retail finance sector.

7.1.6 ANSI X9.26: *Secure Sign-On*

This standard details a mechanism to allow protected sign-on to a host computer.

7.1.7 ANSI X9.30: *Digital Signature Standard*

This standard provides details of the Digital Signature Standard promulgated as FIPS 186. The publication describes the Digital Signature Algorithm (DSA), the Secure Hash Algorithm (SHA), and the management of certificates to support DSS.

7.1.8 ANSI X9.31: *RSA*

This standard provides details of the Rivest-Shamir-Adleman (RSA) public key system. The

publication describes the use of the RSA algorithm to generate digital signatures, and the various hash algorithms (MD2, MD4, MD5, SHA, MDC-2) that can be used with RSA. The standard also describes certificate management.

7.1.9 ANSI X9.41: *Security Services Management*

This standard provides an overview of the management of the security services used in the X9 series of financial industry standards.

7.1.10 ANSI X9.42: *Diffie-Hellman Key Agreement*

This publication describes the use of the Diffie-Hellman cryptographic technique to achieve key agreement.

7.1.11 ANSI X9.43: *Key Archiving and Retrieval*

This standard explains why cryptographic keys need to be archived, and describes the mechanisms to be used for their archiving and subsequent retrieval.

7.1.12 ANSI X9.44: *Key Transport using RSA*

This standard describes how RSA is used to exchange confidentiality keys for subsequent symmetric encryption of messages, and provides details of how the RSA algorithm should be used to achieve key exchange.

7.1.13 ANSI X9.45: *Authorization Certificates*

This publication describes the use of security certificates to store and present authorization credentials.

7.1.14 ANSI X9.50: *Certificate Management for Encryption Key Management*

This standard describes how public key certificates are managed to provide for protection of the key exchange required to perform message encryption.

7.1.15 ANSI X9.52: *Triple Data Encryption Algorithm*

This standard provides details of the encipherment of financial transactions using the Triple-DES algorithm.

7.1.16 ANSI X9.55: *Certificate Extensions for X9*

The X.509 v3 certificate standard provides for user-defined extensions. X9.55 defines the specific extensions used for security and certificate handling in the financial sector.

7.1.17 ANSI X9.57: *Certificate Management*

X9.57 describes the management techniques for public key certificates used in the financial sector.

7.1.18 ANSI X9.62: Elliptic Curve Digital Signature Algorithm

This standard describes the implementation of a digital signature algorithm using elliptic curve techniques.

8 US NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

8.1 Federal information processing standards

8.1.1 FIPS Pub 31: *Guidelines for ADP Physical Security and Risk Management*

This document provides guidance to federal organizations in developing physical security and risk

management programs for their ADP facilities. It covers security analysis, natural disasters, failure of supporting utilities, system reliability, procedural measures and controls, protection of off-site facilities, contingency plans, security awareness, and security audit. It can be used as a checklist for planning and evaluating the security of computer systems.

8.1.2 FIPS Pub 41: *Computer Security Guidelines for Implementing the Privacy Act of 1974*
This publication provides guidance in the selection of technical and related procedural methods for protecting personal data in automated information systems. It discusses categories of risks and the related safeguards for physical security, information management practices, and system controls to improve system security.

8.1.3 FIPS Pub 46-2: *Data Encryption Standard*
This standard reaffirms the Data Encryption Algorithm (DEA) until 1998 and allows for implementation of the DEA in software, firmware or hardware. The DEA is a mathematical algorithm for encrypting and decrypting binary-code information.

8.1.4 FIPS Pub 48: *Guidelines on Evaluation Techniques for Automated Personal Identification*
This guideline discusses the performance of personal identification devices, how to evaluate them and considerations for their use within the context of computer systems security.

8.1.5 FIPS Pub 65: *Guideline for Automatic Data Processing Risk Analysis*
This guideline presents a technique for conducting a risk analysis of an ADP facility and related assets. It provides guidance on collecting, quantifying, and analysing data related to the frequency of occurrence and the damage caused by adverse events. This guideline describes the characteristics and attributes of a computer system that must be known for a risk analysis and gives an example of the risk analysis process.

8.1.6 FIPS Pub 73: *Guidelines for Security of Computer Applications*
This guideline describes the different security objectives for a computer application, explains the control measures that can be used, and identifies the decisions that should be made at each stage of the life cycle of a sensitive computer application. The guideline is designed for use in planning, developing and operating computer systems which require protection.

8.1.7 FIPS Pub 74: *Guidelines for Implementing the Data Encryption Standard*
This document provides guidance for the use of cryptographic techniques when such techniques are required to protect sensitive or valuable computer data. The guidelines should be used in conjunction with FIPS Pub 46-2 and FIPS Pub 81.

8.1.8 FIPS Pub 81: *DES Modes of Operation*
This standard defines four modes of operation for the Data Encryption Standard which may be used in a variety of applications. The modes specify how data will be encrypted (cryptographically protected) and decrypted (returned to original form). The modes included in this standard are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.

8.1.9 FIPS Pub 83: *Guideline on User Authentication Techniques for Computer Network Access Control*
This document provides guidance in the selection and implementation of techniques for authenticating the users of remote terminals in order to safeguard against unauthorized access to computers and computer networks.

8.1.10 FIPS Pub 87: *Guidelines for ADP Contingency Planning*
This guideline describes what should be considered when developing a contingency plan for an ADP facility. It provides a suggested structure and format which may be used as a starting point from which to design a plan to fit each specific operation.

8.1.11 FIPS Pub 88: *Guideline on Integrity Assurance and Control in Database Administration*
This guideline provides explicit advice on achieving database integrity and security control. It identifies integrity and security problems and discusses procedures and methods which have proven effective in addressing these problems. It provides an explicit, step-by-step procedure for examining and verifying the accuracy and completeness of a database.

8.1.12 FIPS Pub 94: *Guideline on Electrical Power for ADP Installations*
This guideline provides information on factors in the electrical environment that affect the operation of ADP systems. It describes the fundamentals of power, grounding, life-safety, static electricity, and lightening protection requirements, and provides a checklist for evaluating ADP sites.

8.1.13 FIPS Pub 102: *Guideline for Computer Security Certification and Accreditation*
This guideline describes how to establish and carry out a certification and accreditation program for computer security. Certification consists of a technical evaluation of a sensitive system to see how well it meets its security requirements. Accreditation is the official management authorization for the operation of the system and is based on the certification process.

8.1.14 FIPS Pub 112: *Standard on Password Usage*
This standard defines ten factors to be considered in the design, implementation, and use of access control systems that are based on passwords. It specifies minimum security criteria for such systems and provides guidance for selecting additional security criteria for password systems which must meet higher security requirements.

8.1.15 FIPS Pub 113: *Standard on Computer Data Authentication*
This standard specifies a Data Authentication Algorithm (DAA) which, when applied to computer data, automatically detects unauthorized modifications, both intentional and accidental. Based on the Data Encryption Standard (DES), this standard is compatible with the requirements adopted by the Department of Treasury and the banking community to protect electronic fund transfer transactions.

8.1.16 FIPS Pub 139: *Interoperability and Security Requirements for the Use of Data Encryption Standard in the Physical Layer of Data Communications*
This standard facilitates the interoperation of government data communication facilities, systems, and data that require cryptographic protection using the Data Encryption Standard (DES) algorithm. The standard specifies interoperability and security-related requirements using encryption at the physical layer of the ISO/IEC Open Systems Interconnect (OSI) reference model (see ISO/IEC 7498-2) in the telecommunications systems conveying ADP or narrative text information.

8.1.17 FIPS Pub 140-1: *Security Requirements for Cryptographic Modules*
This standard provides specifications for cryptographic modules which can be used within computer and telecommunications systems to protect unclassified information in a variety of different applications.

8.1.17.1 FIPS Pub 140-2: *Security Requirements for Cryptographic Modules*
This standard specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments. The areas covered, related to the secure design and implementation of a cryptographic module, include specification; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

8.1.18 FIPS Pub 141: *Interoperability and Security Requirements for the Use of Data Encryption Standard with CCITT Group 3 Facsimile Equipment*
This standard specifies interoperability and security-related requirements for use of encryption with International Telegraph and Telephone Consultative Committee (CCITT) Group 3 facsimile equipment conveying computer and/or narrative text information.

8.1.19 FIPS Pub 171: *Key Management using ANSI X9.17*
This standard specifies a selection of options for the automated distribution of keying material by the federal government when using the protocols of ANSI X9.17. The standard defines procedures for the manual and automated management of keying materials and contains a number of options. The selected options will allow the development of cost effective systems which will increase the likelihood of interoperability.

8.1.20 FIPS Pub 180: *Secure Hash Standard*
This standard specifies a Secure Hash Algorithm (SHA) which can be used to generate a condensed representation of a message called a message digest. The SHA is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required for federal applications. The SHA is used by both the transmitter and the intended receiver of a message in computing and verifying a digital signature.

8.1.21 FIPS Pub 181: *Automatic Password Generator (APG)*
This publication specifies a standard to be used by federal organizations that require computer generated pronounceable passwords to authenticate the personal identity of an automated data processing system user, and to authorize access to system resources. The standard describes an automated password generation algorithm that randomly creates simple pronounceable syllables as passwords. The password generator accepts input from a random number generator based on the Data Encryption Standard (DES) cryptographic algorithm defined in FIPS Pub 46-2.

8.1.22 FIPS Pub 185: *Escrowed Encryption Standard*
This standard specifies a technology developed by the federal government to provide strong encryption protection for unclassified information and to provide that the keys used in the encryption and decryption processes are escrowed.

8.1.23 FIPS Pub 186: *Digital Signature Standard (DSS)*
This standard specifies algorithms appropriate for applications requiring a digital, rather than written, signature. A digital signature is represented in a computer as a string of binary digits. A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified. An algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key which corresponds to, but is not

the same as, the private key. Each user possesses a private and public key pair. Public keys are never shared. Anyone can verify the signature of a user by employing that user's public key. Signature generation can be performed only by the possessor of the user's private key

8.1.24 FIPS Pub 188: *Standard Security Label for Information Transfer*
This standard defines a security label syntax for information exchanged over data networks and provides label encodings for use at the Application and Network Layers of the Open Systems Interconnect (OSI) reference model. Security labels convey information used by protocol entities to determine how to handle data communicated between open systems. Information on a security label can be used to control access, specify protective measures, and determine additional handling restrictions required by a communications security policy.

8.1.25 FIPS Pub 190: *Guideline for the use of Advanced Authentication Technology Alternatives*
This publication provides guidance on the use of advanced cryptographic authentication and biometric systems for entity authentication.

8.1.26 FIPS PUB 191: *Guideline For The Analysis Of Local Area Network Security*
This guideline can be used as a tool to help improve the security of a local area network (LAN). A LAN security architecture is described that discusses threats and vulnerabilities that should be examined, as well as security services and mechanisms that should be explored.

8.1.27 FIPS Pub 196: *Entity Authentication using Public Key Cryptography*
This publication provides guidance on the use of asymmetric cryptographic techniques, in particular digitally signed security certificates, to achieve entity authentication.

8.1.28 FIPS Pub 197: *Advanced Encryption Standard (AES)*
The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher-text; decrypting the cipher-text converts the data back into its original form, called plaintext.

8.1.29 FIPS Pub 198: *The Keyed-Hash Message Authentication Code (HMAC)*
This standard describes a keyed-hash message authentication code (HMAC), a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative Approved cryptographic hash function, in combination with a shared secret key. The cryptographic strength of HMAC depends on the properties of the underlying hash function. The HMAC specification in this standard is a generalization of Internet RFC 2104, HMAC, Keyed-Hashing for Message Authentication, and ANSI X9.71, Keyed Hash Message Authentication Code.

8.2 Special publications

8.2.1 NBS Spec Pub 500-61: *Maintenance Testing for the Data Encryption Standard*
This publication details for developers of DES hardware and software cryptographic systems a standard set of tests with which to verify the correctness of their products.

8.2.2 NBS Spec Pub 500-120: *Security Of Personal Computer Systems - A Management Guide*
NBS 500-120 provides both managers and users of personal computer systems with an

understanding of the information security threats involved in using such systems, and defines approaches for reducing the associated risks. The publication covers the three areas of confidentiality of data, integrity of data and the processes that handle data, and the availability of the systems and the data or services they support.

8.2.3 NBS Spec Pub 500-133: *Technology Assessment: Methods For Measuring The Level Of Computer Security*

This publication provides a summary of the methods for measuring the level of computer security in computer applications, systems, and installations. The need for computer security measurement and the difficulty in doing so are well known, and while a variety of techniques have been developed the inherent complexity of computer systems and the relative lack of experience in performing positive measurements have hampered progress. This publication provides a logical basis or such assessments.

8.2.4 NBS Spec Pub 500-134: *Guide On Selecting Adp Backup Process Alternatives*

This document provides managers and others responsible for developing automatic data processing contingency plans with an approach for selecting an alternative processing capability. It describes alternatives that are currently available and provides guidance on developing selection criteria. A checklist for evaluating the suitability of the alternatives is provided.

8.2.5 NBS Spec Pub 500-153: *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach*

This guide describes a process for auditing the system development life cycle of an automated information system to ensure that controls and security are designed and built into the system. The guide was developed by the Electronic Data Processing Systems Review and Security Work Group of the Computer Security project within the President's Council on Integrity and Efficiency, and contains bibliographies and a description of the pertinent laws and regulations.

8.2.6 NBS Spec Pub 500-156: *Message Authentication Code (MAC) Validation System: Requirements and Procedures*

This publication describes the Message Authentication Code (MAC) validation system which was developed by NBS to test message authentication devices for conformance to two data authentication standards (including FIPS Pub 113). This publication describes the basic design and configuration of the validation system, and the requirements and administrative procedures to be followed for requesting validations.

8.2.7 NIST Spec Pub 500-157: *Smart Card Technology: New Methods For Computer Access Control*

This document describes the basic components of a smart card and provides background information on the underlying integrated circuit technologies. The capabilities of a smart card are discussed, especially its applicability for computer security. The report describes research being conducted on smart card access control techniques; other major U.S. and international groups involved in the development of standards for smart cards and related devices are listed in the appendix.

8.2.8 NIST Spec Pub 500-166: *Computer Viruses And Related Threats: A Management Guide*

This document contains guidance for managing the threats of computer viruses and related software and unauthorized use. It is geared towards managers of end-user groups and managers dealing with multi-user systems, personal computers and networks. The guidance is general and

addresses the vulnerabilities that are most likely to be exploited.

8.2.9 NIST Spec Pub 500-169: *Executive Guide to the Protection of Information Resources*

8.2.9.1

Federal agencies are becoming increasingly dependent upon automated information systems to carry out their missions. While in the past, executives have taken a hands-off approach in dealing with these resources, essentially leaving the area to the computer technologist, they are now recognizing that computers and computer-related problems must be understood and managed, the same as any other resource.

8.2.9.2

The success of an information resources protection program depends on the policy generated, and on the attitude of management towards securing information on automated systems. This publication provides policy makers with guidance in the areas of risk reduction, compliance with laws and regulations, assurance of operational continuity, and information integrity and confidentiality.

8.2.10 NIST Spec Pub 500-170: *Management Guide to the Protection of Information Resources*

8.2.10.1

Today computers are integral to all aspects of operations within an organization. As organizations become more dependent upon computer information systems to carry out their missions, computers and computer-related problems need to be understood and managed as much as any other resource. It is important to set policies, goals, and standards for protection of data, information, and computer resources, and to commit resources for information security programs. All managers who use any type of automated information system must become familiar with the policies and procedures for protecting the information which is processed and stored within those systems.

8.2.10.2

Adequately secure systems deter, prevent, or detect unauthorized disclosure, modification, or use of information. Information also requires protection from intruders, as well as from employees with authorized computer access privileges who attempt to perform unauthorized actions. Protection is achieved not only by technical, physical and personnel safeguards, but by also articulating and implementing agency policy regarding authorized system use to information users and processing personnel at all levels.

8.2.10.3

This guide is one of three brochures; the “Executive Guide to the Protection of Information Resources” and the “Computer User’s Guide to the Protection of Information Resources” complete the series.

8.2.11 NIST Spec Pub 500-171: *Computer Users’ Guide to the Protection of Information Resources*

Today’s computer technology, with microcomputers and on-line access, has increasingly forced users to take responsibility for the protection of information stored on or processed by their computers. While excellent progress has been made in computer technology, more progress is needed to inform users of the vulnerability of data and information to such threats as unauthorized modification, disclosure, and destruction, either deliberate or accidental. This guide aims to increase user awareness of the undesirable things that can happen to data and to provide practical solutions for reducing risks to these threats.

8.2.12 NIST Spec Pub 500-172: *Computer Security Training Guidelines*

This publication provides managers and others responsible for the provision of computer security training with an overview of the areas of training and an approach to providing such training.

8.2.13 NIST Spec Pub 500-174: *Guide for Selecting Automated Risk Analysis Tools*

8.2.13.1

This document recommends a process for selecting automated risk analysis tools. It is primarily intended for managers and those responsible for managing risks in computer and telecommunications systems. The document describes important considerations for developing selection criteria for acquiring risk analysis software. The information presented is derived from reviews of risk analysis software tools in the Risk Management Research Laboratory which is cooperatively sponsored by the National Institute of Standards and Technology (NIST) and the National Computer Security Center (NCSC) and from experiences of organizations in the Federal government and private sectors.

8.2.13.2

This document recommends selecting a group of personnel with special skills to participate in the risk analysis studies. Concepts and definitions of terms necessary to understand risk analysis are also provided. This report describes three essential elements that should be present in an automated risk analysis tool: data collection, analysis, and output results. When developing site-specific requirements criteria, mandatory requirements should be separated from those that are desirable.

8.2.14 NIST Spec Pub 500-189: *Security In ISDN*

This document discusses the standards needed to implement user security in Integrated Services Digital Network (ISDN) technology. The publication provides a broad discussion of user security needs and suggests possible solutions.

8.2.15 NIST Spec Pub 800-2: *Public-Key Cryptography*

8.2.15.1

This publication presents a state-of-the-art survey of public-key cryptography circa 1988-1990. In doing so, it covers a number of different topics including: 1. The theory of public-key cryptography. 2. Comparisons to conventional (secret-key) cryptography. 3. A largely self-contained summary of relevant mathematics. 4. A survey of major existing public-key systems. 5. An exploration of digital signatures and hash functions. 6. A survey of public-key implementations in networks. 7. An introduction to zero-knowledge protocols and probabilistic encryption. 8. An exploration of security issues and key sizes.

8.2.15.2

The treatment of public-key cryptography in this publication includes both theory and practice. Much of the existing published work, including those documents listed in the references, treats either the theory or specific systems/implementations, but not both. The viewpoint here is that the theory and practice are inseparable.

8.2.16 NIST Spec Pub 800-3: *Establishing A Computer Security Incident Response Capability*

This publication describes increased computer security efforts, designated as Computer Security Incident Response Capabilities (CSIRC), which offer an efficient and cost-effective response to computer security threats. A CSIRC is a proactive approach to computer security, one that combines reactive capabilities with active steps to prevent future incidents.

8.2.17 NIST Spec Pub 800-4: *Computer Security Considerations In Federal Procurements: A Guide For Procurement Initiators, Contracting Officers, And Computer Security Officials*

This document assists federal agencies in selecting and acquiring cost-effective computer security by explaining how to include computer security requirements in federal information processing procurements.

8.2.18 NIST Spec Pub 800-5: *A Guide To The Selection Of Anti-Virus Tools And Techniques*

This guide gives criteria for judging the functionality, practicality, and convenience of anti-virus tools so that users can determine which tools are best suited to target environments.

8.2.19 NIST Spec Pub 800-6: *Automated Tools For Testing Computer System Vulnerability*

This document discusses the use of automated tools to perform system vulnerability tests. The tests examine a system for vulnerabilities that can result from improper use of controls or mismanagement, such as easily guessed passwords or improperly protected system files.

8.2.20 NIST Spec Pub 800-7: *Security in Open Systems*

8.2.20.1

Beginning with the ISO/IEC OSI and the IEEE POSIX operating system interface standard, a great many open systems standards are beginning to appear, and open systems products are being provided by every major computer vendor. In short, an open system standard is an interface specification to which any vendor can build products.

8.2.20.2

There are two important points. First, the specification simply defines an interface. For example, although POSIX is derived from UNIX, non-UNIX operating systems such as Digital's VMS can also provide a POSIX interface. Second, the specification is available to any vendor and evolves through a consensus process that is open to the entire industry.

8.2.20.3

In the past, users have often been "locked in'' to products from a particular vendor because their applications would run only on that vendor's operating system. The move to open systems reduces this dependence and application systems can increasingly be built on products from a variety of vendors. But many needed standards are not complete, and some non-standard functions will always be needed because standards must necessarily lag innovations in technology.

8.2.20.4

The term "open'' applies to two different aspects of the telecommunications environment: the FCC's ONA requirements that allow multiple vendors to have equal access to the network; and the open system platforms based on standards, such as POSIX and OSI, that are used in building computer based applications for the new open telecommunications environment. Security is thus a vital concern with open systems - it may be easier for intruders to attack a system whose behavior is standardized and well known, or which shares common flaws with other systems built on the same standards. A recent Bellcore report found that ``intruders were assisted in their endeavors by the openness and standardization that the telecommunications industry has undergone in the last decade.''

8.2.20.5

This report was prepared to help service designers use standard, open systems platforms in building security into their software applications. Security in an open system environment may be affected by the need to use both standard and non-standard components, and by the possibility

for incompatibilities among products that claim to meet the same standard. The large number of third party service providers whose products must work together may severely complicate efforts to ensure dependability and security of the PSN.

8.2.21 NIST Spec Pub 800-8: *Security Issues in the Database Language SQL*

The Database Language SQL (SQL) is a standard interface for accessing and manipulating relational databases. An SQL-compliant database management system (DBMS) will include a minimum level of functionality in a variety of areas. However, many additional areas are left unspecified by the SQL standard. In addition, there are multiple versions of the SQL standard; the functionality will vary according to the particular version. This document examines the security functionality that might be required of relational DBMS's, and compares them with the requirements and options of the SQL specifications. The comparison will show that the security functionality of an SQL-compliant DBMS may vary greatly. A variety of security policies are considered which can be supported by SQL. The document ends by showing which types of functions are required by the examined security policies.

8.2.22 NIST Spec Pub 800-9: *Good Security Practices For Electronic Commerce, Including Electronic Data Interchange*

This report presents security procedures and techniques, including internal controls and checks, that constitute good practice in the design, development, testing, and operation of electronic commerce systems. Security techniques considered include audit trails, contingency planning, use of acknowledgements, electronic document management, activities of support networks, user access controls to systems and networks, and cryptographic techniques for authentication and confidentiality.

8.2.23 NIST Spec Pub 800-10: *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*

8.2.23.1

This document provides an overview of the Internet and security-related problems. It then provides an overview of firewall components and the general reasoning behind firewall usage. Several types of network access policies are described, as well as technical implementations of those policies. Lastly, the document contains pointers and references for more detailed information.

8.2.23.2

The document is designed to assist users in understanding the nature of Internet-related security problems and what types of firewalls will solve or alleviate specific problems. Users can then use this document to assist in purchasing or planning a firewall.

8.2.24 NIST Spec Pub 800-12: *An Introduction To Computer Security: The NIST Handbook*

This handbook provides assistance in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. It gives a broad overview of computer security to help readers understand their computer security needs and to develop a sound approach in selecting appropriate security controls.

8.2.25 NIST Spec Pub 800-13: *Telecommunications Security Guidelines For Telecommunications Management Network*

This document gives guidance on enhancing the security of the Public Switched Network (PSN) which provides critical commercial telecommunications services and National Security and

Emergency Preparedness (NSEP). The guidance assists telecommunications vendors in developing systems and service providers in implementing systems with appropriate security for integration into the PSN. It is also useful to government agencies or commercial organizations in formulating a specific security policy.

8.2.26 NIST Spec Pub 800-14: *Generally Accepted Principles And Practices For Securing Information Technology Systems*

This document provides a baseline that organizations can use to establish and review their information technology (IT) security programs. It presents a foundation of generally accepted system security principles and gives common practices that are used in securing IT systems. The guideline assists managers, internal auditors, users, system developers, and security professionals to gain an understanding of basic security requirements.

8.2.27 NIST Spec Pub 800-15: *Minimum Interoperability Specifications for PKI Components (MISPC)*

This publication specifies a minimum set of features, transactions, and data fomats for Certification Authorities (CAs), Organizational Registration Authorities (ORAs), and PKI clients. The publication addresses certificate generation, renewal, and revocation; certificate and certificate path validation; signature generation and verification; and cross certification.

8.2.28 NIST Spec Pub 800-16: *Information Technology Security Training Requirements: A Role And Performance-Based Model*

This document is designed for use by organizations who develop security training and awareness courses, or for those personnel who develop information technology (IT) security training for government use. The document emphasizes training criteria or standards, rather than fixed content of specific courses and audiences. The emphasis on roles and results gives the training requirements flexibility, adaptability, and longevity.

8.2.29 NIST Spec Pub 800-17: *Modes of Operation Validation System (MOVS): Requirements and Procedures*

8.2.29.1

The National Institute of Standards and Technology (NIST) Modes of Operation Validation System (MOVS) specifies the procedures involved in validating implementations of the DES algorithm in FIPS PUB 46-2 The Data Encryption Standard (DES) and the Skipjack algorithm in FIPS PUB 185, Escrowed Encryption Standard (ESS). The MOVS is designed to perform automated testing on Implementations Under Test (IUTs). This publication provides brief overviews of the DES and Skipjack algorithms and introduces the basic design and configuration of the MOVS.

8.2.29.2

Included in this overview are the specifications for the two categories of tests which make up the MOVS, i.e., the Known Answer tests and the Modes tests. The requirements and administrative procedures to be followed by those seeking formal NIST validation of an implementation of the DES or Skipjack algorithm are presented. The requirements described include the specific protocols for communication between the IUT and the MOVS, the types of tests which the IUT must pass for formal NIST validation, and general instructions for accessing and interfacing with the MOVS. An appendix with tables of values and results for the DES and Skipjack Known Answer tests is also provided.

8.2.30 NIST Spec Pub 800-18: *Guide for Developing Security Plans for Information Technology Systems*

8.2.30.1

The purpose of a security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager. Additional information may be included in the basic plan and the structure and format organized according to agency needs, so long as the major sections described in this document are adequately covered and readily identifiable.

8.2.30.2

This document provides guidance on how to develop a security plan. It builds on the practices portion of the NIST Handbook of Computer Security and the Generally Accepted Principles and Practices for Securing Information Technology Systems documents. The NIST Handbook should be used to obtain additional detail or explanation on any of the controls listed, and the Principles and Practices document should be used as a reference to describe the controls and used as a guide for reviewing the plan. Each planning guide control chapter easily maps to the NIST Handbook and the Principles and Practices document since the chapters in all three documents are listed under the same three controls, i.e., management, operational, and technical.

8.2.31 NIST Spec Pub 800-19: *Mobile Agent Security*

Over the years computers have evolved from centralised monolithic computing devices into client-server systems that allow complex forms of distributed computing. A new evolution is under way allowing complete mobility of cooperating applications among supporting platforms to form a large scale, loosely coupled system. The catalyst for this evolution is the mobile software agent, programs that are goal directed and capable of suspending their processing on one platform and transferring it for resumption on another. This document examines the threats to confidentiality, integrity, and availability caused by the use of mobile agents and provides recommendations on countermeasures.

8.2.32 NIST Spec Pub 800-20: *Modes of Operation Validation System for the Triple Data Encryption Algorithm*

The Modes of Operation Validations System is designed to perform automated testing on Implementations Under Test (IUT) of cryptographic algorithms. This publication introduces the basic design and configuration of the Triple Data Encryption Algorithm Modes of Operation Validation System (TMOVS) and details the procedures involved in validating implementations of TDEA using TMOVS and in seeking formal NIST validation of implementations. Included in this publication are the specifications for two categories of the tests that make up the TMOVS, i.e. the Known Answer tests and the Monte Carlo tests.

8.2.33 NIST Spec Pub 800-21: *Guideline for Implementing Cryptography in the Federal Government*

The purpose of this document is to provide guidance to Federal Agencies on how to select cryptographic controls for protecting sensitive unclassified information. The document focuses on federal standards documented in the FIPS publications and the cryptographic modules and algorithms that are validated against these standards. Additional (ISO, ANSI) standards for cryptographic security are also discussed. The publication is intended to provide management

and technical staff with sufficient information to allow them to make informed decisions about the cryptographic methods that will meet their specific needs to protect the confidentiality, authentication, and integrity of data that is transmitted or stored in a system or network. The document is in three parts. The first part overviews cryptographic services and products. Part two focuses on the Cryptographic Module Validation Programme and PKI. Part three details how to select services and products, and provides examples of Federal projects that use cryptography.

8.2.34 NIST Spec Pub 800-22: *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*

The need for random and pseudorandom numbers arises in many cryptographic applications. For example, common cryptosystems employ keys that must be generated in a random fashion. Many cryptographic protocols also require random or pseudo random inputs at various points, eg for auxiliary quantities used in generating digital signatures, or for generating challenges used in cryptographic protocols.

This document discusses the randomness testing of random number and pseudorandom number generators that may be used for many purposes including cryptographic, modelling and simulation applications. The focus of this document is on those applications where randomness is required for cryptographic purposes. A set of statistical tests for randomness is described in this document. Given that some statistical anomalies are to be expected in generators, guidance on interpreting the results of statistical testing is also provided.

8.2.35 NIST Spec Pub 800-23: *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*

This guideline provides advice on the security assurance of products used for the protection of sensitive unclassified information, to ensure confidence in the technical and operational security measures. These guidelines cover understanding information assurance, how information assurance supports security, evaluation and conformance testing procedures for information assurance, selection and risk analysis of products against information assurance standards, and methods for integration of information security products into systems while retaining assurance levels. The guideline also includes overviews of the US National Information Assurance Acquisition Policy and the National Information Assurance Programme.

8.2.36 NIST Spec Pub 800-24: *PBX Vulnerability Analysis*

A Private Branch Exchange (PBX) is a sophisticated computer-based switch that manages the connections and additional functions required of modern telephony systems. This document provides a methodology for conducting an analysis of a digital PBX in order to identify security vulnerabilities, and covers the areas of system architecture, hardware, maintenance, administrative database/software and user features.

8.2.37 NIST Spec Pub 800-25: *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*

This document provides guidance to US Federal Agencies for the use of public key technology for digital signatures or authentication over the Internet, specifically assisting in the evaluation of potential applications of PKI from technical, policy, business, and legal perspectives. It also provides guidance on the implementation of PKI based applications.

8.2.38 NIST Spec Pub 800-26: *Security Self-Assessment Guide for Information Technology Systems*

Adequate security of information and the systems that process it is a fundamental management responsibility. Management must understand the current state of their information security programme and controls in order to make informed judgements and investments that appropriately mitigate risks to an acceptable level.

Self assessments provide one method to determine the current status of information security programmes and, where necessary, establish a target for improvement. This self assessment guide utilises an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. The control objectives and techniques are extracted from long standing requirements found in statute, policy, and guidance on security.

This document provides guidance on applying the Federal IT Security Assessment Framework by identifying 17 control areas and provides control objectives and techniques which can be measured for each area.

8.2.39 NIST Spec Pub 800-27: *Engineering Principles for Information Technology Security*

This document presents generic principles of IT Security that apply to all IT systems. It provides 32 security principles and shows how they fit into the system initiation, development, implementation, operation, maintenance, and disposal IT system life cycle.

8.2.40 NIST Spec Pub 800-28: *Guidelines on Active Content and Mobile Code*

Active content refers to electronic documents that can carry out or trigger actions automatically without an individual directly or knowingly invoking the actions. Exploits based on vulnerabilities in active content technologies by their very nature can be insidious. This document provides key guidelines for dealing with active content.

8.2.41 NIST Spec Pub 800-29: *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*

On 17 July 1995, NIST established the Cryptographic Module Validation Program (CVMP) that validates cryptographic modules to the Federal Standard FIPS 140-1 and other cryptography standards. The CMVP is a joint activity between NIST and the Communications Security Establishment of the Government of Canada. Products validated as conforming to FIPS 140 are accepted by both countries for Federal use. A government and industry working group composed of both users and vendors developed the FIPS 140-1 standard which lists eleven security areas and four levels of assurance. In 1998, FIPS 140-1 was reviewed to consider new and/or revised requirements needed to meet technological and/or economic change. In June 2001, the revised standard FIPS 140-2 came into full use in the CMVP. This document describes the differences between the FIPS 140-1 and FIPS 140-2 standards.

8.2.42 NIST Spec Pub 800-30: *Risk Management Guide for Information Technology Systems*

This guide provides a foundation for the development of an effective risk management programme, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The guidance is based on the general concepts presented in NIST Special Publication 800-27 *Engineering Principles for Information Technology Security.* The publication consists of an overview of risk management, a nine-step risk assessment methodology, the risk mitigation process through selection of cost-effective security controls, and the ongoing procedures for ongoing risk evaluation and assessment.

8.2.43 NIST Spec Pub 800-31: *Intrusion Detection Systems (IDS)*
This guidance document is intended as a primer on intrusion detection, developed for those that need to understand what security goals intrusion detection systems serve, how to select and configure intrusion detection systems for their specific system and network environments, how to manage the output of intrusion detection systems, and how to integrate intrusion detection functions with rest of the organisational security infrastructure.

8.2.44 NIST Spec Pub 800-32: *Introduction to Public Key Technology and the Federal PKI Infrastructure*
Public Key Infrastructures (PKIs) can speed up and simplify the delivery of products and services by providing electronic approaches to processes that traditionally have been paper based. These solutions depend upon integrity and authenticity, characteristics which can be achieved by the use of a unique digital signature created using a public key associated with an individual and protected in such a way it cannot be forged. In addition, PKIs can support encryption services to provide confidentiality of information storage and transfer.

This publication is intended to allow managers to determine whether a PKI solution is appropriate for their organisation, and how PKI services can be deployed most effectively, and reviews the risks and benefits of PKI components and describes the planning process for PKI deployment. It also provides an overview of the issues related to the emerging Federal PKI.

8.2.45 NIST Spec Pub 800-33: *Underlying Technical Models for Information Technology Security*
The purpose of this standard is to provide a description of the technical foundations, called 'models', that underlie secure information technology. These models should be considered in the design and development of technical security capabilities. The models cover the five principles of confidentiality, integrity, availability, assurance, and accountability.

8.2.46 NIST Spec Pub 800-34: *Contingency Planning Guide for IT Systems*
This guide provides instructions, recommendations and considerations for government IT contingency planning. Contingency planning refers to interim measures to recover IT services after an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, recovery of IT functions using alternative equipment, or performance of IT functions using manual methods.

The information in this publication addresses seven IT platform types: mainframes, distributed systems, wide area networks, local area networks, servers, websites, and desktop/portable systems. The contingency process is a seven stage process designed to integrate into each stage of the system development life cycle. The stages are develop contingency planning policy, conduct a business impact analysis, identify preventative controls, develop recovery strategies, develop the contingency plan, test the plan and train personnel, and maintain the plan.

A sample format for a contingency plan is given, with three phases of actions following a disaster. These are notification/activation, recovery, and reconstitution. Four controls common across platforms are identified and discussed: offsite storage, interoperability, redundancy, and coordination with security controls.

8.2.47 NIST Spec Pub 800-38a: *Recommendation for Block Cipher Modes of Operation*
This standard specifies five confidentiality modes of operation for symmetric key block cipher algorithms. The modes may be used in conjunction with any symmetric key block cipher

algorithm that is approved by a Federal Information Processing Standard. The five modes specified in the publication are Electronic Codebook (ECB), Cipher Block Chaining (CBC) Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) mode.

8.2.48 NIST Spec Pub 800-40: *Procedures for Handling Security Patches*
Security flaws in standard commercial software are often addressed by the use of security patches that can be applied by end user organisations. This document describes and recommends the use of a systematic, accountable, and documented process for handling security patches and vulnerabilities. In addition, the document provides specific advice for obtaining, testing, distributing, and installing security patches.

8.2.49 NIST Spec Pub 800-41: *Guidelines on Firewalls and Firewall Policy*
Firewalls protect sites from the inherent vulnerabilities in the TCP/IP protocol and from exploitation of vulnerabilities existing in the systems used in internal networks. There are several types of firewalls, ranging from boundary routers that can provide access control based on Internet Protocol packets, to powerful firewalls that can filter traffic based on the contents of the packet. This document provides information about firewalls and firewall policies to assist those responsible for network security. It addresses concepts related to the design, selection, deployment and management of firewalls and firewall environments.

8.2.50 NIST Spec Pub 800-42: *Guidelines on Network Security Testing*
This document describes a methodology for using network-based tools for testing systems for vulnerabilities. The primary aim of the document is to help administrators and managers get started with a program for testing on a routine basis. The methodology recommends focusing first on those systems that are accessible externally, e.g., firewalls, web servers, etc., and then moving on to other systems as resources permit. The document includes many pointers to various testing applications and contains more detailed descriptions of several of the more popular test tools.

8.2.51 NIST Spec Pub 800-43: *System Administration Guidance for Windows 2000 Professional*
Windows 2000 Professional has many security features System Administrators can enable to protect their users and their networks. This document describes the security features and registry security settings in a simple, easy to understand way and recommends security settings for Windows 2000 and various applications. Using this publication, Systems Administrators can familiarise themselves with the full usability and impact of Windows 2000's security features. In addition, the publication provides a substantial reference to security publications and sites, and overviews Remote Systems Management and Windows XP security features. Two security templates are included to assist Administrators in implementing security.

8.2.52 NIST Spec Pub 800-44: *Guidelines on Securing Web Servers*
This document provides detailed guidance on securely setting up and maintaining a public Web server, and includes pointers to related material.

8.2.53 NIST Spec Pub 800-45: *Guidelines on Electronic Mail Security*
At the most basic level, the email process can be divided into two basic components: (1) mail servers, which are applications that deliver, forward, and store mail; and (2) mail clients which interface with users and allow users to receive, read, compose, send, and store email messages.

After Web servers, mail servers are often the most targeted and attacked hosts on an organisations network, because the computing and networking technology that underpins email is ubiquitous and therefore makes it easier for attackers to exploit such systems. Threats include malicious exploitation of software flaws, denial of service, unauthorised access and distribution, interception and modification of information transmitting between mail clients and servers. This publication provides detailed guidance on installing, operating, and maintaining secure mail servers and clients, and includes pointers to related material.

8.2.54 NIST Spec Pub 800-46: *Security for Telecommuting and Broadband Communications*
Telecommuting is an increasingly important trend in information systems and networking. Accompanying and supporting this approach to work is the availability of broadband telecommunication services to the home user. While there is a good general understanding of the management and technical requirements for security in office environments, security of home workstation and network environment is less well defined. In addition, the use of permanent connections for broadband access to the Internet makes remote targeted attack much more likely than in the case of dial up connections.

This publication provides introductory information about broadband communications security and policy, security of the home office systems, and considerations for system administrators. It addresses concepts relating to the selection, deployment and management of broadband communications for a telecommuting user. Step by step instructions are provided for configuring systems and selecting security options. In particular, the document discusses the use of personal firewalls and virtual private networks.

8.2.55 NIST Spec Pub 800-47: *Guide for Interconnecting Information Systems*
This document provides guidance for planning, establishing, maintaining and terminating interconnections between information systems that are owned and operated by different organisations. It provides a logical framework for organisations that have not previously interconnected information systems, and it provides information that other organisations may use to enhance the security of their existing interconnections. The document includes guidance on developing an Interconnection Security Agreement, a Memorandum of Understanding which defines the responsibilities of each party, and a System Interconnection Implementation Plan.

8.2.56 NIST GCR 93-635: *Private Branch Exchange (PBX) Security Guidelines*
This document presents the basic concepts of PBX security. It describes a telephone switch system, hardware and software assets, specific security threats, and the functions of the PBX administrator. An example of a security policy and some controls needed to secure the PBX environment are also given.

8.3 Reports

8.3.1 NBSIR 86-3386: *Work Priority Scheme for EDP Audit and Computer Security Review*
This publication describes a methodology for prioritising the work performed by EDP auditors and computer security reviewers, and enables users to evaluate computer security systems for both EDP audit and security review functions and to develop a measurement of the risk of the systems.

8.3.2 NISTIR 5153: *Minimum Security Requirements for Multi-User Operating Systems*
This document provides basic commercial computer system security requirements applicable to

both government and commercial organizations. These requirements form the basis for the commercially oriented protection profiles used in the Common Criteria.

8.3.3 NISTIR 5308: *General Procedures for Registering Computer Security Objects*
This publication describes the object-independent procedures for operating the Computer Security Objects Register (CSOR) which services organizations and individuals seeking to use a common set of tools and techniques in computer security.

8.3.4 NISTIR 4939: *Threat Assessment Of Malicious Code And External Attacks*
This report provides an assessment of the threats associated with malicious code and external attacks on systems using commercially available hardware and software.

9 EUROPEAN ELECTRONIC SIGNATURE STANDARDISATION INITIATIVE (EESSI)

9.1 EESSI Overview

9.1.1 On 1999-12-13 the European Commission published Directive 191999/93/EC to provide a Community framework for electronic signatures (hereafter [Dir.1999/93], for download see *http://www.ict.etsi.org/eessi/Documents/e-sign-directive.pdf*). This Directive focuses on the legal recognition of electronic signatures. It identifies minimal requirements for certificates, certification service providers and signature creation and verification devices.

9.1.1.1 The European ICT Standards Board, with a mandate from the European Commission, launched an industry initiative bringing together industry and public authorities, experts and other market players, in support of the European Directive on electronic signatures: the European Electronic Signature Standardization Initiative (EESSI). The initiative is open to all who wish to participate.

9.1.2 Under the work programme defined and co-ordinated by the EESSI Steering Group the development and maintenance of the required standards is entrusted to two separate bodies. These bodies are the Comité Européen de Normalisation, Information Society Standardisation System (CEN/ISSS) and the European Telecommunications Standards Institute (ETSI). Each has developed a range of de facto standards under their own procedures, but under the umbrella of the EESSI programme and in close co-operation with one another. In each case the standards are drafted by expert teams, subsequently reviewed by the industry representatives attending the respective working groups of CEN and ETSI, and finally approved by members of the organisations.

9.1.3 The Directive allows the European Commission to establish and publish references of generally recognised standards for electronic signature products. As a consequence, European Union Member States' laws shall presume compliance with the requirements laid down in [Dir.1999/93] when an electronic signature product meets those standards.

9.1.4 Further information regarding EESSI may be found at http:**//** *www.ict.etsi.org/eessi/EESSI-homepage.htm***.**

9.1.5 In the two following sub-sections, listing both CEN- and ETSI-developed deliverables from the EESSI programme, the documents are ordered not by strict numeric sequence but in a form of hierarchy, commencing with those dealing with policy and requirements, descending through those dealing with services and systems, through to those which cover products, processes and technical specifications.

9.1.6 In describing these standards a small set of special terms are used, which may be unfamiliar to the reader. These are all capitalised and originate from the specific terminology used by [Dir.1999/93]. Since the majority of readers of this text are not expected to be familiar with this EC Directive, use of its special terms has been limited as far as possible, but a minimum set of terms has necessarily been retained in order to effectively describe and 'bind' together the standards produced under EESSI.

Note: Where the standard concerned is work in progress and has yet to be published this is indicated by the notation 'wip', within the reference.

9.2 CEN Workshop Agreements

9.2.1 The Comité Européen de Normalisation, Information Standardisation System (CEN/ISSS) has developed the standards for which it has been given responsibility through the operation of an open workshop 'E-SIGN', created specifically for this purpose. As a product of the E-SIGN workshop, draft documents are approved as CEN Workshop Agreements, henceforth CWAs. CWAs are consensus-based specifications, drawn up in an open Workshop environment. This more flexible approach assures a quicker process to developing a de facto standard which industry can put to immediate use. A CWA may subsequently be progressed through the more formal channels to become an EN (Européen Norme – European Standard).

9.2.2 Further information is available from http://www.cenorm.be/isss/workshop/e-sign and the CWAs identified below are available for download free of charge from: *http://www.cenorm.be/isss/CWAs/cwalist.htm#Electronic%20Signatures*.

9.3 STANDARDS

9.3.1 CWA 14167-1:2001: *E - Trustworthy Systems: System Security Requirements*

This CWA has three distinct and separate parts – this sub-section deals with Part 1 exclusively, which specifies security requirements on products and technology components, used by certification service providers, managing the issuing of both Qualified and non-Qualified Certificates. These certificates are used in conjunction with electronic signatures and advanced electronic signatures in accordance with [Dir.1999/93].

9.3.1.1 This Part is specifically relevant for manufacturers of Trustworthy Systems used for managing certificates but may be adopted by anyone deploying systems and wanting to meet the requirements of [Dir.1999/93]. It provides an overview of a certification service, decomposed into component sub-services delivering specific functionality, security requirements for which are expressed in this Part. It thus gives service providers a common basis for use of trustworthy systems, and help users to have assurance that a provider uses trustworthy systems

9.3.2 CWA 14167-2:2002: *E- trustworthy Systems: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)*

This CWA has three distinct and separate parts – this sub-section deals with Part 2 exclusively, which specifies the security requirements of a cryptographic module used by a certificate service provider as part of its trustworthy system to provide signing services, such as certificate generation services or certificate status information signing services. These requirements are expressed in the form of a Common Criteria Protection Profile intended for application to cryptographic modules. This PP is independent from, whilst being compatible with, Part 3 of this CWA.

9.3.3 CWA 14167-3: wip *Trustworthy Systems: Cryptographic Module for CSP Key Generation Services — Protection Profile (CMCKG-PP)*

This CWA has three distinct and separate parts – this sub-section deals with Part 3 exclusively,which specifies the security requirements of a cryptographic module used by a certificate service provider as part of its trustworthy system to provide key generation services and signing device provision services. These requirements are expressed in the form of a Common Criteria Protection Profile intended for application to cryptographic modules.

9.3.4 CWA 14168:2002: *E - Secure Signature Creation Devices "EAL4"*

This CWA defines security requirements for secure signature creation devices, in accordance with [Dir.1999/93], formulated as a Common Criteria Protection Profile. The aim is to standardise the security requirements for SSCDs and to ensure their conformity with [Dir.1999/93] and their mutual interoperability. The CWA is based on the working assumption of being technology-neutral. The security requirements for SSCDs are as technology-neutral as possible. Following this approach, the CWA tries to cover as many different SSCD implementations as possible according to the current technology status. This CWA defines the Protection Profile to an assurance level EAL4 (cf. CWA 14169).

9.3.5 CWA 14169:2002: *E - Secure Signature Creation Devices "EAL4+"*

This CWA is effectively the same as CWA 14168, save that it defines the Protection Profile to an assurance level EAL4+ (augmented).

9.3.6 CWA 14170:2001: *E - Security Requirements for Signature Creation Applications*

This CWA supports the objectives of [Dir.1999/93] by specifying recommended security requirements for those signature creation systems which create advanced electronic signatures with the help of Secure Signature Creation Devices and Qualified Certificates.

9.3.6.1 The CWA provides guidance for application and computer system environments for the creation of signatures. By following this specification, it is ensured that application and computer system environments incorporating signature creation are implemented in a way that provides the functionality necessary for signature creation that is of sufficient quality to minimise the likelihood of any dispute.

9.3.7 CWA 14171:2001: *E - Procedures for Electronic Signature Verification*

This CWA contains a specification for the signature verification procedure, including both the products used for verification, and their management. It provides guidance for application and computer system environments performing the verification of signatures. By following this specification, it is ensured that application and computer system environments incorporating signature verification are implemented in a way that provides the functionality necessary for signature creation that is of sufficient quality to minimise the likelihood of any dispute.

9.3.8 CWA 14355:2002: *E - Guidelines for the implementation of Secure Signature-Creation Devices*

This CWA is built upon CWA14168 and CWA 14169. Because those CWAs are based on the working assumption of a technology-neutral approach they are not able to emphasise strengths of any certain technologies. This specific CWA therefore gives guidelines on implementing secure signature creation devices in specific platforms (such as smart cards, PCs, PDAs and mobile phones) and in specific environments (such as public terminals or secured environments).

9.3.9 CWA tba:wip**: -** *Application Interface for SmartCards used as Secure Signature Creation Devices*

In this CWA, the interface between a smart card implementation of a secure signature creation device and its environment is standardised. This involves command sets, file specifications etc. This will allow for full mobility of smart card PKI module, much like the SIM mobility in a GSM phone.

9.3.10 CWA 14172-n:2001: *E - Conformity Assessment Guidance*

This CWA provides guidance with a view to harmonising the application of the standards for services, processes, systems and products for Electronic Signatures developed under the European Electronic Signature Standardisation Initiative (EESSI) by the CEN/ISSS Workshop on Electronic Signatures and the ETSI SEC ESI Working Group. The guidance is intended for use by certification-service-providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories involved in assessing conformance to these standards. The CWA has five parts currently published, each separately available:

9.3.10.1 CWA 14172-1:2001 *E - General;*

9.3.10.2 CWA 14172-2:2001 *E - Certification Authority services and processes;*

9.3.10.3 CWA 14172-3:2001 *E - Trustworthy systems managing certificates for electronic signatures;*

9.3.10.4 CWA 14172-4:2001 *E - Signature Creation Applications and Procedures for Electronic Signature Verification;*

9.3.10.5 CWA 14172-5:2001 *E - Secure signature creation devices*.

9.3.10.6 Additionally, the following further parts are under consideration, but no formal commitment has yet been made to their development:

CWA 14172-5: wip *Secure signature creation devices (for Qualified Certificates);*
CWA 14172-6: wip *Certification Authority services and processes (for non-Qualified certificates);*
CWA 14172-7: wip *Secure signature creation devices (for non-Qualified Certificates;*
CWA 14172-8: wip *Time-Stamping Authorities;*
CWA 14172-9: wip *Cryptographic Modules for CSP Signing Operations.*

9.3.11 CWA 14365: wip *Guide on the Use of Electronic Signatures*

This CWA will address general signatures that do not fall within the specific requirements laid down for qualified signatures in [Dir.1999/93]. The CWA therefore analyses the differences between cryptographic mechanism of digital signatures, qualified electronic signatures (according to [Dir.99.93]), and general electronic signatures (generally those which are not addressed by specific requirements within [Dir.1999/93]). The CWA is aimed mainly at e-commerce scenarios with a high deployment capability. Guidance is given on the requirements in different use cases. Subsequently, a more relaxed Protection Profile for a general signature creation device for this type of use is introduced. In addition, electronic signatures and certification-services are broken up into their basic elements and the proof provided by each element is discussed from a legal perspective in order to establish the coherence between the technical elements and their legal effect.

9.4 ETSI Technical Standards and Technical Reports

The European Telecommunications Standards Institute (ETSI) develops its standards through the

Technical Committee – Electronic Signatures and Infrastructure (ESI), through the operation of an open workshop 'ESI'. The principal documents produced are Technical Standards (TS) and a fewer number of Technical Reports (TR) which establish requirements on which some TS documents are founded. Further details can be located at http://www.etsi.org/sec/el-sign.htm (click on Electronic Signatures and Infrastructures). All of the following documents can be downloaded free of charge, after initially registering.

9.4.1 ETSI TS 101 456:ver. 1.2.1 - *Policy requirements for Certification Authorities issuing Qualified Certificates*[1]

This ETSI Technical Specification defines security management and policy requirements for certification authorities (CAs) issuing qualified certificates. It defines 2 specific policies for:

(a) CAs issuing Qualified Certificates to the public

(b) CAs issuing Qualified Certificates to the public requiring use of a Secure Signature Creation Device.

In addition, it defines a general framework for other policies for CAs issuing qualified certificates including those applicable to closed communities. By conforming to this policy the CA indicates to the certificate users that:

(a) it meets the requirements of specific annexes within [Dir.1999/93], as well as, depending on the policy implemented, that: the certificate is covered by the liability provisions for certificates issued to the public, as defined in [Dir.1999/93],

(b) the certificate authenticates a subscriber who is using an Secure Signature Creation Device as defined in [Dir.1999/93].

Through use of the appropriate policy option CAs can assure users that an electronic signature meets all the requirements of [Dir.1999/93], including being covered by its liability provisions.

This TS provides a common policy baseline for CSPs issuing Qualified Certificates, thereby leading to the establishment of a quality CSP infrastructure for electronic signatures across Europe (and potentially beyond) and so providing an essential component for electronic commerce.

9.4.2 ETSI TS 102 042:ver. 1.1.1 *Policy requirements for certification authorities issuing public key certificates*

This ETSI Technical Specification is based on, and adopts the same structure and approach as, ETSI TS 101 456, but is applicable to the general requirements of certification in support of cryptographic mechanisms, including other forms of electronic signature, as well as the use of cryptography for authentication and encryption. The specification establishes a set of requirements which allow the achievement of the same level of quality as in the issuance of Qualified Certificates (as addressed specifically by ETSI TS 101 456) but in a "normalised" form of expression, allowing for wider applicability and for ease of alignment with other similar specifications and standards from other sources and institutions. By this approach, harmonisation of the quality level established by [Dir.1999/93] can become embodies more readily into other widely recognised and accepted specifications. The specification also allows for certain options based upon the normalised certificate policy.

9.4.3 ETSI TS 102 023:ver. 1.1.1 *Policy requirements for time-stamping authorities*

This ETSI Technical Standard specifies policy requirements relating to the operation of Time-

[1] The term 'Qualified Certificate' has specific meaning as defined in the referred EC Directive, [Dir.1999/93].

stamping Authorities (TSAs). It addresses requirements on the operation and management practices of TSAs such that subscribers and relying parties may have confidence in the operation of time-stamping services. These policy requirements are primarily aimed at time-stamping services used in support of qualified electronic signatures (as required by [Dir.1999/93]), but they may be applied to any application requiring proof that a specific datum existed at a particular time

9.4.4 ETSI TR 102 041:ver. 1.1.1 *Signature Policies Report*
This ETSI Technical Report gives guidance on the technical, organisational and legal issues related to a signature policy. Its readership will gain the best understanding of it by first reading ETSI TS 101 733, upon which this report builds.

9.4.5 ETSI TR 102 045:ver. 1.1.1 *Signature policy for extended business model*
This ETSI Technical Report will elaborate on the signature policy concept, address certain aspects of multiple. There is a need to address specific trade transactions, such as the UN Trade Transactions Model or *ad hoc* models, such as the notary example etc. where multiple (i.e. more than one) signatures are used. The report will focus on the implications of signature policies in various types of transactions or unilateral declarations. This will include consideration of the roles, documents used, formalities, and relationships (e.g. concurrency and their implications in multiple signatures) during the signing process. On the basis of this work the report will evaluate the circumstances of the policy's application and, if necessary, propose specific extensions to the standard (ref. ETSI TS 101 733) and the corresponding RFC.

9.4.6 ETSI TS tba: ver. wip *Signature Policies*
Following the publication of a sample signature policy in ETSI TS 101 733, ETSI has produced or is in the process of preparing a number of technical reports on signature policies:

(a) **ETSI TR 102 041** Signature Policies Report;
(b) **ETSI TR 102 045** Signature policy for extended business model;
(c) **ETSI TR 102 038** XML Format for Signature Policies.

These reports will establish the basis of requirements for the production of this Technical Specification which will include the policies for multiple signatures and countersignatures.

9.4.7 ETSI TR 102 044: ver. wip *Policy requirements for attribute authorities*
This ETSI Technical Report will review emergent practices for certifying roles and attributes, such as; Attribute Certificate standards from the IETF, using extensions to existing authentication certificates, and others. Such practices may be used to support the notion of roles within an organisation or professional roles. The report will consider these issues in light of the implications of the requirements of [Dir.1999/93], and present a set of conclusions and recommendations based on findings.

9.4.8 ETSI TS tba: ver. wip *Policy requirements for CSPs issuing attribute certificates*
This ETSI Technical Standard will provide requirements for the management of attribute and role certification services. The standard will draw upon the findings of ETSI TR 102 044 and will also, for its structure and some of the contents, draw upon ETSI TS 101 456.

9.4.9 ETSI TR 102 030: ver 1.1.1 *Provision of harmonised TSP status information*
The ETSI Technical Report defines minimum requirements for the provision of harmonised status information on certification-service-providers and other Trust Service Providers (TSPs) and for the means to provide such information. It defines a preliminary data structure for the management and presentation of such information, referred to as a Trust Status List. The

requirements will be used as the starting point for the development of an ETSI Technical Standard.

9.4.10 ETSI TS tba: ver wip *Provision of harmonised TSP status information*
This ETSI Technical Specification will take as its basis the findings of ETSI TR 102 030, above) and develop a standard fore the management and presentation of a Trust Status List which will allow interoperable provision of TSP status information to relying parties and others who need to establish the status of a trust service, including specifically to validate its trustworthiness at the time the service was rendered.

9.4.11 ETSI TS 101 862: ver. 1.2.1 *Qualified certificate profile*
This ETSI Technical Specification defines how the X.509 public key certificate format, which dominates the public key infrastructure market, may be used to meet the requirements of [Dir.1999/93].In addition, where there is currently no defined X.509 mechanism for meeting any requirement of [Dir.1999/93] the specification builds on the existing extension capabilities of X.509 to define the necessary optional data structures.

Through use of this document parties relying on Qualified Certificates can maximise the ability to verify signatures supported by Qualified Certificates issued by different CAs. Through use of this standard the technical interoperability between CAs, signature creation and signature verification applications is significantly improved, thereby maximising the openness of the electronic market.

By building on a standard that is already widely adopted (X.509) this specification has minimised the cost to suppliers of implementing [Dir.1999/93].

9.4.12 ETSI TS 101 861: ver. 1.2.1 *Time stamping profile*
This ETSI Technical Specification defines how the Internet specification for time-stamping may be used to support advanced electronic signatures to provide long term validity as defined in ETSI TS 101 733. Through use of this specification the interoperability between applications requiring long-term validity of electronic signatures and CSPs providing time-stamping services has been maximised

9.4.12 ETSI TS 101 733: ver. 1.3.1 *Electronic signature formats*
This ETSI Technical Specification defines a format for advanced electronic signatures based on the existing standard format that dominates the e-mail and document security market (i.e. CMS – Internet specification RFC 2630). It also specifies how time-stamping or trusted archiving services may be used to ensure that the electronic signature remains valid for long periods so that it can be later presented as evidence in the case of a dispute.

This specification may be used either for qualified electronic signatures, when used in conjunction with Qualified Certificates and Secure Signature Creation Devices as defined in [Dir.1999/93], or for other forms of electronic signature as recognised by [Dir.1999/93], which need to be presented as reliable evidence some time after they were created.

This document defines how the Internet specification RFC 2630 cryptographic message syntax should be used for advanced electronic signatures and defines additional fields and procedures, which are compatible with this syntax, to support long term validity. The evidence provided through use of the ETSI format protects against the signatory later repudiating having signed a document, since the signature can be verified even after the expiry of the validity of the supporting certificate.

Through use of this specification and the different optional syntaxes available for the extra assurance required for long-term validity, the interoperability between signature creation and

signature verification applications is significantly improved, thereby maximising the openness of the electronic market. Also, by building on a standard that is already widely adopted (ITU-T standard X.509) this specification has minimised the cost of electronic signatures that have long term validity.

9.4.13 ETSI TR 102 038: ver. 1.1.1 *XML format for signature policies*

This ETSI Technical Report presents a first version of an XML format for Signature Policies able to hold information on Signature Polices as specifies by ETSI TS 101 733. As a preliminary effort in this field, the report raises a number of open issues as a basis for discussion, and possibly for subsequent definition. It is anticipated that subsequent revisions of this report will make gradual improvement in the use of new XML types defined, aligning them with broader efforts in the XML arena

9.4.14 ETSI TS 101 903: ver. 1.1.1 *XML Advanced Electronic Signatures (XadES)*

This ETSI Technical Standard covers electronic signatures for various types of transactions, including business transactions (e.g. purchase requisition, contract and invoice applications). The standard is intended to be applicable to any type of transaction, i.e. citizen – business, business – business, citizen / business – government, etc. The standard has been developed in close liaison with the W3C, to allow easy insertion into the W3C framework for XML digital signatures

10 US NATIONAL COMPUTER SECURITY CENTRE

10.1 Rainbow series Standards

The Rainbow Series is set of books on evaluating "Trusted Computer Systems" according to the National Security Agency. The term "Rainbow Series" stems from the fact that each book is a different color. The main book (upon which all other expound) is the Orange Book. Note that many of these documents have been superseded.
(Available from **http://www.fas.org/irp/nsa/rainbow.htm)**

10.1.1 CSC-STD-001-83: Trusted Computer System Evaluation Criteria, (*TCSEC)*

10.1.1.1

The “Orange” book. Although now replaced by the ISO/IEC 15408 Common Criteria series, the Trusted Computer System Evaluation Criteria were developed for a number of reasons. They provide users with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information.

10.1.1.2

They provide guidance to manufacturers as to what security features to build into their new and planned, commercial products in order to provide widely available systems that satisfy trust requirements. They also provide a basis for specifying security requirements in acquisition specifications.

10.1.2 CSC-STD-002-85: *Password Management Guidelines*

The security provided by a password system depends upon the passwords being kept secret at all times. In a password based authentication system, the passwords are vulnerable to compromise due to five essential aspects of the password system: a password must be initially assigned to a user; a password must be changed periodically; a password database must be retained on the host system; users must remember their passwords; and users must enter their

password at authentication time. This guideline prescribes the steps to be taken to minimise the vulnerability of passwords in each of these circumstances.

10.1.3 CSC-STD-003-85: *Guidance for applying TSEC in specific environments*
This publication provides guidance for specifying computer security requirements for the US Department of Defense by calculating a risk index and identifying the minimum class of system required for that risk index.

10.1.4 CSC-STD-004-85: *Technical Rationale Behind CSC-STD-003*
The purpose of this standard is to present background discussion and rationale for the computer security requirements stated in CSC-STD-003. This document presents the method used to calculate the minimum security requirements for each environment, and a metric for categorising systems according to the security protection they require.

10.1.5 CSC-STD-005-85: *Magnetic Remanence Security Guideline*
It is important that computer personnel be aware of the retentive properties of magnetic storage media, and be aware of the known risks in erasing and/or releasing such media. This document provides approved security procedures that help avoid disclosure of sensitive information.

10.2 Rainbow Series Technical Guides

10.2.1 NCSC-TG-001: *A Guide to understanding Audit in Trusted Systems*
The TCSEC requires that a user's actions in a trusted system be open to scrutiny by means of an audit. The audit process of a secure system is the process of recording, examining, and reviewing any or all security-relevant activities on the system. This guideline is intended to discuss the issues involved in implementing and evaluating an audit mechanism.

10.2.2 NCSC-TG-002: *Trusted Product Evaluations - A Guide for Vendors*
This publication provides a guide for vendors on the evaluation processes and requirements for trusted systems.

10.2.3 NCSC-TG-003: *A guide to Understanding Discretionary Access Control*
One of the features required in a trusted system is the enforcement of discretionary access control (DAC). This is a means of restricting access to objects based on the identity of users. The controls are discretionary in the sense that access is not predetermined, but is at the discretion of a security authority. This guideline discusses the issues involved in designing, implementing, and evaluating a DAC feature.

10.2.4 NCSC-TG-004: *Glossary of Computer Security Terms*
This document provides a glossary of computer security terms used in the various NCSC documentation.

10.2.5 NCSC-TG-005: *Trusted Network Interpretation (TNI) of the TSEC*
This document provides an interpretation of the TCSEC for trusted computer/communications network systems. The specific security features, the assurance ratings, and the rated structure of the TCSEC are extended to networks of computers ranging from local area networks to wide area inter-networking systems. A number of additional security services (communications integrity, denial of service, transmission security) are described.

10.2.6 NCSC-TG-006: *A Guide to Understanding Configuration Management*
Configuration management procedures are used to establish baseline configurations and manage changes to systems. This guideline discusses the concepts of configuration management and how it applies to computer systems to support the control, accounting, and auditing of all changes made to the security-relevant aspects of a trusted system.

10.2.7 NCSC-TG-007: *A Guide to Understanding Design Documentation in Trusted Systems*
This publication provides a statement of the requirements of design documentation necessary for the formal evaluation of a trusted system by the NCSC for inclusion on the Evaluated Products List.

10.2.8 NCSC-TG-008: *A Guide to Understanding Trusted Distribution*
Trusted distribution of the hardware, firmware, and software of a trusted system is a requirement of the TCSEC. Trusted distribution includes procedures to ensure all configuration items distributed to a customer site arrive exactly as intended by the vendor without any alterations. Also included may be procedures that enable the customer site to confirm correct receipt. This guideline provides advice to vendors of trusted systems on what trusted distribution is, its importance, and how to select and implement an effective trusted distribution system.

10.2.9 NCSC-TG-009: *Computer Security Subsystem Interpretation of the TSEC*
This document provides an interpretation of the TCSEC for computer security subsystems such as a third party security module.

10.2.10 NCSC-TG-010: *A Guide to Understanding Security Modeling*
This document gives guidance on the construction, evaluation, and use of security policy models for automated information systems used to protect sensitive information whose unauthorized disclosure, alteration, loss, or destruction must be prevented. The guideline is intended to give vendors and evaluators of trusted systems a solid understanding of the modeling requirements of the Trusted Computer System Evaluation Criteria and the Trusted Network Interpretation.

10.2.11 NCSC-TG-011: *Trusted Network Interpretation Environments Guideline*
This document provides an environmental assessment process that helps determine the minimum level of trust recommended for specific network operational environments. The primary focus of the document is on the hardware, firmware, and software aspects of security for the network. The document also includes a tutorial on network security, discusses the cascade condition, and reviews encryption and encryption mechanisms.

10.2.12 NCSC-TG-012
This standard is not currently identified.

10.2.13 NCSC-TG-013: *The Rating Maintenance Phase (RAMP)*
This document describes the process of updating an evaluation rating as new versions of evaluated products are developed, to avoid the time and cost involved in a full evaluation.

10.2.14 NCSC-TG-014: *Guidelines for Formal Verification Systems*
This document explains the requirements for formal verification systems that are candidates for the NCSC's Endorsed Tools List and is primarily intended for developers of verification systems to use in the development of trusted systems.

10.2.15 NCSC-TG-015: *A Guide to Understanding Trusted Facility Management*
This guideline presents the issues involved in the design of trusted facility management. It covers the inherent vulnerabilities of the administrative roles, the TCSEC requirements for trusted facilities management, and the need for separation between the administration and operations functions.

10.2.16 NCSC-TG-016: *Guidelines for Writing Trusted Facility Manuals*
This document provides details of what should be in a trusted facility manual, including the requirements for configuration and installation of a secure system, secure system operations, management of system privileges and protection mechanisms, and control of administrative functions. The document is intended for the developer of a trusted facility manual.

10.2.17 NCSC-TG-017: *A Guide to Understanding Identification and Authentication in Trusted Systems*
This document provides guidance to vendors on how to design and incorporate effective identification and authentication mechanisms into their systems. It is also written to help vendors and evaluators understand the requirements of identification and authentication.

10.2.18 NCSC-TG-018: *A Guide to Understanding Object Reuse*
This document is written to help vendors and evaluators understand the object reuse requirement of the TCSEC. It also provides guidance to vendors on how to design and incorporate effective object reuse mechanisms into their systems.

10.2.19 NCSC-TG-019: *Trusted Product Evaluation Questionnaire*
The purpose of this document is to assist system developers and vendors in gathering the data required for a formal product evaluation under the TCSEC. The document provides evaluators with an understanding of the various hardware, and software configurations, architectures and their ability to support trusted computing base isolation, non-circumventability, and covert channel analysis.

10.2.20 NCSC-TG-020-A: *Rationale for Selecting UNIX Access Control List Features*
This document discusses the rationale for the recommendations of the Trusted UNIX Working Group with respect to the requirements of Access Control Lists in trusted UNIX systems. The document discusses the selections, gives details of each of the requirements, and provides a worked example.

10.2.21 NCSC-TG-021: *Trusted Database Interpretation (TDI) of TSEC*
This document provides an interpretation of the TCSEC for database systems in order to provide manufacturers with a standard for security features that can be built into their commercial database products to satisfy trust requirements for applications handling sensitive data.

10.2.22 NCSC-TG-022: *A Guide to Understanding Trusted Recovery*
This document provides a set of good practices related to the recovery of a trusted system after a system failure. This document is intended for vendors and evaluators to understand the requirements for trusted recovery, and the evaluation requirements of the design and implementation of trusted recovery schemes.

10.2.23 NCSC-TG-023: *A Guide to Understanding Security Testing and Test Documentation*
This document provides a set of good practices related to security testing and the development of test documentation. It is intended to assist with developing tests that can determine the adequacy

of system security mechanisms and assess the degree of consistency between such mechanisms and their associated documentation.

10.2.24 NCSC-TG-024: *A Guide to Procurement of Trusted System***s**

This four volume document provides the procurement initiator, i.e. the Program manager, user, or Security Manager, with guidelines on writing Request for Proposals (RFPs) relating to trusted systems. The document is intended to facilitate the contacting process, provide uniformity in competitive acquisitions, minimise procurement cost and risk, avoid delays in the solicitation process, and help ensure the solicitation process is complete before its issuance.

10.2.25 NCSC-TG-025: *A Guide to Understanding Data Remanence*

Data remanence is the residual physical representation of data that has been in some way erased. This document discusses the security aspects related to data remanence in the reuse and release of storage media.

10.2.26 NCSC-TG-026: *A Guide to Writing the Security Features User Guide*

This guideline identifies and discusses the considerations that influence the development and evaluation of a security features user's guide. It is intentionally descriptive as opposed to prescriptive.

10.2.27 NCSC-TG-027: *A Guide to Understanding Information Systems Security Officer's Responsibilities for Automated Information Systems*

This guideline identifies the system security responsibilities of Information System Security Officers (ISSOs). While the guide emphasises computer security, it is important to ensure that other aspects of security are also addressed in organizational policies and procedures in support of the ISSO.

10.2.28 NCSC-TG-028: *Assessing Controlled Access Protection*

The objectives of this guideline are to provide a methodology for performing a technical analysis to support the certification of controlled access in systems submitted for evaluation, to provide an approach for achieving its protection, and to clarify the intent, security functionality, and level of protection that controlled access provides.

10.2.29 NCSC-TG-029: *Introduction to Certification and Accreditation Concepts*

The purpose of this document is to discuss the high level certification and accreditation process and its relationship to risk analysis. The document also clarifies the roles the Departmental Accreditation Authority and key security officials play in the certification and accreditation process.

10.2.30 NCSC-TG-030: *A Guide to Understanding Covert Channel Analysis*

This publication provides guidance to vendors and evaluators on how to identify covert channels, assess their maximum attainable bandwidth, and how to handle them in a well defined security policy. It presents the relative merits of various covert channel analysis methods and defines the type of evidence required for assurance evaluation.

11 OTHER STANDARDS

11.1 Institute of Electrical and Electronic Engineers

11.1.1 IEEE 802.10: *Standards for interoperable LAN/MAN Security (SILS) and supplements: Key Management (Clause 3), IEEE Std 802.10c-1998 Security Architecture Framework (Clause 1), IEEE Std 802.10a-1999*

11.1.1.1

This standard describes an OSI Layer 2 security protocol that can be used to protect IEEE 802 Local Area Networks (LANs) and Metropolitan Area Networks (MANs). The standard allows confidentiality and connectionless integrity and, in conjunction with key management support, can also provide data origin authentication and access control. IEEE 802.10 uses the Secure Data Exchange (SDE) entity as the foundation for security services. The IEEE 802.10 SDE service operates within the IEEE 802.2 Logical Link Control (LLC) sub-layer, and provides a connectionless service immediately above the Medium Access Control sub-layer in the various 802 LANs and MANs.

11.1.2 IEEE 802.11: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*

This standard defines the protocol and compatible interconnection of data communication equipment via the“air”, radio or infrared, in a local area network (LAN) using the carrier sense multiple access protocol with collision avoidance (CSMA/CA) medium sharing mechanism. The medium access control (MAC) supports operation under control of an access point as well as between independent stations. The protocol includes authentication, association, and re-association services, an optional encryption/decryption procedure, power management to reduce power consumption in mobile stations, and a point coordination function for time-bounded transfer of data.

11.2 European Computer Manufacturers’ Association

11.2.1 ECMA TR/46: *Security in Open Systems*

This report provides an overview of security needs and of the basic functionality needed to answer these needs. Using a generic building block approach, it shows how supportive security applications may be constructed to satisfy a wide range of uses. The standard is based on the Security Domain and Security facilities concepts, and shows how these concepts map to other architectures such as the OSI Reference Model and the ECMA Distributed Office Applications Framework.

11.2.2 ECMA 205: *Commercially-oriented Functionality Class for Security Evaluation*

11.2.2.1

The objective of this ECMA Standard is to define a widely accepted basic security functionality class for the commercial market. It is articulated in a structured way consistent with TCSEC, ITSEC and MSFR concepts. Readers unfamiliar with security and these concepts are encouraged to read TCSEC, ITSEC and MSFR if they wish to understand fully this text.

11.2.2.2

This standard addresses only IT security. Other security areas like personnel security, physical security and procedural security are not covered. This standard defines a basic functionality class for the commercial market. It addresses multi-user, stand-alone IT-systems without considering networking or remote access. Multi-processor systems however are covered as long as a single

system image is provided.

11.2.3 ECMA 206: *Association Context Management, including Security Context Management*

11.2.3.1
This Standard defines a model for management of the characteristics of associations between applications in a distributed system. The associations can be for interactive (e.g. VT) and non-interactive (e.g. FTAM) applications. It is also a framework to provide achievement of availability, integrity and confidentiality of an association, and defines an Association Context Information Model which is the “language” to manage the characteristics of associations.

11.2.3.2
The standard defines Service and Protocol for association context management that meets the requirements for a Secure Association Service as defined in Standard ECMA-138. It maps association management to a (non-exclusive) set of application layer protocols: ACSE, ROSE, OSI-RPC.

11.2.3.3
ECMA-206 is security policy independent, e.g. an association might be either application- or system-initiated. It supports associations across multiple domains. The field of application of this ECMA Standard is the design and implementation of distributed open systems that support access of users to applications and access between distributed applications.

11.3 RSA - Public Key Cryptography Standards

(Available from http://www.rsasecurity.com)

11.3.1 PKCS #1: *RSA Encryption and Signature*
PKCS #1 describes a method, called RSA Encryption, for encrypting data using the RSA public-key cryptosystem. Its intended use is in the construction of digital signatures and digital envelopes, as described in PKCS #7. also describes a syntax for RSA public keys and private keys. The public-key syntax would be used in certificates; the private-key syntax would be used typically in encrypted private keys (PKCS #8).

11.3.2 PKCS #3: *Diffie-Hellman*
PKCS #3 describes a method for implementing Diffie-Hellman key agreement, whereby two parties, without any prior arrangements, can agree upon a secret key that is known only to them (and, in particular, is not known to an eavesdropper listening to the dialogue by which the parties agree on the key). This secret key can then be used, for example, to encrypt further communications between the parties. The intended application of PKCS #3 is in protocols for establishing secure connections, such as those proposed for OSI’s transport and the network layers [ISO/IEC90a][ISO/IEC90b].

11.3.3 PKCS #5: *Password-based Encryption*

11.3.3.1
PKCS #5 describes a method for encrypting an octet string with a secret key derived from a password. The result of the method is an octet string. Although PKCS #5 can be used to encrypt arbitrary octet strings, its intended primary application to public-key cryptography is for encrypting private keys when transferring them from one computer system to another, as described in PKCS #8.

11.3.3.2
PKCS #5 defines two key-encryption algorithms: pbeWithMD2AndDES-CBC and pbeWithMD5AndDES-CBC. The algorithms employ DES secret-key encryption in cipher-block chaining mode, where the secret key is derived from a password with the MD2 or MD5 message-digest algorithm.

11.3.4 PKCS #6: *Extended Certificate Syntax*

11.3.4.1
PKCS #6 describes a syntax for extended certificates. An extended certificate consists of an X.509 public-key certificate and a set of attributes, collectively signed by the issuer of the X.509 public-key certificate. Thus the attributes and the enclosed X.509 public-key certificate can be verified with a single public-key operation, and an ordinary X.509 certificate can be extracted if needed, e.g., for Privacy-Enhanced Mail.

11.3.4.2
The intention of including a set of attributes is to extend the certification process beyond just the public key to include other information about a given entity, such as electronic-mail address. A non-exhaustive list of attributes is given in PKCS #10.

11.3.4.3
The preliminary intended application of PKCS #6 is in the cryptographic-enhancement syntax standard (PKCS #7), but it is expected that other applications will be developed.

11.3.5 PKCS #7: *Cryptographic Message Syntax*

11.3.5.1
PKCS #7 describes a general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes. The syntax admits recursion, so that, for example, one envelope can be nested inside another, or one party can sign some previously enveloped digital data. It also allows arbitrary attributes, such as signing time, to be authenticated along with the content of a message, and provides for other attributes such as countersignatures to be associated with a signature. A degenerate case of the syntax provides a means for disseminating certificates and certificate-revocation lists.

11.3.5.2
PKCS #7 is compatible with Privacy-Enhanced Mail (PEM) in that signed-data and signed-and-enveloped-data content, constructed in a PEM-compatible mode, can be converted into PEM messages without any cryptographic operations. PEM messages can similarly be converted into the signed-data and signed-and-enveloped data content types.

11.3.5.3
PKCS #7 can support a variety of architectures for certificate-based key management, such as the one described for Privacy-Enhanced Mail in RFC 1422. Architectural decisions such as what certificate issuers are considered “top-level,” what entities certificate issuers are authorized to certify, what distinguished names are considered acceptable, and what policies certificate issuers must follow (such as signing with secure hardware, or requiring entities to present specific forms of identification) are left outside PKCS #7. Dissemination of “hot lists” of invalid certificates (certificate-revocation lists) is also left outside.

11.3.6 PKCS #8: *Private Key Information Syntax*

11.3.6.1
PKCS #8 describes a syntax for private-key information. Private-key information includes a private key for some public-key algorithm and a set of attributes. PKCS #8 also describes a syntax for encrypted private keys. A password-based encryption algorithm (e.g., one of those described in PKCS #5) could be used to encrypt the private-key information.

11.3.6.2
The intention of including a set of attributes is to provide a simple way for a user to establish trust in information such as a distinguished name or a top-level certification authority's public key. While such trust could also be established with a digital signature, encryption with a secret key known only to the user is just as effective and possibly easier to implement. A non-exhaustive list of attributes is given in PKCS #9.

11.3.7 PKCS #9: *Selected Attribute Syntaxes*
PKCS #9 defines selected attribute types for use in PKCS #6 extended certificates, PKCS #7 digitally signed messages, and PKCS #8 private-key information.

11.3.8 PKCS #10: *Certificate Request Syntax*

11.3.8.1
PKCS #10 describes a syntax for certification requests. A certification request consists of a distinguished name, a public key, and optionally a set of attributes, collectively signed by the entity requesting certification. Certification requests are sent to a certification authority, who transforms the request to an X.509 public-key certificate, or a PKCS #6 extended certificate.

11.3.8.2
The intention of including a set of attributes is twofold: to provide other information about a given entity, such as the postal address to which the signed certificate should be returned if electronic mail is not available, or a "challenge password" by which the entity may later request certificate revocation; and to provide attributes for a PKCS #6 extended certificate. A non-exhaustive list of attributes is given in PKCS #9.

11.3.8.3
Certification authorities may also require non-electronic forms of request and may return non-electronic replies. It is expected that descriptions of such forms, which are outside the scope of PKCS #10, will be available from the certification authority.

11.3.9 PKCS #11: *Abstract Token Interface*
Otherwise known as Cryptoki, this standard defines the interface for tokens, such as PCMCIA and Smart Cards, when used as a cryptographic subsystem. Note that Amendment 1 is also available.

11.3.10 PKCS #13: *Elliptic Curve Cryptography Standard*
A new document being developed by RSA Laboratories as part of its Public-Key Cryptography Standards (PKCS) series, covering public-key techniques based on elliptic curve cryptography. Elliptic curve cryptography has emerged as a promising new branch of public-key cryptography in recent years, due to its potential for offering similar security to established public-key cryptosystems at reduced key sizes. Improvements in various aspects of implementation, including the generation of elliptic curves, have made elliptic curve cryptography more practical than it was when first introduced in the 1980's. As security of elliptic curve cryptography becomes

better understood, an opportunity is available is develop standards for this technology, thereby promoting interoperability at the same time as implementations are being deployed.
Standards efforts for elliptic curve cryptography are already underway. X9.F.1, an ANSI-accredited standards committee for the financial services industry, is developing two standards: ANSI X9.62 for digital signatures and ANSI X9.63 for key agreement and key transport. IEEE P1363 is working on a general reference for public-key techniques from several families, including elliptic curves. PKCS #13 will complement the others, providing a profile of the other standards in the PKCS format and giving guidance for incorporating elliptic curve cryptography into other PKCS # based applications such as those based on PKCS #11 or PKCS #7

11.3.11 PKCS #15: *Cryptographic Token Information Format Standard Background*
It is widely recognized that cryptographic tokens such as Integrated Circuit Cards (ICCs or Smart Cards) offer a great potential for secure identification of users of information systems. But if this potential is ever going to be fully realized, and users are to receive full benefit of these tokens, there is an obvious requirement of credential portability and interoperability.
Interoperability demands standardization, and this document, PKCS #15, is intended at establishing a standard which ensure that users in fact will be able to use cryptographic tokens to identify themselves to multiple, standards-aware applications, regardless of the application's cryptoki (or other token interface) provider.

11.4 Microsoft Cryptographic Application Programmers Interface

The Microsoft Cryptographic Application Programmers Interface (M-CAPI) provides a specification of the interfaces from standard Microsoft applications to cryptographic services provided by a Cryptographic Service Provider.

11.5 Visa/Mastercard – Secure Electronic Transactions

The Secure Electronic Transaction standard is a specification for electronic financial transactions developed by a consortium including VISA, Mastercard, and Microsoft. It defines the use of asymmetric cryptography to protect transactions, details the certificate extensions employed, and provides transaction specifications.

12 STANDARDS OF NATIONAL BODIES

12.1 AS 2805: *Electronic funds transfer – Requirements for interfaces,*
A collection of documents in 14 parts and further subsections.

AS 2805.1 *Communications*
AS 2805.2 *Message structure, format and content*
AS 2805.3 *PIN management and security*
AS 2805.4 *Message authentication*
AS 2805.5 *Cyphers*
Part 1 Data encipherment algorithm 2
Part 2 Modes of operation for an n-bit block cipher algorithm
Part 3 Data encipherment algorithm 2 (DEA 2)
Part 4 Ciphers - Data encipherment algorithm 3 (DEA 3) and related techniques
AS 2805.6 *Key management*
Part 1 Principles
Part 2 Transaction keys
Part 3 Session keys - Node to node
Part 4 Session keys- Terminal to acquirer

Part 5 TCU Initialisation
Part 5.1 Principles
Part 5.2 Symmetric
Part 5.3 Asymetric

AS 2805.7 *Message content*
AS 2805.8 *Financial institution message content*
AS 2805.9 *Privacy of communications*
AS 2805.10 *File transfer integrity validation*
AS 2805.11 *Card parameter table*
AS 2805.12 *Message content*
Part 1 Structure and format
Part 2 Codes
Part 3 Maintenance of codes
AS 2805.13 *Secure hash functions*
Part 1 General
Part 2 MD5
Part 3 SHA-1
AS 2805.14 *Secure cryptographic devices (retail)*
Part 1 Concepts, requirements and evaluation methods

12.2 NZS 6656: *Implementation and Operation of a Trustworthy Computer System*
This standard specifies security requirements for use where a contract between two parties requires the demonstration of a supplier's capability to implement and/or operate a computer system, such as in an outsourcing arrangement, which enforces information confidentiality, integrity, and availability. It applies equally to system acquisition, where the two parties are the system purchaser and the supplier; to facilities management, where the two parties are the system owner and the facilities management; or internal provision of systems and services, where the two parties are the organization's business units and the organization's data processing unit.

12.3 BS 7799.2: *Specification for information security management systems*
Specifies the requirements for establishing, implementing and documenting information security management systems (ISMSs) and the requirements for security controls to be implemented according to the needs of individual organisations.

12.4 SNZ HB 8169 *Health network Code of Practice*
Describes how healthcare organisations can safely exchange electronic health information over a secure network intended for this purpose.

13 LINKS TO WEBSITES

13.1 These sites do not provide Standards per se, but the information presented is frequently of considerable interest to the Security professional.

13.1.1: SANS (The System Administration, Networking and Security Institute): www.sans.org. A respected source of security-related information and training.

13.1.2: CERT/CC (Computer Emergency Response Team/Co-ordination Centre): www.cert.org. The original CERT operation.

13.1.3: SecurityFocus/Bugtraq (www.securityfocus.org). One of the best-known sources of information on bugs and vulnerabilities in Internet-related systems.

13.1.4: SecurityPortal (www.securityportal.org). A portal site to a large range of other security-related sites.

13.1.5: Center for Internet Security (www.cisecurity.org). A global, cooperative initiative involving industry, government, and research leaders to establish basic operational security benchmarks.

13.1.6: International Information Systems Security Certification Consortium Inc. (ISC2) (www.isc2.org). An international not-for-profit consortium best known for its CISSP (Certified Information Systems Security Professional) qualification.

APPENDIX A

VOCABULARY
(Informative)

A.1 Information security definitions

This section is based on the definitions listed in Standing Document 6 of the ISO/IEC Joint Technical Committee 1, Sub-Committee 27 (JTC1/SC27) and ISO/IEC 2382.8. It is included to provide a ready reference which may assist the reader of the main body of the document. It is accepted that there may be other definitions available.

Access control
The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

Access control list
A list of entities, together with their access rights, which are authorized to have access to a resource.

Access level
The level of authority required by an entity to access a resource.

Access right
Permission for an entity to access a particular resource for a specific operation.

Accountability
The property that ensures that the actions of an entity may be traced uniquely to the entity.

Accreditation agent
A person responsible to the accreditation authority for the inspection of a system to ensure it is implemented and operating in compliance with its stated security policy.

Accreditation authority
The entity responsible for authorizing the operation of a system upon submission of evidence that the system is secure.

Active threat
The threat of a deliberate unauthorized change to the state of a system.

Adjudicator
A judge or arbiter capable of resolving disputes by evaluating evidence against a non-repudiation policy.

Appendix
A data item added to a message consisting of a digital signature and other optional information.

Asset
Anything that has value to an organization. This may be tangible, such as computer equipment or software, or intangible, such as information.

Assignment
A data item, which is a function of the witness and possibly part of a message, and which forms part of the input to a digital signature function.

Asymmetric authentication method
A method of authentication in which not all authentication information is shared by both entities.

Asymmetric cryptographic technique
A cryptographic technique that uses two related transforms, a public transform (defined by the public key) and a private transform (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.

Asymmetric encipherment system
A system based on asymmetric cryptographic techniques whose public transformation is used for encipherment and whose private transformation is used for decipherment.

Asymmetric key pair
A pair of related keys where the private key defines the private transformation and the public key defines the public transformation.

Asymmetric signature system
A system based on asymmetric techniques whose private transformation is used for signing and whose public transformation is used for verification. This may or may not use the same asymmetric key pair, depending upon the asymmetric cryptographic technique.

Audit attribute
A piece of information about an audit event or about one of the subjects or objects involved in an event.

Audit description
A part of an audit record that describes one of the subjects and/or objects involved in the audit event.

Audit event
An action, detected internally by the system, which may generate an audit record. If an event causes an audit record to be generated, it is a recorded event, otherwise it is an unrecorded event. The system decides, as each event is detected, whether to generate an audit record by the audit pre-selection algorithm. The set of audit events is based upon a system's security policy.

Audit event class
A way of characterising auditable events into groups on the basis of audit event types. An audit event type may belong to more than one audit event class.

Audit post-selection
The process by which the auditor selects records from the audit trail for analysis. Post-selection provides the auditor with flexibility in selecting records.

Audit pre-selection
The process by which the system decides whether to generate an audit record for a particular

occurrence of an auditable event. Pre-selection provides the auditor with a means of reducing the volume of audit records generated while still generating those records that are important for analysis.

Audit record
The discrete unit of data recorded in the audit trail on the occurrence of a recorded event. An audit record consists of a set of audit descriptions, each of which has a set of audit attributes associated with it. Every audit record always has an audit description for the record's header, and usually has additional audit descriptions describing the subject(s) and object(s) involved in the event.

Authenticated entity
A distinguishing identifier of a principal that has been assured through authentication.

Authentication
The assurance that the claimed identity of an entity is correct.

Authentication certificate
A security certificate that is guaranteed by an authentication authority and that may be used to assure the identity of an entity.

Authentication exchange
A mechanism intended to ensure the identity of an entity by a sequence of one or more transfers of exchange information.

Authentication information
Information used to establish the validity of a claimed identity.

Authentication initiator
The entity that initiates an authentication exchange.

Authentication responder
The entity that responds to the initiator of the authentication exchange.

Authentication token
Information conveyed during a strong authentication exchange, which can be used to authenticate its sender.

Authenticity
The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems, and information.

Authorization
The granting of rights, which includes the granting of access based on access rights.

Availability
The property of being accessible and useable upon demand by an authorized entity.

Baseline controls
A minimum set of safeguards established for a system or organization.

Bilateral counter
A counter that is used and managed exclusively between two communicating entities.

Biometric access control
An access control mechanism based on the identification of an individual through some personal characteristic such as fingerprint or voice pattern.

Block chaining
The encipherment of information such that each block of ciphertext is cryptographically dependent upon the preceding ciphertext block. In this context, a block is a string of bits of a predefined length.

Breach
A violation of security policy which may or may not have resulted in exploitation of the information accessed.

Business continuity plan
See contingency plan.

Capability
A token used as an identifier for a resource such that possession of the token confers access rights for the resource.

Category
A non-hierarchical grouping of sensitive information used to control access more finely than can be achieved with security classifications alone.

Certificate
The public keys of a user, together with some other information, rendered unforgeable by encipherment with the secret key of the certification authority which issued it. This is commonly based on the data structure defined in the X.509/ISO/IEC 9594-8 standard.

Certificate serial number
An integer value, unique within the issuing certification authority, which is unambiguously associated with a certificate issued by that authority.

Certification
The confirmation that an IT system meets all its stated security requirements. Also the process of creating a certificate.

Certification authority
A centre trusted to create and assign public key certificates. Optionally, the certification authority may create and assign keys to the entities.

Certification path
An ordered sequence of certificates of objects in the DIT (directory information tree) which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Challenge
A data item chosen at random and sent by the verifier to the claimant, which is used by the claimant, in conjunction with the secret information held by the claimant, to generate a response which is sent to the verifier. This can be a time variant parameter generated by a verifier.

Channel
An information transfer path.

Ciphertext
Data produced through the use of encipherment. The semantic content of the resulting data is not available, i.e. the data has been transformed to hide its information content. Ciphertext is also known as enciphered information.

Claim authentication information
Information used by a claimant to generate exchange of the information needed to authenticate a principal.

Claimant
An entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

Classification
The determination, or marking associated with a determination, of the level of protection required. This is typically applied as a set of hierarchical classification levels.

Clearance
The permission granted to a user to access specific information or grades of information.

Cleartext
Intelligible data, the semantic content of which is available.

Collision-resistant hash-function
A hash-function from which it is computationally infeasible to find any two distinct inputs which map to the same input.

Communications security (COMSEC)
The protection of information being transmitted across communication links from, typically, interception by eavesdroppers.

Compartmentalisation
A division of data into small, isolated blocks for the purpose of reducing risk. This is often applied, based on the category and/or classification of information.

Compromise
A violation of security policy which has resulted in exploitation of the information accessed.

Compromising emanation
An inadvertent emanation of electro-magnetic radiation from a computer system which contains recoverable information.

Computer security (COMPUSEC)
The protection of data and resources of an IT system from accidental or malicious acts.

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

Contamination
The inadvertent introduction of information of one security classification into data of a lower security classification or different category.

Contingency plan
A plan for activation in the event that some contingency, such as a natural disaster, occurs. Also known as disaster recovery or business continuity plan.

Covert channel
A transmission channel that allows a process to transfer data in a manner that violates security policy.

Credentials
Data that is transferred to establish the claimed identity of an entity.

Cryptanalysis
The analysis of a cryptographic system and/or it's input and outputs to derive confidential variables and/or sensitive data including cleartext.

Cryptographic algorithm
A cryptographic algorithm is defined as an algorithm which transforms data in order to hide or reveal it's information content and which uses at least one secret parameter. This definition includes both symmetric algorithms (e.g. DES and FEAL) and asymmetric algorithms (e.g. RSA and Rabin). In the case of a symmetric algorithm the data is hidden and revealed using a secret parameter. In the case of an asymmetric algorithm the data is hidden using a public parameter and revealed using a secret parameter.

Cryptographic check function
A cryptographic transformation which takes as an input a secret key and an arbitrary string, and which gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall be infeasible.

Cryptographic check value
Information which is derived by performing a cryptographic transformation on the data unit.

Cryptographic equipment
Equipment in which cryptographic functions (e.g. encipherment, authentication, key generation) are performed.

Cryptographic key
A parameter used in conjunction with an algorithm for the purpose of validation, authentication, encipherment or decipherment.

Cryptographic synchronization
The coordination of the encipherment and decipherment process.

Cryptographic system, cryptosystem
A collection of transformations from plain text into ciphertext and vice versa, the particular transformation(s) to be used being selected by keys. The transformations are normally defined by a mathematical algorithm.

Cryptography
This discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

Cryptoperiod
A defined period of time during which a specific cryptographic key is authorized for use, or during which time the cryptographic keys for a given system may remain in affect.

Data integrity
The property that data has not been altered or destroyed in an unauthorized manner, and whose accuracy and consistency are preserved regardless of changes made.

Data origin authentication
The corroboration that the source of data received is as claimed.

Data storage
A container from which data is submitted for delivery, or into which data is put by the delivery authority.

Data string (data)
A string of bits representing an item of information.

Decipherment
The reversal of a corresponding encipherment.

Delivery authority
An authority trusted by the sender to deliver the data from the sender to the receiver, and to provide the sender with evidence on the submission and transport of data upon request.

Denial of service
The prevention of authorized access to resources or the delaying of time-critical operations.

Digital signature
Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

Disaster recovery plan
See contingency plan.

Distinguishing identifier
Information which unambiguously distinguishes an entity.

Domain modulus
A public domain parameter, an integer which is a product of two distinct primes known only to the trusted authority.

Domain parameter
A data item which is common to and known only by all entities within the domain.

Domain verification exponent
A public domain parameter.

Dual control
A process of utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions of information whereby no single person is independently able to access or utilize the materials.

Encipherment
The cryptographic transformation of plaintext data into ciphertext using a reversible process.

End-to-end encipherment
Encipherment of information in the source end-point system, with the corresponding decipherment taking place at the destination end-point system (and not at intermediate points).

Entity authentication
The corroboration that an entity is the one claimed.

Evidence
Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action.

Evidence requester
An entity requesting that evidence be generated either by another entity or by a trusted third party.

Exchange multiplicity parameter
A positive integer used to determine how many times the exchange of entity authentication messages shall be performed.

Feedback buffer
A variable used to store input for the encipherment process, where that input was formed by the previous encipherment step. The start point for the feedback buffer is usually the initialization vector (or starting value).

Firewall
A device which protects an internal network against unauthorized access from an external network by restricting the address and protocols characteristics of external access attempts.

Guard
See security filter.

Hash code
The string of bits which is the output of a hash function, and which typically represents a digested form of a message which is relatively unique to that message.

Hash function
A function which maps an input message of arbitrary size into an output message of a much smaller, fixed size. A hash function is non-reversible and should satisfy the following criteria:
(a) It is computationally infeasible to find, for a given output, a second input which maps to this output;
(b) It is computationally infeasible to find, for a given input, a second input which matches the same output.

Identification data
A sequence of data items, including the distinguished identifier for an entity, assigned to and used to identify an entity.

Identity based security policy
A security policy based on the identities and/or attributes of users and the resources ands objects being accessed.
The result of an unauthorized incident.

Implicit key authentication
The assurance for an entity that only another identified entity can possibly be in possession of the correct key information.

Initialization vector
A number used as a starting point in a sequence of numbers used as input to an encipherment process. The use of an initialization vector (IV) increases security by introducing additional cryptographic variance, and also facilitates the synchronization of cryptographic equipment.

Initializing value
See initialization vector.

Interleaving attack
A masquerade attack which involves use of information derived from one or more ongoing authentication exchanges.

IT security
All aspects related to defining, achieving, and maintaining confidentiality, availability, integrity, accountability, authentication, and reliability of information and information systems.

IT security policy
See security policy.

Key
A sequence of bits that controls the operation of a cryptographic transformation. A cryptographic equipment will generally provide the ability to apply a family of cryptographic transforms; the key

defines one instance within this family.

Key agreement
The process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key.

Key component
One of at least two parameters having the format of a cryptographic key that is combined with the other parameters to form a cryptographic key.

Key confirmation
The assurance for an entity that another entity is in possession of the correct key.

Key control
The ability to choose the key (or key parameters) to be used in a cryptographic process.

Key distribution centre
The facility which generates and issues keys, typically electronically across a network. Entities serviced by the key distribution centre (KDC) would typically each share a key encrypting key with the KDC.

Key encrypting key
A key used to establish a cryptographic process, used to protect another key while being transmitted, e.g. from a key distribution centre to a user equipment.

Key establishment
The process of making available a shared secret key to one or more entities.

Key generating function
A function which takes as input a number of parameters (at least one of which is secret) and provides as output a key appropriate for the cryptographic process for which it is designed.

Key generation exponent
A secret parameter used in a key generation process.

Key generator
See key generation function.

Key loader
A self contained unit used to store one or more cryptographic keys for the purpose of transferring them to other equipment.

Key management
The administration involved in the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation, and destruction of keying material in accordance with a pre-defined security policy.

Key management facility
The protected enclosure in which elements of the key management processes are carried out.

Key offset
The result of adding an offset value to a cryptographic key.

Key token
A key management message sent from one entity to another during a key management process.

Key translation centre
A facility which transforms and returns cryptographic keys for subsequent distribution. A key translation centre (KTC) is typically used to translate keys between entities that share a common key distribution centre.

Key transport
The communications mechanisms used to transfer a key from one entity to another.

Keying material
The variable data required for a cryptographic process, including the cryptographic key and initialization vector.

Link encipherment
The application of encipherment and decipherment at each end of a physical communications link.

Logic bomb
A piece of malicious code which is triggered into action on some predetermined event.

Logical access control
Information-related access control mechanisms such as password access schemes.

Loophole
An unintentional flaw in computer code which allows protection mechanisms to be bypassed.

Mailguard
A special form of firewall which restricts access to messages in electronic mail, typically SMTP, protocols.

Malicious code
Code introduced into a computer program to perform some unauthorized and often harmful action.

Masquerade
The pretence by an entity, usually unauthorized for the action concerned, that it is a different, usually authorized, entity.

Message authentication
The assurance that a message was sent intact, unchanged, from the purported originator to the intended recipient.

Message authentication code
A code appended to a message which can be used to validate the source and part or all of the message.

Mutual authentication
An entity authentication process in which two entities authenticate each other concurrently.

Non-repudiation
A cryptographic service that can be applied to approvals, message delivery, data origin, message receipt, message sending, message submission, and transport. The service is used to provide a guarantee that the action took place and cannot be subsequently denied.

Non-repudiation certificate
A special type of security certificate which constitutes evidence and can be used by a non-repudiation entity for validation.

Non-repudiation exchange
A sequence of one or more transfers of non-repudiation information for the purpose of non-repudiation.

Non-repudiation token
See non-repudiation certificate.

Notarisation
The registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time, and delivery.

One way function
See hash function.

Padding
The process of adding bits to a data item in order to make it a (larger) fixed size.

Passive threat
The threat of a security incident which can be effected by the neglect of entities within the system, rather than by deliberate, external action.

Password
Confidential authentication information.

Physical access control
The physical barriers to access, such as building structures and locks.

Physical security
The aspects of security which involve the physical location, facility, and equipment.

Plaintext
Information represented in an understandable form.

Pre-signature value
A data item created during a digital signature process which is based on the cryptographic key but not the message to be signed.

Private key
One of two keys used in an asymmetric cryptographic function. The private key should be issued to an entity and known only to that entity. See also public key.

Privilege
The ability to carry out a restricted action.

Public key
One of two keys used in an asymmetric cryptographic function. The public key should be made available to any other entity that might require it in a form in which it is bound in an assured way to the entities distinguished name. See also private key.

Public key certificate
The compound data item in which an entity's distinguished name, public key, and various other pieces of information exist in a form which can be verified as accurate.

Randomiser
A facility which produces random numbers on request.

Random number
A number produced by a randomiser in such a way as it is computationally infeasible, without knowing the inputs and processes of the randomiser, to predict the value of subsequent numbers that will be produced.

Redundancy
Any information which is known and can be checked.

Reflection attack
A masquerade which involves sending a previously transmitted message back to its originator.

Replay attack
A masquerade which involves the use of previously transmitted messages.

Repudiation
Denial by an entity of having carried out an action. See non-repudiation.

Residual risk
The risk which remains after security countermeasures have been applied to a system.

Risk
The potential that a given threat will exploit vulnerabilities in an asset to cause loss or damage to the asset.

Risk analysis
The process of identifying threats and vulnerabilities, and so determining the risks to a system.

Risk management
The process of managing the risks to a system though the application of various types of countermeasures.

Round function
A function that combines two bit strings of length L_1 and L_2 into a new string of length L_3.

Routing control
The application of rules during the processing of routing so as to choose or avoid specific networks, links, or relays.

Rule based security policy
A security policy based on global rules imposed for all users within the security domain.

Safeguard
A practice, procedures, or mechanism that reduces risk.

Sanitisation
The process of erasing or overwriting sensitive information on magnetic media so that it cannot be recovered through scavenging.

Scavenging
The process of recovering discarded information from magnetic media by low level access to the magnetic media, typically at the sector level.

Secret key
A key used with symmetric cryptographic techniques.

Secure envelope
A set of data items which is constructed by a trusted third party in such a way as the trusted third party can verify the data items' integrity and origin.

Secure interaction policy
The common aspects of the security policies in effect at each of two communicating entities.

Secure time stamp
A data item with time and date information certified by a trusted time stamp authority.

Security audit
An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures and to recommend any indicated changes in control, policy, and procedures.

Security audit trail
Data collected and potentially used to facilitate a security audit.

Security domain
A collection of IT system resources and users which are controlled by a single security authority, and operate under a common set of security rules and procedures.

Security exchange
The transfer of protocol control information between open systems as part of the operation of a security mechanism.

Security filter
A device which ensures that only specific authorized information can pass through, typically to an external network.

Security label
The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Security life
The time span over which cryptographically protected data has value.

Security policy
The set of rules laid down by the security authority governing the use of security services and facilities.

Security service
A service of a computer application which allows security to be enforced by a system or applied to information.

Security state
State information which is held in an open system and which is required for the provision of security services.

Selective field protection
The protection of specific fields within a data record.

Sensitivity
The characteristic of a resource which implies its value or importance.

Sequence number
A time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period.

Signature
A cryptographic token resulting from the application of a signature function to a message or file.

Signature function
A mathematical transformation using public key cryptography which takes a file or message in and produces a signature which can be proven to have been produced only from the input data.

Signature key
A cryptographic variable issued to an entity for the purposes of creating digital signatures.

Signature process
See signature function.

Signer
The entity generating a digital signature.

Split knowledge
A condition under which two or more parties separately and confidentially have custody of constituent parts of a single information item that, individually, convey no knowledge of the resultant information.

Starting variable
See initialization vector.

Substitution
Encryption that replaces bits or strings with a predefined, alternative set of bits or strings.

Symmetric authentication method
A method of authentication in which both entities share common authentication information.

Symmetric cryptographic technique
A cryptographic technique that uses the same secret key for both the writer's encryption process and the reader's decryption process.

Symmetric encipherment algorithm
See symmetric cryptographic technique.

System integrity
The property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system.

Threat
A potential violation of security.

Ticket
A representation of one or more access rights held by an entity, typically used in the context of a distributed authentication system such as Kerberos.

Time bomb
A piece of malicious code which is triggered into action at some predetermined date/time.

Time stamp
A time variant parameter which denotes a point in time with respect to a common reference.

Time variant parameter
A data item used to verify that a message is not a replay. Random numbers, time stamps, or sequence numbers may be used.

Token
A message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique.

Traffic analysis
The inference of information from observation of traffic flows.

Traffic flow confidentiality
A confidentiality service to protect against traffic analysis.

Traffic padding
The generation of spurious data units to fill communications gaps.

Transposition
Encryption that rearranges bits or strings according to a predefined scheme.

Trapdoor
An intentional loophole in a device which permits subsequent unauthorized access.

Trojan horse
A malicious program which purports to be a well known, harmless program.

Trusted functionality
The functionality of a system which has been independently verified as being correct with respect to some established evaluation criteria.

Trusted third party
A security authority, or its agent, trusted by other entities to carry out security related activities.

Trusted time stamping authority
A trusted third party with responsibility to provide temporal evidence in the form of secure time stamps.

Unilateral authentication
Entity authentication which provides one entity with assurance of the other's identity but not vice versa.

Unique number
A time variant parameter generated by a claimant.

Unprivileged subject
A subject without appropriate privileges to perform an operation.

User identification (userid)
A code, typically alphanumeric, which is associated with a user. A userid is usually, although not necessarily, unique to a user.

Validation
The process of checking the integrity of a message, or selected parts of a message.

Verification authentication information
Information used by a verifier to verify an identity claimed through an authentication exchange.

Verification function
A function in the verification process which is determined by the verification key and which gives a recomputed value of the witness as an output.

Verification key
A value required to verify a cryptographic check value or non-repudiation certificate, or a data item which is mathematically related to an entity's digital signature key and which is used by the verifier in the verification process.

Verification process
A process which takes as input the digital signature of a message, the verification key, and the domain parameters, and which gives as output the result of the signature verification: valid or invalid.

Verifier
An entity that verifies evidence, or an entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication changes.

Virus
A computer program that propagates itself by modifying other programs to include a copy of itself, possibly in a mutated form, that is executed when the affected program is run.

Vulnerability
A weakness of an asset which can be exploited by a threat.

Witness
A data item computed by a claimant and sent to a verifier, or a data item which provides evidence to a verifier.

Worm
A self contained program that can propagate itself through a data processing system or network.

REVIEW OF STANDARDS

Suggestions for improvement of this Handbook will be welcomed. They should be sent to the Chief Executive, Standards New Zealand, Private Bag 2439, Wellington 6020, New Zealand.