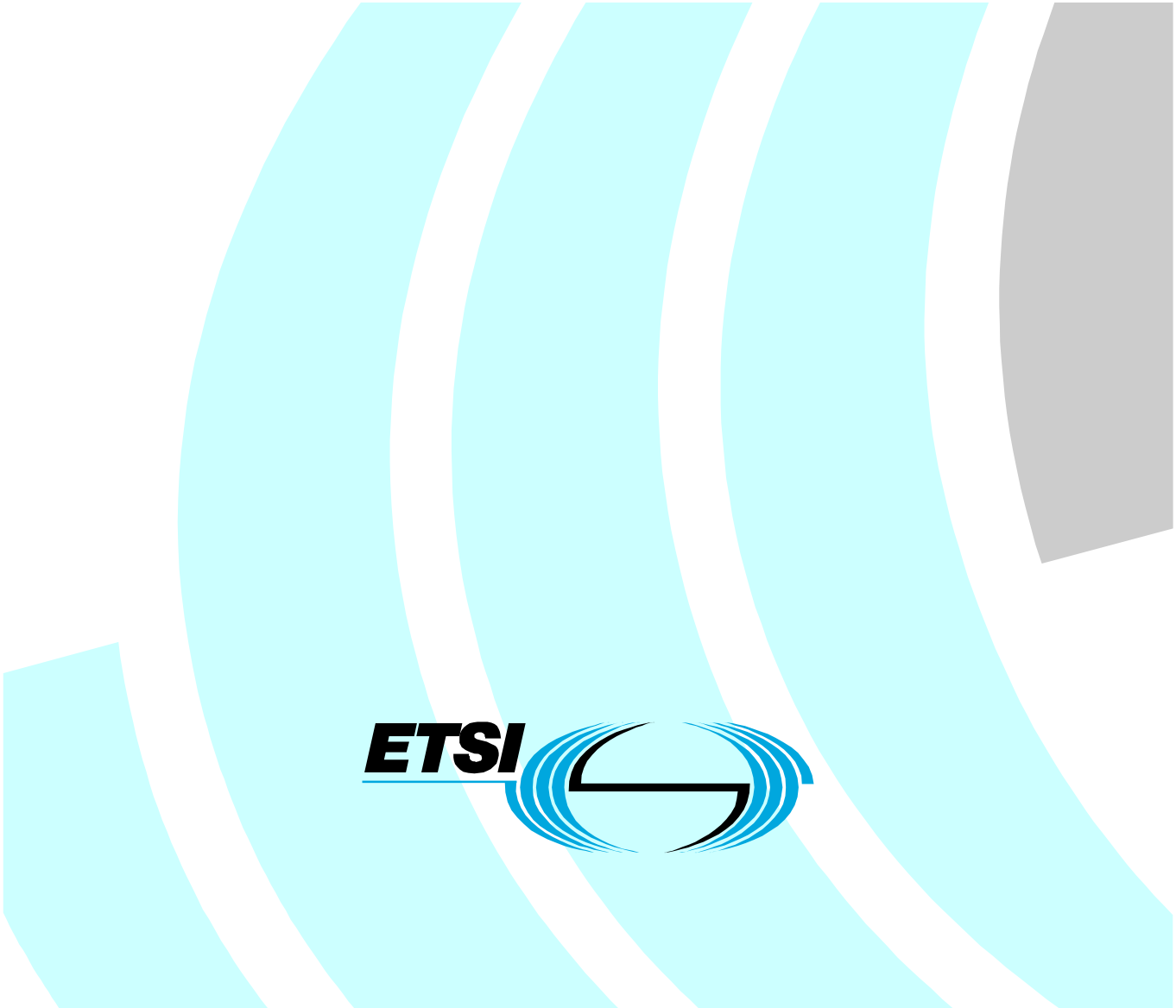
ETSI SR 002 298 V1.1.1 (2003-12)

Special Report

Response from CEN and ETSI to the "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach"



Reference
DSR/BOARD-00004

Keywords
security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Special Report (SR) has been produced by a joint CEN-ETSI Network and Information Security standardization group in response to the European Commission's call for *"a comprehensive strategy on security of electronic networks including practical implementing action"*.

CEN and ETSI share the aims set forward in the Communication from the Commission. It is agreed that there are comprehensive standards available for secure electronic networks. However, the report notes that there are few security frameworks to guarantee multi-vendor systems will operate securely together. Also it is noted that there is a lack of appropriate certification in some areas. The result is fragmentation and uneven implementation in real networks and insecurities remain despite some parts being very secure.

In support of the Commission's aims, certain key issues are central to the report's recommendations:

- **Interoperability:** There are many security standards available. This often leads to problems of interoperability - with potentially annoying consequences for the consumer and perhaps business consequences for the provider of electronic services. A number of mechanisms exist to improve this situation including the use of standards frameworks which can help to identify and incorporate interoperable standards in such a way that users become unaware of interoperability issues. Also interoperability testing can help to ensure equipment conforming to standards and frameworks does really interoperate. The report's recommendations encourage interoperability testing and the incorporation of "overlapping" standards within suitable frameworks which unify as far as possible the different technical means of doing certain tasks.

- **Upgradeability:** Security is not a static problem: the implementation of a standard in a product may need to be updated as weaknesses are discovered; and new standards will be needed whenever existing ones become ineffective in countering threats to security. Several of the report's recommendations are aimed at ensuring this need is recognized and dealt with in a manner that is as simple as possible for the end user, through the use of frameworks that can handle updates in a transparent manner.

- **Home users and Small and Medium Enterprises:** In the near future it is very clear that many home users and many Small and Medium Enterprises will be making new, permanent connections to the Internet for the purposes of e-commerce, information and entertainment. These users will naturally have neither the expertise nor the inclination to apply obscure security measures to consistently prevent security breaches. The report makes recommendations to deal with this issue before it becomes a major problem.

It is hoped that the awareness of these issues generated within the European Standards Organizations will encourage the development of high quality security standards and frameworks in close cooperation with other Standards Development Organizations (whether recognized or not). This will be to the benefit of end users and will help to ensure the development of a more secure environment for electronic communication.

1 Scope

The present document deals with Network and Information Security standardization issues which are relevant to the European Standards Organizations (ESOs). It recommends actions on both the ESOs and on industry standards bodies that when undertaken will improve the availability of secure electronic communication, including e-commerce and the exchange of information within a European environment and beyond.

2 References

For the purposes of this Sepcial Report (SR) the following references apply:

[1] COM(2001) 298 final, 6 June 2001: Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: *Network and Information Security: Proposal for A European Policy Approach*.

[2] 2002/C 43/02: Council Resolution of 28 January 2002: On a common approach and specific actions in the area of network and information security.

[3] e-Government Strategy Framework Policy and Guidelines Version 4.0 September 2002, issued by the UK Office of the e-Envoy.

[4] APEC-TEL Information Systems Security Standards, developed by the APEC-Telecommunications Information Working Group by Standards New Zealand.

[5] OECD Guidelines for the Security of Information Systems and Networks.

[6] Glossary of IT Security Terminology, SD 6, SC27 N2776, issued by the International Organization for Standardization and Electrotechnical Commission (ISO/IEC).

[7] ITU-T Study Group 17, COM - D79: "Security Architecture for Systems Providing End-to-End Communications".

[8] ETSI ETR 336: "Telecommunications Management Network (TMN); Introduction to standardizing security for TMN".

[9] IETF RFC 2633: "S/MIME Version 3 Message Specification".

[10] IETF RFC 2246: "The TLS Protocol Version 1.0".

[11] IETF RFC 2401: "Security Architecture for the Internet Protocol".

[12] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[13] CEN Workshop Agreement CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".

[14] CEN Workshop Agreement CWA 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)".

[15] CEN Workshop Agreement CWA 14169: "Secure Signature-Creation Devices "EAL 4+"".

[16] ISO/IEC 18014-1: "Information technology - Security techniques - Time-stamping services - Part 1: Framework".

[17] ISO/IEC 18014-2: "Information technology - Security techniques - Time-stamping services - Part 2: Mechanisms producing independent tokens".

[18] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities".

[19] ISO/IEC 13888: "Information technology - Security techniques - Non-repudiation".

[20] ISO/IEC TR 13335-2: "Information technology - Guidelines for the management of IT Security - Part 2: Managing and planning IT Security".

[21] ISO/IEC TR 13335-3: "Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security", this provides guidance and methods for risk assessment.

[22] ISO/IEC TR 13335-4: "Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards".

[23] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security". Used for evaluation and certification of security properties of IT products and systems.

[24] FIPS 140-2: "Security Requirements for Cryptographic Modules".

[25] CEN Workshop Agreement CWA 14167-3: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)".

[26] ISO Guide 72: "Guidelines for the justification and development of management system standards".

[27] CEN/ISSS IPSE initiative, 2002 report, http://www.cenorm.be/cenorm/businessdomains/businessdomains/informationsocietystandardizationsystem/

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions given in the Communication from the Commssion [1] apply:

Network and Information Security: the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions. Such events or actions could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via these networks and systems.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CC	Common Criteria
CWA	CEN Workshop Agreement
DES	Digital Encryption Standard
DRM	Digital Rights Management
EA	European co-operation for Accreditation
EESSI	European Electronic Signature Standardization Initiative
EOTC	European Organization for Conformity Assessment
ESO	European Standards Organization
FIPS	Federal Information Processing Standards Publication Series
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISMS	Information Security Management System
IST	Information Society Technologies
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extension

MPEG	Moving Pictures Experts Group
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
POP3	Post Office Protocol
PSTN	Public Switched Telephone Network
RSA	Rivest-Shamir-Addleman
S/MIME	Secure MIME
SAGE	Security Algorithms Expert Group
SCN	Switched Circuit Network
SME	Small and Medium Enterprise
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
UPS	Un-interruptible Power Supplies
VPN	Virtual Private Network
W3C	World Wide Web Consortium

4 Introduction

The present document is issued by CEN and ETSI in response to two documents:

- the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: *"Network and Information Security: Proposal for a European Policy Approach"* [1]; and

- the Council Resolution: *"On a common approach and specific actions in the area of network and information security"* [2].

The first of these documents calls for *"a comprehensive strategy on security of electronic networks including practical implementing action"*. It raises issues for resolution and proposes actions aimed at a number of bodies, with the ultimate aim of facilitating the secure growth of communication and the exchange of information within a European environment and beyond.

A number of actions are proposed by these documents. Some of the actions are specifically addressed to the European Standards Organizations (the ESOs): CEN, CENELEC and ETSI. In particular it is suggested under the heading *"Support for market oriented standardisation and certification"* that:

- "European standardisation organisations are invited to accelerate the work on interoperable and secure products and services within an ambitious and fixed timetable. Where necessary new forms of deliverables and procedures should be followed in order to speed up the work and to strengthen the co-operation with consumer representatives and the commitment from market players.

- The Commission will continue to support, notably through the IST and IDA programs, the use of electronic signatures, the implementation of user friendly interoperable PKI solutions and the further deployment of IPv6 and IPSec (as provided for in the eEurope 2002 Action Plan).

- Member States are invited to promote the use of certification and accreditation procedures on generally accepted European and international standards favouring mutual recognition of certificates. The Commission will assess the need for a legal initiative on the mutual recognition of certificates before the end of 2001.

- European market players are encouraged to participate more actively in European (CEN, CENELEC, ETSI) and international standardisation activities (Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C)).

- Member States should review all relevant security standards. Competitions could be organised together with the Commission, for European encryption and security solutions with a view to stimulate internationally agreed standards".

CEN and ETSI share the aims set forward in the Communication from the Commission. Therefore the aim of the report is to respond to these proposals and make recommendations for standards-related actions to be carried out by the European Standards Organizations, industry standards groups and related bodies in support of the above goals. Appropriate actions include the development of new standards and frameworks, adoption of standards, awareness campaigns and other actions that support the overall aims of the Communication from the Commission.

It should be noted that the term "standard" in the present document is used to refer both to "de jure" and to "de facto" standards. The former are best characterized as those standards issued by the recognized standards bodies and the latter are best characterized as those standards issued by open or closed industry consortia, etc. and used extensively by industry. The term "standard" is also used in the present document to refer to "best practice" consensus-based documents that contribute to Network and Information Security. The practical impact of these distinctions is diminishing.

In considering the present document and its recommendations, one should keep in mind that there is already a lot of security standards work ongoing. Industry plays a leading role in developing and implementing these security standards and solutions. The European IT Observatory's 2003 Report 2003 states that "[a]nalysis of the Western European ICT security market reveals that the end users spent a total of euro 9.4 billion on ICT security in 2002; this will rise to around euro 12 billion in 2003, and euro 18 billion by 2005".

Therefore annexes A to G identify both existing and developing standards that support the security measures identified in the main report. They have been identified by reference to various sources including the APEC-TEL report published by Standards New Zealand [4] and the web sites of the various official and non-official standards developers.

Note that where multiple versions of the same standard are listed (see particularly those listed under ETSI), this is because all versions listed are currently in use.

5 Network and information security

5.1 Definition used in the present document

According to the Communication from the Commission [1]:

- "Network and Information Security can be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions. Such events or actions could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via these networks and systems".

The Commission's Communication groups these security incidents as follows:

- "Electronic communication can be intercepted and data copied or modified. This can cause damage both through invasion of the privacy of individuals and through the exploitation of data intercepted.
- Unauthorised access into computer and computer networks is usually carried out with malicious intent to copy, modify or destroy data and is likely to be extended to systems and automatic equipment in the home.
- Disruptive attacks on the Internet have become quite common and in future the telephone network may also become more vulnerable.
- Malicious software, such as viruses, can disable computers, delete or modify data or reprogram home equipment. Some recent virus attacks have been extremely destructive and costly.
- Misrepresentation of people or entities can cause substantial damages, e.g. customers may download malicious software from a website masquerading as a trusted source, contracts may be repudiated, confidential information may be sent to the wrong persons.
- Many security incidents are due to unforeseen and unintentional events such as natural disasters (floods, storms, earthquakes), hardware or software failures, human error".

Network and Information Security in the context of the present document therefore excludes legal issues and policy (e.g. data protection/telecommunications framework) and excludes law enforcement (e.g. cybercrime). The following chart extracted from COM(2001) 298 [1] illustrates this in figure 1.

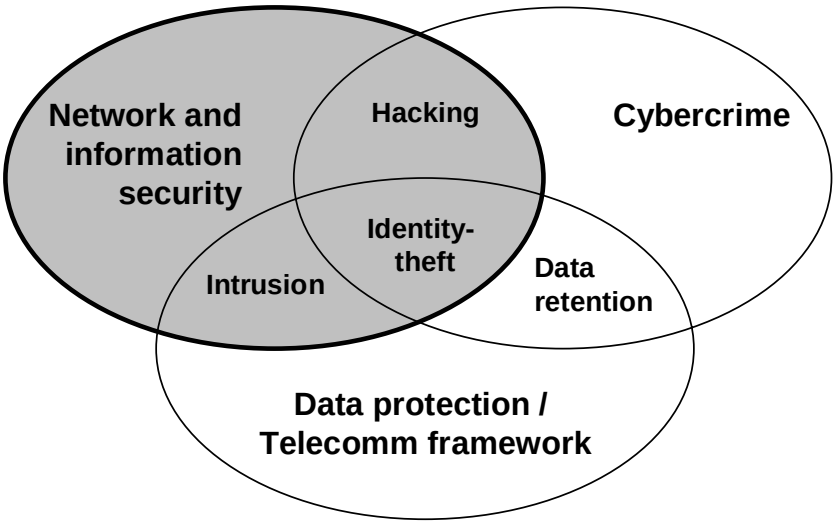


Figure 1

5.2 Other "real world" issues not covered

Other "real world" security issues were raised during the writing of the present document. Whilst having an impact on Network and Information Security they were considered outside the scope of the present document for detailed analysis. Briefly, these issues are mentioned below.

5.2.1 Legal issues

For an overview of legal issues, the reader is referred to other sources, including ETR 336 [8], which provides further information on this subject. Digital Rights Management (DRM) is not covered. It is the subject of a "state of the art" overview by the CEN/ISSS DRM Focus Group, which will shortly be published; standards issues include the work of the Moving Pictures Experts Group (MPEG) in committee ISO/IEC JTC1/SC29. Data protection and privacy is the subject of the 2002 report of the CEN/ISSS IPSE initiative [27].

5.2.2 Vetting of personnel

Incident reports suggest that as many as 80 % of documented security incidents may be caused by trusted "insiders." Whilst national vetting standards exist (particularly in civil and military government, defence and intelligence services and the police for instance), there are no international guidelines. However, this issue is not dealt with any further.

5.2.3 Information security professional qualifications

In view of the removal of barriers to the movement of labour within Europe there is a need for a common understanding of some of the issues which impact upon Information Security, particularly legal issues such as Data Protection and Human Rights. Relevant national authorities should consider whether there is a need for a common Information Security qualification which will demonstrate a competence in this area.

5.2.4 Longevity of archiving

Concern exists over the length of time over which legally-binding signatures, certificates, certificate revocation lists and other cryptographic keys can be archived and successfully retrieved. Even if the raw data remains accessible it is necessary to satisfy the requirements for checking and verification. It is possible that this could be the subject of a CEN CWA on cryptographic keys and the mechanisms to be used for their archiving and subsequent retrieval.

6 Electronic business and other contexts

The present document considers Network and Information Security in the context of the security issues arising in global electronic business, through the context of eEurope 2002, an initiative launched by the European Commission for an Information Society for All that addresses security and trust in electronic business (e-business) carried out over private or public networks (including the Internet). Part of the aim of the initiative is to facilitate the growth of electronic business in the European Community.

It is clear that the provision of a secure and trustworthy infrastructure for carrying out electronic communications in "cyberspace" will encourage e-business growth in Europe. This requires all parties in an e-business environment to accept the responsibility to put in place effective security measures and to then convince the end user that doing business in this way in Europe is not only efficient but also secure.

E-business is defined simply as any normal commercial transaction that is carried out electronically. The report does not address all aspects of network security but essentially those that relate to the user and provider of e-business services. To help understand the scope reference should be made to the security architecture described in COM 17 - D79 [7]. In essence the NIS report addresses those security issues arising in the "End User Plane" as defined in the ITU report. This means that certain significant elements of the internal security of backbone networks are not addressed. These are elements where standards from the ESOs and other such bodies are largely not relevant.

Transactions arising in e-business will include invoicing, ordering, payment etc. Other forms of activity, which may not be strictly commercial, will have similar security issues. A prime example is mobile health care ("e-health") where the security of communications is paramount in order to protect the privacy of patients. The present document does not address the requirements of e-health in detail but appropriate references are made at various points in the report.

In view of the fact that electronic transactions may traverse national boundaries and, where the Internet is concerned the communications path is unpredictable, the end user must be sure that security measures throughout the Internet conform to common security standards and wherever necessary meet the requirement for interoperability.

The emphasis in the report is therefore on the secure use (not secure provision) of generic, interconnected, multi-vendor public IP-based based networks. However specific reference is also made to the use of Virtual Private Networks, wireless LANs and 3G networks since it is likely that any e-business transaction may utilize one or more of these types of networks. Thus it is crucial that the various protocols (including security protocols) must be interoperable over these networks wherever required to establish and maintain the end-to-end communications path as well as conduct the e-business transaction.

7 The structure of the present document

The present document first responds in general to the actions recommended by the Commission's Communication [1]. It deals in clause 7 with recommendations arising from the actions addressed to the ESOs, and also some of the other actions where a response is appropriate.

Then, in order to achieve more detail in its recommendations, the report identifies (in the annexes) relevant existing and developing standards that contribute to Network and Information Security and support the requirement for interoperability in a global e-business environment. It also identifies development activity being carried out by groups outside the official standardization bodies that may result in the production of suitable standards. This information is intended also to provide base-line information to assist in executing the follow-up actions.

Using this information, based on input kindly provided by Standards New Zealand [4], the report finally seeks to identify conflicts and overlaps between existing standards and to highlight gaps in the standards spectrum. In this way the report arrives at its more detailed recommendations.

However, the threats identified in the Commission's Communication [1] are not countermeasures. Detailed recommendations can only be made in the domain of solutions so it is necessary to identify the security measures appropriate to each threat and identify the deficiencies of the solutions in each relevant domain. The translation from threat to solution domain is done in two ways. First, several important "use cases" are identified from the points of view of different types of user and their requirements. This gives rise to a first set of detailed recommendations in clause 8. Second, the general security measures are examined, grouped under an established set of security services covering the identified threats. This results in a second set of detailed recommendations in clauses 11 to 16.

8 CEN and ETSI response to proposed actions

In this clause the report provides recommendations arising from those actions specifically proposed in the Communication from the Commission [1] which are directed at or are relevant to the ESOs.

8.1 Awareness raising

There are three proposed awareness-raising actions in [1] aimed at Member States.

Although these actions are aimed at the Member States, the ESOs can also continue to contribute to awareness-raising within their own membership and within their own technical organizations. Such actions are ongoing and are integrated, as appropriate, in later clauses and recommendations in the present document.

8.2 Technology support

There are two proposed actions in [1] on Technology Support aimed at Member States and the Commission, concerning security in the 6th Framework programme and pluggable strong encryption.

It should be noted that the purpose of "pluggability" in this context, the unbundling of security systems at appropriate standardized interfaces, has the purpose of allowing different core solutions for end-to-end strong encryption to be easily incorporated, under user control, into existing complete security solutions. This may be needed, for example, to facilitate operation within the varying cryptography constraints of differing legal requirements in different territories or to ensure resistance against evolving forms of attack by allowing for the upgrading of strong encryption algorithms within a security system.

However, "pluggability" may be only one possible mechanism that can achieve the overall requirement for the rapid updating under user control of interoperable strong encryption algorithms. Furthermore, the need for such updates is not confined to strong encryption.

The ESOs and industry standards groups are places where successful ideas for all types of security algorithm can be standardized if appropriate. However there is a need within the security standards and other products of the ESOs to continue to recognize the need for security standards to support upgradeable, interoperable security technologies including, but not limited to, strong encryption. Interoperation of end-to-end security in real systems, as transparently as possible to the user, must be maintained whenever the relevant security standards are updated in response to recognized vulnerabilities or for other reasons such as technology development.

Recommendation 1: The ESOs and industry standards groups should review their security standards and, if appropriate, enhance their user-friendly support for resistance to evolving forms of attack on core security technologies including, but not limited to, strong encryption.

8.3 Support for market oriented standardization and certification

8.3.1 Interoperability

- "European standardisation organisations are invited to accelerate the work on interoperable and secure products and services within an ambitious and fixed timetable. Where necessary new forms of deliverables and procedures should be followed in order to speed up the work and to strengthen the co-operation with consumer representatives and the commitment from market players".

Especially in the Information and Communications Technologies, the ESOs and industry standards groups have offered a comprehensive range of deliverables for many years, including rapidly-produced consensus documents that do not need to undergo the full process to become formal European Standards. ANEC, the European Association for the Representation of Consumers in Standardization, participates as fully as possible in all three ESOs, and has an ICT Working Group, although resourcing direct consumer participation in all technical groups is not practicable. Since the ESOs operate on an open basis, their activities necessarily require the commitment of market players in order to produce the results. NORMAPME, European office of crafts, trades and small and medium sized enterprises for standardization, participates also as fully as possible in each ESO, and contributed significantly to the work of ETSI STF 228 on interoperability criteria for users.

Interoperability of implementations is a key aim of standards, but not always achieved. The availability of interoperability events represents an ongoing commitment from the ESOs and industry standards groups, which will ensure that standards for protocols where users may reasonably expect a high degree of interoperability will deliver this promise.

This type of products from the ESOs and industry standards groups might also be extended to encompass similar events aimed at testing the security from attack of products built to secure standards or best practice documents. Alternatively, the availability of formal security test procedures from the ESOs or industry standards groups might be taken up by others to offer such a service.

Recommendation 2: The ESOs and industry standards groups should continue to develop existing and new mechanisms to ensure interoperability of key standards supporting Network and Information Security, including interoperability assurance or testing services and formal methods for ensuring interoperability. For example security testing standards should be developed.

The correct degree of interoperability is essential for supporting e-business applications in Europe. Its absence not only inhibits growth but may lead to the development of non-interoperable ad-hoc services.

Recommendation 3: A list of security frameworks supporting e-business, perhaps including those from EESSI and TIPHON, should be produced in order to support the development of the Article 17 list of standards under the Framework Directive.

8.3.2 EU initiatives

- "The Commission will continue to support, notably through the IST and IDA programs, the use of electronic signatures, the implementation of user friendly interoperable PKI solutions and the further deployment of IPv6 and IPSec (as provided for in the eEurope 2002 Action Plan)".

Recommendation 4: Collaboration between the ESOs and industry standards groups and EU programmes such as IST and IDA should be strengthened, in order to ensure that the programmes are properly aware of the standards "state of the art" and to ensure that relevant outputs from these programmes are made available to standards groups.

8.3.3 Certification and accreditation

- "Member States are invited to promote the use of certification and accreditation procedures on generally accepted European and international standards favouring mutual recognition of certificates. The Commission will assess the need for a legal initiative on the mutual recognition of certificates before the end of 2001".

Recommendation 5: The policy regarding which products and services need certification and accreditation is not a matter for the ESOs. However, the ESOs and industry standards groups should continue to respond to decisions on certification and accreditation policies with the development of supporting standards, best practice documents and test suites.

8.3.4 Participation in standardization activities

- "European market players are encouraged to participate more actively in European (CEN, CENELEC, ETSI) and international standardisation activities (Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C))".

The problem of international standardization is that it is so fragmented - there are well over 200 industry standards consortia in the ICT sector. This makes it difficult and expensive for European companies to participate, or even to obtain a clear picture of what work is going on where.

Recommendation 6: The ESOs and industry standard groups should continue to improve the provision of information to European market players on global activities, and to encourage participation in their own activities.

8.3.5 Stimulation of standardization activities

- "Member States should review all relevant security standards. Competitions could be organised together with the Commission, for European encryption and security solutions with a view to stimulate internationally agreed standards".

The Communication recommends a role for Member States in reviewing security standards, but in practical terms this should not be carried out in isolation without reference to the European and global standards environments.

Recommendation 7: The Member States should adopt a concerted approach to their review of security standards, involving also the ESOs and industry standards groups. There should be no competitions, unless the results can be accommodated with interoperability within a framework (see pluggable encryption); any activities to provide internationally-agreed standards should in any case be carried out in consultation with the relevant standards bodies as well as the private sector.

8.3.6 Proposed European Network and Information Security Agency

Recommendation 8: The ESOs should establish communication channels to the European Network and Information Security Agency.

8.4 International co-operation

There is one proposed action aimed at the Commission.

Recommendation 9: The ESOs and industry standards groups have a role in global cooperation on security standards which they should continue to develop and pursue.

9 User requirements

The general recommendations proposed in this clause are based upon a consideration of the security requirements of various classes of potential users of e-business services. The User classes are home users, Small and Medium Enterprises (SMEs) and large organizations and industries. More specific recommendations are also made in clauses 11 to 16.

Roles and responsibilities must be carefully separated. The users of equipment, whoever they are, cannot escape responsibility for the correct installation and use of their equipment. Manufacturers may acquire the responsibility to provide security capabilities but they cannot acquire the responsibility for their correct use. For example end users must accept the responsibility to ensure the equipment they connect to a shared public network, such as the Internet, does not cause damage or inconvenience to others.

9.1 Home users

The home user today typically has a single PC and will use either dial-up over public switched networks (PSTN or ISDN) or broad band access facilities such as xDSL or a cable modem. In general there will be a single gateway (to the public Internet).

The following clauses describe current and envisaged future home user applications.

9.1.1 Home working

It is envisaged that there will also be significant growth in the near future in number of home workers requiring access to office-based systems. This will lead to a requirement for standards for communications protocols (e.g. to provide connection from home-based workstations and networks to wide area networks providing global connectivity). There will be a requirement for information transmitted between home and base office to be protected.

9.1.2 Personal business

Many home users will wish to carry out personal business transactions with online suppliers of products and services using the Internet. In the vast majority of cases these transactions will include the use of web-based services or email facilities.

9.1.3 Microprocessor control of domestic equipment

It is envisaged that in the near future there will be significant growth in the use of home devices - such as heating systems, refrigerators, alarm systems, ovens - containing embedded microcontrollers that can be accessed remotely. There will be a requirement for the home user to control such systems using personal computers in the home. Additionally it will be necessary for the home user to have limited remote control and system configuration facilities whilst not in the home.

An international standard exists that specifies the requirements for home gateways and work has also been carried out by Telemetry Associates on behalf of the UK Department for Trade and Industry. Annex G lists standards and reports available.

9.1.4 General security requirements

Consideration of the above use cases leads to the following general security requirements for home users:

a) Many home users will be generally unfamiliar with computer security and would benefit from the availability of guidance in the form of security checklists. Existing checklists should be identified and promoted.

b) The home user cannot always protect the integrity and confidentiality of personal information after it leaves his personal computer. Online suppliers of products and services and ISPs should be encouraged to provide basic security services to assist their customers (e.g. firewalls and virus checking of e-mail). Although not removing an end user's responsibilities for his or her own security, this will help provide the confidence to the home user that the confidentiality and integrity of private information being exchanged between the home user and the online supplier (such as credit card details, identity information) is protected.

c) The home user will need effective consumer-oriented security products to be available to protect personal information stored on the home PC. These products need to be easy to use (ideally "transparent" to the user) by non-computer experts and will counter the threat of hacking and virus attacks. The onus here is on the product suppliers.

d) Application software to support the home user (e.g. PC operating systems, word processing packages, spreadsheet packages etc.) will be expected to be resistant to attack. Manufacturers of software for home systems should be responsible for ensuring that this is the case and for providing guidance on the safe operation of their systems.

e) The home worker will need to be provided by his employer with ready-to-use systems with good security such as VPNs or end to end encryption facilities.

f) Many devices in the home that contain embedded microcontrollers will become accessible from the Internet and thus vulnerable to attack. Because, in many cases, they operate independently of human input, the establishment of automatic and remote methods of protection are necessary together with codes of practice and standards that underpin them. This should be regarded as a major area of concern for Network and Information Security.

Note that the legal aspects on the "interception" for the purposes of ANTI-SPAM and ANTI-VIRUS handling is now under scrutiny:

- At the European level in CEN/ISSS Workshop data protection and privacy; and
- At the International level in IWGDPT, in the International Working Group for Data Protection on Telecommunications.

9.2 Small and medium enterprises

The SME user will typically be an organization with a small number of employees (typically up to 50, although formally less than 250). The SME will generally have a Local Area Network providing connectivity via a public network. In general there will be a limited number of gateways (perhaps just one) to the external network.

Unlike the large organization, the SME will typically not be directly concerned with security standards (indeed the cost of obtaining them will typically be considered too great). The SME will largely be concerned with security solutions, for hardware, for software and for skills development.

The following paragraphs describe typical use cases for SMEs. In general a single SME may be both a user and a supplier of e-business services and consequently both the use cases will apply to the SME.

9.2.1 The SME as a user of e-business services

An example is an organization that uses an Internet-based trading service to source raw materials or office supplies.

The typical SME will share some of the concerns of the home user (see clause 9.1). However the SME will also hold personal data relating to employees, commercial data relating to trading partners business critical data such as customer lists, contract information etc. The SME will in general have a more complex requirement than the average home user from the point of view of applications and network architecture but on the other hand will often have sufficient expertise and knowledge to resolve security issues which arise.

Also a loss of confidentiality, integrity or availability of information could have a significant impact on the SME including for instance infringement of legislation such as data protection, loss of business etc. and could in extreme cases lead to closure of the business. Hence SMEs in general need to be highly aware of the need for effective information security.

9.2.2 The SME as a supplier of e-business services

In this case the SME will be offering goods or services over the Internet probably using web based applications. The SME will be responsible for protecting sensitive information held on its customers. It may also be perceived by its customers as having responsibility for security for the whole transaction path between itself and the customer.

9.2.3 General security requirements

Consideration of the above use cases leads to the following general security requirements for SMEs:

a) In many cases the SME may be unfamiliar with computer security and in consequence may benefit from the supply of awareness, training and guidance material. SME trade bodies such as NORMAPME have a clear role in contributing in the elaboration of such services and products as well as in providing channels for the dissemination of such material.

b) The SME as a user of e-business will expect that the ISP and the e-business supplier will protect the confidentiality and integrity of both personal and commercially sensitive data when it leaves the domain of the SME.

c) The SME will expect that effective security products will be available to protect personal and commercially sensitive information stored on the internal network. This will include the availability of secure web server application software. These products should be easy to use (ideally "transparent" to the user) by non-computer experts and will counter the threat of hacking and virus attacks that could affect the availability of the SME system. Note that the legal aspects of Anti-SPAM and Anti-Virus are being addressed - see clause 9.1.4, final paragraph.

d) The establishment of a security guidance framework through SME trade bodies will help promote understanding of security issues by those with little background in information security.

9.3 Large organizations and industries

The large organization user will typically have multiple sites possibly in several countries. It will normally have a large range of e-business partners (both providers of service and users) including commercial suppliers, banks, government organizations and Trusted Third Parties (e.g. Certification and Registration authorities). The organization will have large numbers of networked workstations and may make use of Virtual Private Networks (VPNs). In the context of the present document "large organizations" include government organizations where the communication is between government and citizen but government to government is outside the scope.

Use cases for large organizations are similar to SMEs but large organizations will invariably act as both a supplier and a user of e-business services.

9.3.1 General security requirements

Consideration of the above leads to the following general security requirements:

a) Large organizations will mirror those of the SMEs though it is expected that they will in general be aware of the need to provide adequate security to protect their systems and communications.

b) However, they may not have sufficient specialist security resources to formulate and operate a security regime. Consequently they may need advice, guidance and standards on security policies, risk assessments and the like.

c) In general it is likely that large organizations will be prepared to pay more for their security products than home users and SMEs and will be inclined to place trust in the major software suppliers.

d) The business of large organizations may extend to multiple sites in several countries and their trading partners will also be global in nature. As a result they will be more inclined to use security products conforming to international standards. Hence there is a need to address the interoperability of standards for Trust Service Providers and technologies such as Public Key Infrastructures which facilitate global e-business.

9.4 Recommendations

The home user market and the SME (as both provider and consumer of network services) must be recognized as a major future security issue. The home user's "home gateways" and the SME's "business gateways" will become a key element in ensuring boundary security for a growing number of small networks in the hands of administrators who cannot be expected to be well acquainted with security matters.

Recommendation 10: The ESOs, industry standards groups and European SME associations (in cooperation with other bodies if required) should identify existing good-practices, including those addressing formal test procedures for such small gateways which recognize the needs of SMEs and home users. Note that software gateways such as ICS (Internet Connection Sharing) in Microsoft Windows and the GPL netfilter project (called iptables in Linux) should be taken into account.

Non-PC based domestic networks in the home and in commercial buildings (e.g. central heating, burglar alarms) may be vulnerable to attack from Internet based threats.

Recommendation 11: The ESOs and industry standards groups should initiate work to identify and, if needed, develop standards and codes of practice to address the vulnerability of non-PC based domestic networks in the home and in commercial buildings.

Gateways, especially those including NAPT (Network and Port Address Translation) functionality, may continue to hinder the end-to-end interoperability of certain protocols. The design of IPSec, for example, allows a number of operational modes which will never successfully transit a NAPT gateway without special encapsulation. Home and SME gateways need to be designed to handle IPSec and enterprise IPSec servers need to be set up properly to ensure transparency.

Recommendation 12: The ESOs and industry standards groups in collaboration where appropriate with European SME associations should identify and, if needed, develop (for IPSec) gateway transparency and best-practice, including test procedures. Also IPSec security profiles for enterprise gateways should be set up which are home and SME gateway-friendly.

Recommendation 13: The ESOs and industry standards groups, especially trade associations representing SMEs, should continue to contribute to the widespread appreciation of best practice for home users and SMEs through aiding awareness activities.

10 General threats to network and information security

The assets of the e-business service must be protected in order to preserve the Authenticity, Confidentiality, Integrity, Accountability and Availability of the service. The assets of the e-business service are:

a) The data of organizations and citizens using the e-business service.

b) The assets of the e-business service itself (e.g. systems, networks, information).

c) Data and remote control information to networked home based equipment and systems.

d) User authentication credentials.

The threats to the assets of the e-business service are summarized in the Commission's communication [1] as follows:

T1 "Electronic communication can be intercepted and data copied or modified. This can cause damage both through invasion of the privacy of individuals and through the exploitation of data intercepted".

T2 "Unauthorised access into computer and computer networks is usually carried out with malicious intent to copy, modify or destroy data and is likely to be extended to systems and automatic equipment in the home".

T3 "Disruptive attacks on the Internet have become quite common and in future the telephone network may also become more vulnerable".

T4 "Malicious software, such as viruses, can disable computers, delete or modify data or reprogram home equipment. Some recent virus attacks have been extremely destructive and costly".

T5 "Misrepresentation of people or entities can cause substantial damages, e.g. customers may download malicious software from a website masquerading as a trusted source, contracts may be repudiated, confidential information may be sent to the wrong persons".

T6 "Many security incidents are due to unforeseen and unintentional events such as natural disasters (floods, storms, earthquakes), hardware or software failures, human error".

The threats T1 to T6 can be countered by the application of a set of security services. Each of these security services will comprise a number of technical, procedural and policy security countermeasures covered in clauses 11 to 16 inclusive. For the purposes of the present document, the security services are defined as follows (see note 1).

a) **Registration and Authentication Services.** These services provide the means to ensure that users are uniquely and unambiguously identified and granted access only to those assets for which they have been authorized. The overall security of the e-business services and their assets rely ultimately on the capability to authenticate users of the service.

b) **Confidentiality and Privacy Services.** These services provide the means whereby e-business information is stored and transferred securely (including possibly the identities of participants). They also ensure that private information (such as an individual's medical information) is protected in accordance with legislation such as data protection.

c) **Trust Services.** These services are required to ensure that e-business transactions are properly traceable and accountable to authenticated individuals and cannot be subsequently disavowed. They are the services that enable e-business service providers and e-business clients to make commitments in electronic form.

d) **Business Services.** These services are required to ensure that the e-business applications are designed, configured and operated in a secure manner and their information assets properly protected against non-malicious threats including accidental failure. E-business applications include the web servers that present the information to the e-business users and the back-office systems that host the applications.

e) **Network Defence Services.** These services ensure that the physical assets, stored data and other assets of the e-business service are properly protected against malicious attack.

f) **Assurance Services.** These services are intended to provide the e-business user with confidence that the technical (hardware and software applications) and non-technical (physical, personal and procedural) security measures provide protection against the assessed risk to the services. That confidence is achieved by ensuring that e-business services have been designed, configured and operated in a manner in accordance with identified standards. The end result of the process is often a statement to that effect in the form of a certificate (see note 2) Assurance services apply therefore across all the high-level security services defined above.

NOTE 1: These security services are adapted from the framework devised by the UK government's Office of the e-Envoy for representing the security requirements in the context of an "e-citizen e-business e-government" environment.

NOTE 2: The use of "certificate" in this context is not the same as a "digital certificate" that is used to prove ownership of a public key.

Table 1 shows the relationship between threats T1 to T6 and the set of security services defined above (note that Assurance services are not included because they do not counter threats in themselves but define what confidence can be placed in security countermeasures).

Table 1

Threat	Security Services				
	Registration and authentication	Confidentiality and privacy	Trust	Business	Network defence
T1		X			
T2	X	X			
T3					X
T4					X
T5	X		X		
T6				X	

In order to protect the network and information systems that form the basis of the e-business service, the threats to the service must be countered by a number of technical, policy or procedural security measures. The following clauses of the report, each associated with an annex containing a list of relevant standards and related work, now describe these security measures under the high level security services defined in the previous clause and contain relevant recommendations:

- Clause 11 and annex A: Registration and authentication services;
- Clause 12 and annex B: Confidentiality and privacy services;
- Clause 13 and annex C: Trust services;
- Clause 14 and annex D: Business services;
- Clause 15 and annex E: Network defence services; and
- Clause 16 and annex F: Assurance services.

11 Registration and authentication services

It is of paramount importance that effective and secure registration and authentication services are put in place in an e-business environment, since registration and authentication represents the "front line" in the defence of the e-business services and data. For the purpose of the present document the definitions of "authentication" and "registration" are taken from *e-Government Strategy Framework Policy and Guidelines* [3]:

- **Registration.** Registration is the process by which a user of the e-business service gains a credential (such as a username or digital certificate) for subsequent authentication. In many cases this will require the potential user to present proof of real-world identity (e.g. a birth certificate or passport) to the registration authority. It includes the case for anonymous or pseudonymous identity (i.e. the holder of the credential is entitled to a service without revealing a real world identity).

- **Authentication.** Authentication is the process by which the asserted electronic identity of a user (as represented by the credential supplied in the registration process) is validated by the e-business system to access specific e-business services. In general the authentication process checks that the user is the true owner of the credential supplied during the registration process by means of a password or biometric for instance.

A list of completed documents can be found in annex A.

11.1 Security measures

Registration and authentication services comprise the following security measures:

a) Effective user registration;

b) Effective user identification and authentication;

c) Effective access control;

d) Effective user management.

11.1.1 Effective user registration

The aim of user registration is to ensure that access credentials are only issued to those whose bona fides have been properly established. This is normally achieved by procedural means. In some cases an independent Trusted Service Provider may be involved in operating the registration process.

11.1.2 Effective user identification and authentication

The aim of user identification and authentication is to ensure that access to the service is only granted to individuals whose credentials have been validated. It is achieved by the following measures:

a) The asserted credential is verified by a **password**, **biometric** or **digital certificate**. A **smartcard** may be used to support the authentication mechanism.

b) The use of **firewalls**, **intrusion detection systems** and **penetration testing** will help prevent all unverified users (including "hackers") from gaining unauthorized access to e-business services (these matters are dealt with in clause 15).

Note that in some cases (notably in health care) it may be necessary to protect the real world identity of the individual and provide pseudonymous or anonymous identity.

11.1.3 Effective access control

The aim of access control is to ensure that access to the services and the information is in accordance with user profiles. Access control may be based on software-based access control mechanisms operating at a service, file or record level and access permissions held in digital certificates.

11.1.4 Effective user management

The aim of user management is to control and maintain user profiles in order that e-business service users may access those parts of the e-business service that are necessary to carry out their business requirement. The use of digital certificates may be appropriate to maintain such profiles.

11.2 Passwords

Username/password combinations are relatively insecure. Passwords are vulnerable to opportunistic attacks (e.g. badly structured passwords may be guessed, passwords may be accidentally disclosed to unauthorized individuals) or directed attacks such as password cracking. Standards have been issued by various bodies providing general guidance on password selection, usage, management and maintenance. Additionally local guidance has been issued widely by individual organizations and national entities.

One-time password systems provide better protection because each password may be used once only. Passwords are typically generated automatically using software.

11.3 Biometrics

In some cases the use of biometric-based authentication methods on their own may offer a convenient and practical alternative to identify and verify individuals. However, used this way they do have specific vulnerabilities. Biometrics based authentication systems need to allow for day-to day changes in a biometric. A "margin of error" is necessary so that day-to-day variations in an individual's offered biometric do not cause an authorized user to be rejected because the offered biometric does not match exactly with the stored biometric template. However, this margin of error may allow an unauthorized user to gain access to the system. Other biometric vulnerabilities include mimicry (e.g. of signature or voice), spoofing (e.g. fake finger using the residual image left behind on a fingerprint reader).

Nevertheless, Biometric-based authentication systems offer flexibility and convenience in use. For instance they can be used in the same way as a password to verify a claimed identity (i.e. one to one comparison) or in pure identification mode where an individual asserts his identity simply by presenting a biometric alone (one to many comparison). They may also be used for both positive identification (i.e. similarly to passwords - to prove I am who I say I am) or in negative identification (i.e. to prove I am not who I say I am not).

The use of biometrics for authentication is a relatively new technique which potentially offers advantages over traditional authentication techniques particularly in terms of convenience and some security aspects (e.g. a biometric cannot be stolen or guessed). However, current issues over performance mean that biometric systems in isolation may be suitable only for use in situations where the highest level of certainty is not demanded.

For situations where a higher degree of certainty is needed, biometrics may be effectively combined with other authentication technologies to provide a combined security measure. Experience shows that such a combination of several different attributes, something you have (e.g. a smart card), something you know (e.g. a password or PIN) and something you are (e.g. a biometric) has the potential to provide state of the art security levels.

There are also general public concerns about the physiological/health effects of the use of biometrics. Furthermore, privacy concerns arise related to the holding of biometrics records by the authorities rather than having the records held securely by the user alone. It is considered that these issues need to be addressed before biometrics can become widely accepted by the public, but they are not considered to be issues for standardization.

In addition to activity on official standardization bodies work on biometrics issues is also being carried out in several national and international groupings.

11.4 Digital certificates

A digital certificate contains information in electronic form that identifies the owner of a specific public/private key pair. A third party, trusted by the e-business service provider, digitally signs the certificate to prove its authenticity. The digital certificate then represents the means by which the e-business service authenticates the user. A Public Key Infrastructure is generally required to support the distribution, management and maintenance of digital certificates. Digital certificate standards define the format of the certificate and privacy enhancing features.

11.5 Smart cards

A smart card is a credit card sized token containing a micro processor enabling it to *process* and store information, to support single or multiple applications and to operate both off-line and on-line. They may be used as *contact* cards where the card and the card reader are in contact during the operation or *contactless* cards where the card and the card reader communicate with each other over a short distance.

Smart cards are an important enabler of e-business applications particularly because they can be used to hold authentication information such as a user's private key in a PKI infrastructure scheme or a user's biometric template. The card may be activated by a user PIN or biometric sample thus avoiding security issues associated with sending authentication credentials over computer networks. In addition to providing secure access control, smart cards may also be used in a wide variety of other applications such as electronic purses, storage of confidential information and loyalty cards.

Though smart cards are vulnerable to physical attacks, these attacks are technologically difficult to mount and require the attacker to have possession of the card.

Many of the standards associated with smart cards are associated with defining the physical design of the card in order to achieve interoperability with card readers. Other standards are application specific and describe how the smart card interacts with the application.

In addition to work being carried out by the official standardization bodies there are also several industry and user groupings involved in developing specifications and best practice documents for smart card applications. These include the eEurope Smart Card Forum, the Personal Computer Smart Card workgroup, the Smart Card Alliance and Eurosmart.

11.6 Recommendations

11.6.1 Registration

Registration procedures are largely a matter between the issuer of a credential and the person or entity being accredited. However since registrations in systems open to the public need to be accepted by a wide community as meeting appropriate minimum standards, such registrations should be conducted according to an agreed standard for best practice.

Recommendation 14: The ESOs and industry standards groups should identify and, if needed, develop a code of good practice for those who issue credentials.

11.6.2 Authentication

The interoperability considerations for all authentication measures (including digital signatures which are dealt with in clause 12) are the same: interoperability to a widely (ultimately globally) agreed standard is required for the customer to be able to authenticate him or herself in any transaction.

The primary standard needs to be a framework that can accommodate changing technical mechanisms, multiple mechanisms and alternatives according to need. The framework needs to handle digital signatures, passwords, biometrics, digital certificates and smart cards. The framework should handle multiple instances of the individual methods in a transparent manner (to the user).

Recommendation 15: The EESSI project should issue a report on the integration of multiple authentication mechanisms, including passwords, biometrics, digital certificates and smart cards, into the EESSI framework taking in the results of the CEN/ISSS WS eAuthentication (launched in September 2003).

Recommendation 16: ESOs and industry standards groups should work with industry and government to help educate users about the security risks resulting from poorly selected passwords and provide guidance to users about constructing effective passwords.

11.6.3 Interoperability and framework considerations

Individual mechanisms also need to interoperate. Even if the framework will handle multiple methods, the acquisition and use by a user of many individual authentication mechanisms will complicate interoperability.

Recommendation 17: The ESOs and industry standards groups should cooperate, perhaps in conjunction with ISO/ITU and non-European bodies in GTSC, to develop a convergence roadmap for minimizing the global number of overlapping standards for individual authentication mechanisms.

11.6.4 Biometrics

It seems likely that the developing discipline of biometrics will continue to develop and may provide alternative and, in some cases more convenient, authentication methods. There is, however, a lack of authoritative information, best practice and standards available to enable potential users to make informed decisions on the selection and deployment of biometric-based authentication solutions.

Recommendation 18: The ESOs and industry standards groups should identify and, if needed, develop "best practice" documents for biometrics usage.

Recommendation 19: ESOs and industry standards groups should review the activities of the various biometrics working groups with a view to the development of potential standards for performance testing, evaluation methodology, protection profiles (under the Common Criteria standard), APIs and template.

11.6.5 Other mechanisms

The following areas have been identified by the eEurope group as requiring additional standardization effort:

- Chip-based ID management and Privacy issues.
- Harmonization of multi-application platforms covering issues such as loading and deletion of individual applications.
- Agreed Protection Profiles and certification procedures (beyond EAL4) for chipcards and chip card infrastructure components.

Recommendation 20: The ESOs and industry standards groups should set up workgroups to address Chip-based ID management and Privacy issues, harmonization of multi-application smart card platforms and Protection Profiles and Certification standards for chip cards and chip card infrastructures.

12 Confidentiality and privacy services

Confidentiality services provide the means by which sensitive information held on or transmitted from e-business systems is prevented from being disclosed to individuals not authorized to see it. This includes Information that may be sensitive at a national level (e.g. national security), or at a corporate (e.g. commercial) level or appertaining to a specific individual (privacy).

Unauthorized disclosure can cause damage both through invasion of the privacy of individuals and through the exploitation of data intercepted. It may also be subject to statutory requirements such as Data Protection or Human rights or legislation associated with national security such as Lawful Interception. ETSI has issued a series of technical papers through Technical Committee LI on aspects of Lawful Interception and work is also being undertaken in Technical Subgroups such as SPAN, TETRA, TIPHON and 3GPP.

A list of completed documents can be found in annex B.

12.1 Security measures

The *aim* of Confidentiality services is to prevent the disclosure of sensitive information stored within the e-business services or in transit over networks to individuals not authorized to receive the information.

The *aim* of Privacy services is to ensure that private data appertaining to an individual (such as medical or financial data) is protected in accordance with data protection and other legislation. Note that in some cases it may be necessary to provide protection for some but not all of the transaction fields including identity, origin (see note), destination etc. See http://www.mobihealth.org.

NOTE: Protection of origin information will not be appropriate in the case of emergency services.

The security measures that support confidentiality and privacy are mainly predicated upon effective access control functions and consequently are the same as those for authentication (see clause 11). However, this clause of the report deals with additional measures over and above those for authentication.

The additional security measures required are:

a) The use of **encryption** to control access to stored or transmitted data.

b) An effective **object re-use** procedure to prevent the accidental release of sensitive information to unauthorized individuals.

Encryption may be used to protect information stored within the systems providing the e-business services and the end user systems. It may also be applied at various levels in the networking infrastructure to protect transmitted information.

12.2 Encryption of stored information

There are many stand-alone consumer-oriented PC-based products available for encrypting stored information. Unfortunately these are often difficult to use for the non-technical user. Documentation is generally poor and there is a lack of information on issues such as key management. Stand-alone systems may be based upon symmetric key techniques involving the end-user in key generation and distribution. More efficient products are based upon a mixture of symmetric encryption for encryption of stored information, supported by asymmetric (public key) encryption for transfer of keys. Many products also require the recipient to have the same encryption product installed on his system. In some cases encryption features are included in application products such as word processing packages.

Some of the more sophisticated products are supported by a **Public Key Infrastructure** to provide for the maintenance and distribution of key material.

12.3 Electronic mail encryption

The de-facto standard for defining the content, format and capabilities of electronic mail is the Multipurpose Internet Mail Extensions (MIME) specification. MIME enables the encryption of messages and multi-media attachments. Secure MIME (S/MIME) adds security to email messages using the MIME standard. Messages are encrypted using symmetric encryption but use an asymmetric (public key) mechanism for key exchange. Note that S/MIME also provides a digital signature using a public key mechanism. S/MIME utilizes the X.509 certificate standard for the provision of certificate hierarchy. The S/MIME standard is defined in RFC 2633 [9].

S/MIME supports the Digital Encryption Standard (DES), Triple DES and RC2 for symmetric encryption and the Rivest-Shamir-Addleman algorithm (RSA) for public key encryption.

Other products such as Pretty Good Privacy (PGP) are also widely used but are not yet regarded as official standards. The main issue surrounding the use of products such as PGP is a lack of interoperability with other encryption products.

12.4 Network encryption

The industry standard network layer protocol for the Internet is the Internet Protocol (IP) standard. IP protocol is a packet switching protocol providing for the fragmentation, routing and re-assembly of packets.

The main industry standard transport layer protocol for the Internet is the Transmission Control Protocol (TCP). TCP adds reliable communication, flow control, multiplexing and connection-oriented communication to the IP services. TCP is used to communicate between client and server in a client/server environment and supports applications such as Web services, electronic mail and file transport.

Transport Layer Security (TLS) protocol was developed by the Internet Engineering Task Force (IETF) to provide encrypted communications on the Internet. TLS is based upon the proprietary product Secure Sockets Layer developed by Netscape. SSL/TLS provides transport layer communications security by encrypting the content of a TCP connection between two end points in a network. It may be used to provide security for use with protocols such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP3) and Lightweight Directory Access Protocol (LDAP) but it is mainly used to provide security between web browsers and web servers. TLS/SSL also allows sessions that are not encrypted but are authenticated and proof against tampering.

TLS/SSL has the advantage of being present in most of the common web browsers on the market. However, it should be borne in mind that it only provides security between TCP endpoints in a network; it does not provide security for stored data or application level security. The TLS standard is defined in RFC 2246 [10].

IPSec is a security architecture developed by the IETF for securing the transmission of data across IP based networks. It may be used in Transport mode to encrypt the data part of the transmitted package (i.e. routing information is sent in clear) or in Tunnel mode where the whole package is encrypted. In the former it is widely used as the mechanism for creating IP based Virtual Private Networks (VPNs). The IPSec standard is described in RFC 2401 [11].

Note that the current protocol standard for IP networks is IPv4. The successor to IPv4 is IPv6 which is compatible with IPSec.

The increasing use of voice over IP may introduce security concerns resulting from the unmanaged and unpredictable nature of voice traffic. ETSI has established the "TIPHON (Telecommunications and Internet Protocol Harmonization over Networks) group in order to establish standards initially for voice over IP networks, but now covering multimedia, end-to-end quality of service and end-to-end security.

The project's objective is to support the market for voice communication and related voiceband communication (such as facsimile) between users. It will ensure that users connected to IP based networks can communicate with users in Switched Circuit Networks (SCN - such as PSTN /ISDN and GSM, and vice versa. as well as between users in SCN, where IP-based networks are used for connection/trunking between the SCN involved.

The support comes in the production of appropriate ETSI deliverables: technical specifications and reports. In addition, the activity will include validation and demonstrations, in order to confirm the appropriateness of the solutions proposed.

Given the universal nature of IP networks, the prime goal is to produce global standards. As ETSI is essentially a European body, it recognizes that co-operation with relevant groupings in ITU-T and IETF is necessary. ETSI specifically believes that it has a role in opinion leadership and in helping to build consensus between all the major market players. The Institute co-operates closely with relevant Fora, especially the IMTC VoIP Activity Group.

The following workshop themes have been identified:

- Requirements for service interoperability, technical aspects of charging/billing and security;
- Architecture and reference configurations;
- Call control procedures, information flows and protocols;
- Naming, numbering and addressing;
- Quality of Service (QoS);
- Verification and demonstration implementation.

A major issue for the future security of network security is the potential use of many communications protocols (e.g. IP, Wireless telephony such as Bluetooth, mobile telephony) within a single transaction. Security will need to be both effective and user transparent over the transaction path. There is a requirement for the standardization bodies to develop interoperability standards which will facilitate the security of transactions over multiple protocols.

12.5 Cryptographic algorithms

ETSI SAGE (Security Algorithms Expert Group) is a task force with responsibility for standardization in the areas of cryptographic algorithms, fraud prevention, unauthorized access to private and public telecommunications services and privacy of user data. In particular SAGE has recently delivered algorithm specifications to the Third generation Partnership Project (3GPP) for the protection of confidentiality and integrity of information transmitted over some of the IMT-2000 third generation (3G) cellular communication systems.

The NESSIE project under the auspices of the Information Society Technologies (IST) has been set up to develop methods to assess the performance of cryptographic algorithms. The aim is to enable users to make informed selection of cryptographic products. More details can be found at http://www.diffuse.org.

12.6 Object re-use policy

An object re-use policy should be in place to prevent the inadvertent release of sensitive information to unauthorized individuals. This applies to unauthorized individuals within the e-business environment (i.e. in the domain of the e-business supplier or within the domain(s) of e-business users. In most cases the threat will arise if workstations or computers or magnetic media (e.g. floppy discs, tapes, CD ROMs, removable hard discs) are released for disposal. Disclosure of sensitive information may be subject to data protection legislation.

The use of secure physical disposal procedures and/or the use of reputable software based data erasure products are appropriate measures against this threat.

12.7 Recommendations

12.7.1 Encryption of stored information

The encryption of stored information is a local matter. Standards for interoperability are not relevant in the context of the present document. Best practice documents should cover this. There are no other recommendations.

12.7.2 Network and electronic mail encryption

Interoperation of encryption systems for transport and e-mail exchange is vital. There is a need to integrate e-signature properly. There is also a need to have a standard framework where encryption components can be replaced whenever needed.

Recommendation 21: The ESOs and industry standards groups should adopt appropriate existing frameworks for transport and e-mail exchange such as S-MIME.

The increasing diversity of networks (e.g. Internet, Virtual Private Networks, wireless LANs, 3G) will invariably raise interoperability problems as global e-business expands. It is likely that a specific transaction may need to utilize a number of different protocols in its path. Thus it is crucial that the various protocols (including security-related ones) must be interoperable in order to maintain the integrity and confidentiality of the data over the communications path.

Recommendation 22: ESOs and industry standards groups, including IETF, W3C, WiFi Alliance and 3GPP should maintain their efforts on open protocols and specifications that promote interoperability of secure transactions.

12.7.3 Object re-use policy

Object re-use policy is a local matter. Standards for interoperability are not relevant in the context of the present document. Best practice documents should cover this. There are no other recommendations.

13 Trust services

Trust services provide the confidence that e-business transactions have in fact been carried out by those individuals purporting to have carried them out and provide the necessary evidence that to support that fact. They ensure that commitments were made by authenticated individuals cannot be subsequently disavowed. Effective Trust Services are predicated on the fact that individuals have been subject to a rigorous registration and authentication process to establish their credentials.

The evidence created may be required to support informal or formal agreements between parties, financial transactions or legal actions between parties. In many cases it may also be necessary to retain evidence that transactions resulting from the commitment were in fact carried out.

Trust Services will often be provided by independent Trusted Service Providers (TSPs) to participants in the e-business service.

A list of completed documents can be found in annex C.

13.1 Security measures

In the context of the present document Trust Services comprises the following security measures:

a) Key Management.

b) Non-Repudiation.

c) Evidence of Receipt.

d) Trusted Commitment Service.

e) Integrity.

Other services which are commonly supplied by TSPs include archive services (e.g. long term storage of documents, key pairs, certificates), directory services and notarization services. These services are considered to be outside the scope of the present document.

Note that the activities described below may be carried out by a single TSP or a combination of TSPs.

13.1.1 Key management

The aims of key management are as follows:

a) Provide the means for the secure generation, storage, distribution, revocation, and recovery of cryptographic keys;

b) Protect secret keys from disclosure to unauthorized individuals whilst in storage or in transit;

c) Protect the integrity of archived keys and if appropriate apply **time-stamping** to indicate the validity period of the key.

d) Where appropriate provide key escrow facilities to enable key recovery under legal warrant or for business purposes. (ETSI LI group has developed several documents (including European Standards) covering standards for Lawful Interception. They are not covered in the present document but can be found at http://portal.etsi.org/li).

13.1.2 Non-repudiation

The aim of a non-repudiation service is to furnish evidence that the originator of an electronic transaction or communication must have the real world identity associated with the electronic identity. Measures which support this service are:

- At very low risk levels user identity and a transaction number may provide the appropriate level of confidence. Additional confidence may be provided using agreed **passwords** to authorize the transaction.
- Stronger measures will be based upon **electronic signatures** supported by proof of ownership of public keys.
- Procedural measures such as audit log files showing transaction times and records of system activities may be used to support the security measures.
- A secure **time-stamp** may be used to show the specific time that an e-business transaction was carried out.
- Independent Certification Authorities may be used to confirm the identity of individuals, prove the ownership of public keys and provide a **Public Key Infrastructure (PKI)** to support the generation, distribution and maintenance of key material.
- **Smart cards** may be used as signature creation devices to carry public and private keys and **digital certificates**.

13.1.3 Evidence of receipt

The aim of an evidence of receipt service is to furnish evidence that the intended recipient of an electronic transaction has in fact received the communication. Depending on the nature of the transaction the evidence provided will range from simple proof that the recipient's communication equipment or his electronic address has received the communication to proof that the communication has been delivered and read by the real world identity of the recipient. The following measures support an Evidence of Receipt service:

a) At very low risk levels simple indications that a message has been received may suffice.

b) Stronger measures will be based upon responses to the originator which are protected by appropriate non-repudiation and integrity services and possibly supported by a **PKI**.

13.1.4 Trusted commitment service

The aim of a trusted commitment service is to furnish evidence that electronic commitments (such as payments) entered into by parties to an e-business transaction have been properly authorized.

A trusted commitment service requires that the *commitment* entered into between parties to the e-business transaction is protected by an appropriate level of non-repudiation, proof of receipt and integrity service. Hence this aim is achieved by the measures defined for non-repudiation, proof of receipt and integrity.

13.1.5 Integrity

The aim of an integrity service is to furnish evidence that the contents of an electronic communication or transaction received by the recipient is the same as the communication sent by the originator and could not have been modified, either deliberately or accidentally, en route to the recipient. The following security measures protect an Integrity requirement:

a) At low risk levels, simple **checksums** may be adequate (to protect against accidental corruption for example).

b) At higher risk levels, **digital signatures** are preferred to create a signed hash of the message that is appended to the transaction by the originator and verified by the recipient. A PKI may be used to support an electronic signature regime.

13.2 Electronic signatures

An electronic signature is data in electronic form that is attached to or logically associated with other electronic subject data and serves as a means of authentication. The definition includes scanned images, signatures produced by hand-written signature capture devices and digital signatures. The present document only addresses **digital signatures**.

A *digital signature* is one form of electronic signature that uses a cryptographic transformation of the data to allow the recipient of the data to prove the origin and integrity of the subject data and to protect against forgery of the data by the recipient. A digital signature is created by encrypting a **hash** of the component to be signed (e.g. an electronic message) with the originator's private key. The digital signature is transmitted to the recipient of the message. The message recipient decrypts the digital signature with the originator's public key to prove origin and integrity of the message.

On 1999-12-13 the European Commission published Directive 1999/93/EC [12] to provide a Community framework for electronic signatures. Details can be found at 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. Individual Member States were tasked with implementing the Directive in national legislation.

The European ICT Standards Board, with a mandate from the European Commission, has 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). Further information regarding EESSI can be found at http://www.ict.etsi.org/EESSI_home.htm.

CEN/ISSS has developed documents through the operation of an open technical Workshop "E-SIGN", created specifically for this purpose. Documents developed and approved by this process are CEN Workshop Agreements (CWAs). See annex C for a list of current E-SIGN Workshop agreements. Further information is available from http://www.cenorm.be/cenorm/businessdomains/businessdomains/informationsocietystandardizationsystem/.

In ETSI, standardization in the area of electronic signatures and infrastructures is currently taking place in the ETSI Technical Committee ESI. ETSI TC ESI collaborates with interested parties and stakeholders in the marketplace including vendors, operators, user organizations and other standards bodies. The overall aim of ETSI TC ESI is to address some basic needs of secure electronic commerce and of secure electronic document exchange in general by providing specifications for a selected set of technical items that have been found both necessary and sufficient to meet minimum interoperability requirements. Examples of business transactions based on electronic signatures and public key certificates are purchase requisitions, contracts and invoice applications.

Under a Commission Decision of 14 July 2003, two CEN Workshop Agreements (CWA 14167-1 [13] and CWA 14167-2 [14]) have been cited in a "List of generally recognized standards for electronic signature products that Member States shall presume are in compliance with the requirements laid down in annex II f to Directive 1999/93/EC" and a third (CWA 14169 [15]) in a separate list of the generally recognized standards in compliance with Annex III of the Directive.

The core activity of the EESSI is drawing to a close, and the future arrangements, including for the maintenance of the standards produced, are under review.

13.3 Hash functions

A hash function is a function which compresses strings of bits (input string) to fixed length strings (output string) such that:

a) it is not computationally feasible to determine the input string from the output string; and

b) it is not computationally feasible to generate for a given output string a second different output string.

13.4 Time-stamping

A time stamping function creates a verifiable cryptographic binding between a data item (such as a digital signature) and the time the data item was generated. ISO/IEC has issued ISO/IEC 18014-1 [16] and ISO/IEC 18014-2 [17] a two part standard comprising Part 1: Framework and Part 2: Mechanisms involving independent tokens. ETSI have also produced TS 102 023 [18] *Policy requirements for time-stamping authorities*.

13.5 Non-repudiation

Non-repudiation services are intended to resolve (legal) disputes relating to a wide range of actions and events. Examples include:

a) Non-repudiation of creation. Providing proof that the originator created the message.

b) Non-repudiation of delivery. Providing proof that the intended recipient received the message and recognized the content.

c) Non-repudiation of knowledge. Providing proof that a recipient took account of the message contents.

d) Non-repudiation of origin. Providing proof that the originator created and sent message.

e) Non-repudiation of receipt. Providing proof that the intended recipient has received the message.

f) Non-repudiation of sending. Providing proof that the originator did send the message.

g) Non-repudiation of submission. Providing proof that a delivery authority accepted the message for transmission.

h) Non-repudiation of transport. Providing proof that a delivery authority has delivered the message to the intended recipient.

The standard that describes non-repudiation mechanisms is ISO/IEC 13888 [19].

13.6 Public Key Infrastructures (PKI)

In a global e-business environment a Public Key Infrastructure (PKI) is required to support the following services:

a) Registration, storage and maintenance of public keys owned by users of the e-business service.

b) Retrieval and delivery of public keys of participants in the e-business service.

c) Archive and retrieval of public key certificates for the life-time of the documents to which they refer.

d) Verification of the ownership of specific public keys.

e) Where required, the creation and distribution of public/private key pairs and symmetric keys to participants in the e-business services.

f) Key recovery for lost keys, revocation of stolen keys and, where appropriate, the provision of facilities for access to keys for law enforcement purposes (key escrow).

Various groups such as the PKIX WG, NIST, The Open Group and national governments, are developing PKI standards. There are also many commercial PKI products in the market place. In general though there is a lack of attention to interoperability requirements.

13.7 Harmonization of trust services

ETSI and CEN via the European Electronic Signature Standardization Initiative (EESSI) is undertaking work on the harmonization of trust service provider services. The scope of the work is to provide the set of specifications, which will allow interoperable provision of TSP (CA) status information to relying parties, who need to validate the trustworthiness of the service which certified the signer of a contract, transaction, etc.

The standardization effort needs the support of the different national organizations that run and supervise national certification schemes. These organizations need to be involved in the standards development, promotion and implementation process. In order to help achieve this EESSII and the UK department of Trade and Industry hosted a workshop in December 2002 aimed at reviewing a proposed standard for establishing trust in electronic signatures.

13.8 Recommendations

The growth of a global e-business environment will be facilitated by the availability of interoperable PKI products. At the current time there are many commercial PKI products available but many of these are not interoperable with other products. Though valuable work is being carried out based upon PKI interoperability testbeds at a European level in projects such as the IST project "PKI challenge" and at national level, there are as yet no international interoperability standards.

Recommendation 23: The ESOs and industry standards groups should define what features of PKI systems are necessary to provide global interoperability and work with product suppliers and with international and national testbed projects to develop specifications and standards to facilitate global interoperability.

There are several "standards" for digital signature products. In general products conforming to one standard do not interoperate with products conforming to another standard. Users unfamiliar with digital signature technology should not be expected to decide which standard to use on a specific occasion.

Recommendation 24: The ESOs and industry standards groups should continue to develop and implement compatible digital signature standards to facilitate interoperability according to market need and demand, and raise awareness of such standards.

The uptake of global e-business will be inhibited by the lack of harmonization of standards and procedures for Trust Service Providers.

Recommendation 25: The ESOs and industry standards groups should review the development of common procedures for TSPs being carried out by groups such as the UK t-Scheme with a view to their adoption as international standards. This should address in particular the procedures for the long-term archive and retrieval of essential message recovery information such as cryptographic keys, certificates, certificate revocation lists.

14 Business services

Business services refer to the applications and infrastructure within the domain of the e-business service that support the delivery of that service to the user. In this context the term e-business service will also include TSPs supporting the e-business service. Business services are intended to protect the systems and network infrastructures supporting the e-business service from non-malicious threats such as faulty hardware or software.

Business Services in the context of the present document includes applications such as web services, interactive services and electronic messaging.

A list of completed documents can be found in annex D.

14.1 Security measures

Business services comprises the following security measures:

a) Service availability.

b) Information availability.

c) Effective accounting and audit.

14.1.1 Service availability

The aim of service availability is to ensure that access to the software applications and infrastructure including web facilities comprising the e-business service is provided in a timely manner. It is supported by the following measures:

a) The use of commercial best practise products and adherence to good practise for system design, implementation and operations.

b) Ongoing **Failure Impact analysis**, **Capacity Planning**, **Business Continuity Planning** and **Configuration Management**.

c) Alternative communications facilities in case of failure, the availability of battery backup or Un-interruptible Power Supplies (UPS) need to be in place.

d) Regular testing of system recovery.

e) Service Level Agreements setting out availability targets with clients of the service.

14.1.2 Information availability

The aim of information availability is to ensure that access to the information associated with the required e-business service is provided in a timely manner. Measures to aid information recovery after an accidental interruption to service include:

a) A planned programme of information data backups.

b) Technical measures such as **checksums** or **cyclic redundancy checks** to safeguard the integrity of system software, configuration data and storage facilities.

c) Regular testing of Recovery Plans.

d) A password or key recovery mechanism should be provided to users of the service in cases where a password has been lost.

14.1.3 Effective accounting and audit

The aim of accounting and audit is to ensure that relevant user related information is recorded for specified user transactions. The service will also provide the means to record and analyse client and service transactions that could compromise the service. The level of accounting and audit will depend upon the assessed impact of a failure but may include:

a) **Accounting:** Recording of client information for each transaction undertaken (e.g. client identifier, time of transaction, type of transaction, success or failure of transaction, current transaction status).

b) **Audit:** The capability to display and carry out detailed analysis of accounting records.

c) The requirement to protect the confidentiality, integrity and availability of audit logs particularly in cases where transactions are financial in nature or are legally binding or may be subject to legal requirements such as data protection.

14.2 Failure impact analysis

Failure impact analysis determines the impact of failure of a service component upon the e-business provider. The analysis may need to take into account external factors (such as time of year that may affect the impact.

14.3 Capacity planning

E-business service providers must assess the potential load on the service and ensure that the system and network infrastructure is sufficient to meet current and forecasted future demand in accordance with agreed availability targets.

14.4 Business continuity planning

A business continuity plan is required to cover the following activities:

a) Management roles and responsibilities for business continuity;

b) Recovery procedures and audit trails;

c) Security related recovery actions.

Though guidance documents on Business Continuity Planning exist at national and industry sector level there is as yet no internationally approved standards.

14.5 Configuration management

A configuration management plan identifies the processes, information systems and communications components that make up the e-business service. The plan identifies all components that are affected by specific changes to the system configuration.

14.6 Checksums and cyclic redundancy checks

These functions detect a loss of integrity in a data item. A checksum detects changes in data by calculating a number such as sum of all the bits of a data item to be transmitted. The checksum is transmitted with the data item and is subsequently compared with a checksum created from the transmitted data item. A cyclic redundancy check uses a more complicated formula to determine a function of the transmitted data item for subsequent comparison.

14.7 Recommendations

There is a lack of advice on general security guidance, standards and operating procedures for organizations wishing to set up e-business applications in Europe. This not only inhibits growth but may lead to the development of interoperable ad-hoc services.

Recommendation 26: The ESOs should identify or support the development of security frameworks to support e-business security standards and technologies and operational codes of practice.

15 Network defence services

Network defence services provide the means by which *malicious* threats emanating from electronic connection to external IT resources and networks (including the Internet) are countered. If such threats materialize they may have one or more of the following effects:

a) Undermine the continued availability of the e-business services;

b) Compromise the integrity of the e-business services or information;

c) Cause damage to user systems connected to the e-business services.

A list of completed documents can be found in annex E.

15.1 Security measures

The aim of network defence is protect the network infrastructure from electronic attack. There are two types of security measures which provide protection:

a) Measures that *prevent* the attack taking place;

b) Measures that *detect* the attack.

15.1.1 Preventative measures

Preventative measures comprise a combination of procedural and technical measures:

a) Processes that prevent the automatic execution of imported macros in the absence of express permission for their execution;

b) Effective, current **anti-virus policies**. Screening of all imported and exported material for recognizable virus signatures. Recording of all imports transaction for audit purposes.

c) Procedures that discourage employees of e-business service providers from accessing web sites that are not pertinent to their job function. Import of material should be controlled and limited as far as possible to that which is necessary to carry out their job. Where software is imported it should preferably be restricted to "trusted" (i.e. digitally signed) objects. Where appropriate **PKI-based certification** of software objects should be used.

d) Using suitably configured **firewalls** to prevent hacking attacks. System responses to service refusals should be designed to prevent a potential hacker deducing useful system information such as physical IP addresses (see note).

e) Restricting access to e-business services in accordance with agreed user profiles.

f) Setting up arrangements with an appropriate national or international security incident and response organization (CERT) to obtain information about potential attacks and to report and disseminate security incidents. For further information about CERTS see http://www.ecsirt.net.

NOTE: Firewalls which are effective against IPv4 may not be effective against the emerging IPv6 protocol.

15.1.2 Detection measures

The main technical measure is the deployment of **Intrusion Detection Systems**. These are designed to detect unusual activity on the network. Additionally **Penetration Tests** may be used periodically to identify potential vulnerabilities in the system and associated network infrastructure.

15.2 Recommendations

Many home users will be unfamiliar with computer security and would benefit from the availability of guidance in the form of security checklists.

Home users in particular may be generally unaware of the need for PC-based software to be resistant to attack. In a global e-business environment this could increase the spread of malicious software such as computer viruses. In response to increased security threats and market demand, developers of application software are continuing to enhance and improve the security of their products.

Recommendation 27: ESOs, industry standards groups and European SME associations should contribute to the development of best practice security guides for home users and SMEs including, for instance, the need for users to implement and maintain antivirus software.

Application software to support the home user (e.g. PC operating systems, word processing packages, spreadsheet packages etc.) will be expected to be resistant to attack.

Recommendation 28: ESOs and industry standards groups should continue to work with product suppliers in order that system and application software for the home user is not vulnerable to attack.

Many devices in the home will contain embedded microcontrollers and will become accessible from the Internet and thus vulnerable to attack. Because, in many cases, they operate independently of human input, the establishment of automatic and remote methods of protection are necessary together with codes of practice and standards that underpin them. Since the average home user will be generally unaware of network security, this should be regarded as a major area of concern for Network and Information Security.

Recommendation 29: The ESOs and industry standards groups should continue to develop standard protocols, for a secure, intelligent home, where Internet-enabled microcontrollers are embedded in different household appliances.

16 Assurance services

Previous clauses address the security measures that counter the threats to the security of networks and information systems providing e-business services. In order to encourage the use of electronic services it is important that potential users of the service have confidence that all those technical and non-technical security measures have been designed, configured and are being operated in a secure manner. The aim of Assurance Services is to provide that confidence.

Confidence in an e-business service will also be increased if the organization providing the service conforms to an internationally recognized standard for the overall management of Information Security.

A list of current standards and guidance documents can be found in annex F.

16.1 Security measures

In the context of the present document assurance services comprise the following security measures:

a) Risk assessment.

b) Evaluation.

c) Certification.

d) Accreditation.

16.2 Risk assessment

A risk assessment is carried out to determine the probability and impact of the threats to assets.

ISO/IEC TR 13335-2 [20] together with ISO/IEC TR 13335-3 [21] and ISO/IEC TR 13335-4 [22] is a recognized international reference on security risk management. There are also in existence a number of national and international risk assessment methodologies.

Guidance material has also been issued for specific sectors (national and international) and by industrial and academic consortia.

16.3 Evaluation

Evaluation is a detailed examination of IT products and systems with the aim of determining whether the security functions that make up the security measures are implemented to the appropriate level as required by the risk assessment.

During evaluation, an IT product or system is known as a Target of Evaluation (TOE). Such TOEs include, for example, operating systems, computer networks, distributed systems, and applications.

The main international standard for evaluation is ISO/IEC 15408 [23]; also known as the Common Criteria (CC). The Common Criteria were originally developed to align the European (ITSEC), US (TCSEC) and Canadian (CTCPEC) evaluation schemes. Though CC is intended to replace these schemes they are still being used in certain applications.

The US National Institute of Standards and Technology has issued FIPS 140-2 [24] (which supersedes FIPS 140-1, although FIPS 140-1 is still applicable for former evaluations) aimed at the evaluation of cryptographic modules. The Federal Information Processing Standards Publication Series (FIPS) of the National Institute of Standards and Technology (NIST) of the United States of America comprise official publications relating to standards and guidelines adopted and promulgated for improving the utilization and management of computer and related telecommunications systems in the USA Federal Government. Currently laboratories accredited by the USA Federal Government to carry out FIPS 140-2 conformance are based in the US, Canada and the UK. Work is being undertaken in ISO/IEC JTC1/SC27 (project NP 19790 "Security Requirements for Cryptographic Modules") to convert FIPS 140-2 into an international standard.

Other standards for cryptographic modules have been developed within the EESSI project as Common Criteria Protection Profiles. These standards have been published as CEN Workshop Agreements (CWA 14167-2 [14]and CWA 14167-3 [25]).

16.4 Certification

Two forms of information security certification are currently available:

a) Certification of security-evaluated IT products and systems;

b) Certification of an Information Security Management System (ISMS).

Certification of IT products and systems is done on the basis of evaluation as described in the preceding clause. IT products/systems are often changed, modified, or enhanced and are therefore subject to surveillance in order to ensure continued compliance with the criteria.

Certification of ISMS is a procedure, which assesses the management system of an organization against a recognized standard and provides written assurance that the ISMS conforms to the standard. It also assesses whether an organization has carried out a risk assessment of its operations and has implemented appropriate security measures to counter the assessed risk. Discussions are currently taking place within various European standards groups to agree a common standard for certification. Some European countries have adopted BS7799-2 as their own national standard and are using the present document to assess ISMS compliance, but this has yet to achieve international acceptance. ISO/IEC JTC1/SC27 are discussing this topic in the SC27 ISMS Study Project and as part of the formal ISO Guide 72 [26] assessment.

Organizations that could provide certification services with accredited people should be independent of any other security consulting service and assessed by National Accreditation Bodies (see below) against internationally accepted criteria so that users will have confidence in the certification process and ultimately the services of the certified organization.

16.5 Information security management standards

There are several international and industry standards and recommended codes of practice for Information Security Management. They are listed in clause F.1.

In addition there are other national and international standards aimed at specific sector requirements (e.g. government, banking) as well as guidelines issued by industry (such as the International Security Forum) and academic consortia.

16.6 Accreditation bodies

National accreditation bodies are set up to accredit nation certification organizations based upon strict independability. They are signatories to international agreements in order that the methods and practices of Certification Bodies conform to international standards and guidelines and ensure the consistency and mutual recognition of certificates on a global basis.

Accreditation standards, guidance, procedures and agreements are developed by international and European groupings including the ISO Committee on Conformity Assessment (ISO CASCO), EOTC the European Organization for Conformity Assessment (EOTC) and the European co-operation for Accreditation (EA). More information on these organizations can be found at the respective web sites: http://www.iso.ch/, http://www.eotc.be, http://www.european-accreditation.org/.

16.7 Recommendations

There continues to be a need for internationally recognized compatible certification standards against which an organization's Information Security Management System can be assessed. Such standards should also take account of the fact that costly certification is unlikely to attract widespread support from users particularly for smaller companies and/or where smaller systems are concerned. They should also take into account the need for clarity in what certification achieves, in order to meet the reasonable expectations of their users.

Also current certification procedures do not lend themselves to complex and continuously evolving systems. There is a need to review the certification process for such systems which needs to be fast, effective and affordable.

Recommendation 30: ESOs should encourage the speedy acceptance of internationally recognized and compatible certification standards.

Annex A:
Standards for registration and authentication services

A.1 General authentication standards

A.1.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO/IEC 11131: "Banking - Financial Institution Sign-On Authentication".
- ISO/IEC 9594-8: "Directory Authentication".
- ISO/IEC 9797: "Message Authentication Codes (MACs)". A two part standard comprising:
  - Part 1: "Mechanisms using a block cipher".
  - Part 2: "Mechanisms using a hash-function".
- ISO/IEC 9798: "Entity Authentication":
  - Part 1: "General Model".
  - Part 2: "Entity Authentication Mechanisms using a Symmetric Algorithm".
  - Part 3: "Entity Authentication Using a Public Key Algorithm".
  - Part 4: "Entity Authentication Using Cryptographic Check Function".
  - Part 5: "Entity Authentication Using Zero Knowledge Techniques".
- ISO/IEC 15816:2002/ ITU-T Recommendation X.841: "Security information objects for access control".
- ISO/IEC 10181: "Security Frameworks":
  - Part 1: "Overview".
  - Part 2: "Authentication".
  - Part 3: "Access Control".
  - Part 4: "Non-Repudiation".
  - Part 5: "Integrity".
  - Part 6: "Confidentiality".
  - Part 7: "Audit".
  - Part 8: "Key Management".

A.1.2 European Telecommunications and Standards Institute (ETSI)

- ETSI ETS 300 331 (1995): "Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM)".
- ETSI ETS 300 759 (1997): "Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM); Test specification for DAM".

- ETSI ETS 300 760 (1997): "Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM); Implementation Conformance Statement (ICS) proforma specification".
- ETSI I-ETS 300 768 (1997) - (Historical): "Private Integrated Services Network (PISN); Cordless Terminal Mobility (CTM); Authentication; Service description".
- ETSI I-ETS 300 769 (1997) - (Historical): "Private Integrated Services Network (PISN); Cordless Terminal Mobility (CTM); Authentication; Functional capabilities and information flows".
- ETSI ETS 300 825 (1997): "Digital Enhanced Cordless Telecommunications (DECT); 3 Volt DECT Authentication Module (DAM)".
- ETSI ETS 300 841 (1998): "Telecommunications security; Integrated Services Digital Network (ISDN); Encryption key management and authentication system for audiovisual services".
- ETSI EN 301 492-1 (V1.1.2): "Private Integrated Services Network (PISN); Inter-exchange signalling protocol; Cordless terminal authentication supplementary services; Part 1: Test Suite Structure and Test Purposes (TSS&TP) specification for the VPN "b" service entry point".
- ETSI EN 301 492-2 (V1.1.1): "Private Integrated Services Network (PISN); Inter-exchange signalling protocol; Cordless terminal authentication supplementary services; Part 2: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT) proforma for the VPN "b" service entry point".
- ETSI EN 301 492-2 (V1.2.1): "Private Integrated Services network (PISN); Inter-exchange signalling protocol; Cordless terminal authentication supplementary services; Part 2: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT) proforma specification for the VPN "b" service entry point".
- ETSI EN 301 828 (V1.1.1): "Private Integrated Services Network (PISN); Specification, functional model and information flows; Wireless terminal authentication supplementary services [ISO/IEC 15432 (1999) modified]".
- ETSI TR 101 052 V1.1.1 (1997-06): Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard authentication and key management algorithm set TAA1
- ETSI TR 133 902 (V4.0.0): "Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol (3GPP TR 33.902 version 4.0.0 Release 4)".
- ETSI TR 133 902 (V3.1.0): "Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol (3G TR 33.902 version 3.1.0 Release 1999)".
- ETSI TS 135 205 (V4.0.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1,f1*,f2,f3,f4,f5 and f5*; Document 1: General (3GPP TS 35.205 version 4.0.0 Release 4)".
- ETSI TS 135 205 (V5.0.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General (3GPP TS 35.205 version 5.0.0 Release 5)".
- ETSI TS 135 206 (V5.0.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification (3GPP TS 35.206 version 5.0.0 Release 5)".
- ETSI TS 135 206 (V4.0.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Specification (3GPP TS 35.206 version 4.0.0 Release 4)".

- ETSI TS 135 207 (V4.0.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' Test Data (3GPP TS 35.207 version 4.0.0 Release 4)".
- ETSI TS 135 207 (V5.0.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document3: Implementors' test data (3GPP TS 35.207 version 5.0.0 Release 5)".

A.1.3 US National Institute of Standards and Technology

- FIPS Pub 83: "Guideline on User Authentication Techniques for Computer Network Access Control".
- FIPS Pub 190: "Guideline for the use of Advanced Authentication Technology Alternatives".
- FIPS Pub 196: "Entity Authentication using Public Key Cryptography".
- NIST Spec Pub 800-9: "Good Security Practices For Electronic Commerce, Including Electronic Data Interchange".
- NCSC-TG-017: "A Guide to Understanding Identification and Authentication in Trusted Systems".

A.1.4 Internet Engineering Task Force (IETF)

- IETF RFC 1411: "Telnet Authentication: Kerberos Version 4".
- IETF RFC 1412: "Telnet Authentication: SPX".
- IETF RFC 1413: "Identification Protocol".
- IETF RFC 1414: "Identification MIB".
- IETF RFC 1416: "Telnet Authentication Option".
- IETF RFC 3244: "Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols".
- IETF RFC 1510: "The Kerberos Network Authentication Service (V5)".
- IETF RFC 1734: "POP3 AUTHentication command".
- IETF RFC 1828: "IP Authentication using Keyed MD5".
- IETF RFC 1961: "GSS-API Authentication Method for SOCKS Version 5".
- IETF RFC 1994: "PPP Challenge Handshake Authentication Protocol (CHAP)".
- IETF RFC 2015: "MIME Security with Pretty Good Privacy (PGP)".
- IETF RFC 2025: "The Simple Public-Key GSS-API Mechanism (SPKM)".
- IETF RFC 2069: "An Extension to HTTP: Digest Access Authentication".
- IETF RFC 2082: "RIP-MD5 Authentication".
- IETF RFC 2085: "HMAC-MD5 IP Authentication with Replay Prevention".
- IETF RFC 2138: "Remote Authentication Dial In User Service (RADIUS)".

A.1.5 Institute of Electrical Engineers

- 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".

A.2 Passwords

A.2.1 Internet Engineering Task Force (IETF)

- IETF RFC 1929: "Username/Password Authentication for SOCKS V5".
- IETF RFC 1760: "The S/KEY One-Time Password System (SKEY)".
- IETF RFC 2289: "A One-Time Password System (OTP)".

A.2.2 US National Institute of Standards and Technology

- FIPS Pub 112: "Standard on Password Usage.

A.2.3 US National Computer Centre

- CSC-STD-002-85: "Password Management Guidelines".

A.3 Biometrics

Though there are very few issued standards on biometrics there are numerous groups carrying out activities which could lead to the development of useful standards.

A.3.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- NP 19792: "A framework for security evaluation and testing of biometric technology".
- ISO/IEC/JTC1/SC17 work groups:
  - WG1: "Physical Characteristics of Smart Cards (e.g. location of fingerprint sensor on card)".
  - WG3: "Machine readable travel documents".
  - WG4: "Smart Cards: ISO/IEC 7816 Personal verification through biometrics".
  - WG10: "Motor Vehicle Driver Licenses: Biometrics and Encryption".
  - WG11: "Biometrics: development of BioAPI and CBEFF (see below) into ISO standards".
- ISO/IEC/JTC1/SC 37: The aim of SC37 is to accelerate the development and adoption of Biometrics standards such as BioAPI and CBEFF through the ISO process. Six workgroups have been set up:
  - WG1: "Harmonized Biometric Exchange Framework Format (CBEFF)".
  - WG2: "Biometric Technical Interfaces".
  - WG3: "Biometric Data Interchange Formats".
  - WG4: "Profiles for Biometric Applications".

- WG5: "Biometric Testing and Reporting".
- WG6: "Cross-Jurisdictional and Social Aspects".

A.3.2 ANSI/NIST

- ITL-2000: "Data Format for the interchange of Fingerprint, Facial and Scar Mark/Tattoo".
- X9.84: "Biometrics Management and Security for the Financial Services Industry".
- CBEFF: "Common Biometric Exchange Format".
- BioAPI version 1.1: "Application Programming Interface defines a generic way of interfacing to a broad range of biometric technologies".
- B10.8/AAMVA: "Driving Licenses and Identification. Format for fingerprint minutiae on Driving Licenses".
- Various other ANSI/NIST activities include Performance Testing Methodologies, Assurance, Protection Profiles, and Best Practices.

A.3.3 Other Organizations/Activities

- **European Biometrics Forum/Biovision:** A European Union funded initiative conceived in Framework 5, the programme being carried out in Framework 6. The aim is to produce a "road map" for Biometrics.
- **UK Government:** The UK Biometrics User Group comprising a group of vendors, standards developers and users is organized by the UK National Technical Authority for Information Security (CESG) and mainly funded by the Office of the e-Envoy. The group includes representatives from the US, Canada and Germany. It is active in developing Performance Standards, Best Practice guidance, Protection Profiles and Common Criteria Evaluation Methodology. It is intended that Protection Profiles and Common Criteria may be issued under the ISO Common Criteria standard in due course. Discussions are taking place between the US Biometrics Office to attempt to rationalize the UK developed Protection Profiles and the US Protection Profiles.
- **Biometric Consortium:** A US government based group acting as a focal point for research, development, testing evaluation and application of biometric-based personal identification and verification technologies.
- **US Government:** In the US the NSA and the DoD carry out research into Biometrics. The DoD has established the Biometrics Management Office to ensure the availability of biometrics technologies within the DoD.
- **International Civil Aviation Organization (ICAO):** The ICAO has developed a global harmonized blueprint for the integration of biometric identification information into passports and other biometric-enhanced machine readable travel documents. More information can be found at http://www.icao.org.

A.4 Digital certificates

A.4.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Authentication framework, the ISO/IEC version of the ITU-T Recommendation X.509".

A.4.2 European Standards Committee (CEN)

Workshop Agreements:

- CWA 14167-1 (2001): "E-Trustworthy Systems: System Security Requirements".
- CWA 14167-2 (2002): "E-Trustworthy Systems: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)".
- CWA 14167-3: "E-Trustworthy Systems: Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)".

A.4.3 European Telecommunications and Standards Institute (ETSI)

Technical Specifications

- ETSI TS 101 456 (V1.2.1): "Policy requirements for certification authorities issuing qualified certificates".
- ETSI TS 102 042 (V1.1.1): "Policy requirements for certification authorities issuing public key certificates".
- ETSI TS 101 862 (V1.2.1): "Qualified certificate profile".

A.4.4 Internet Engineering Task Force (IETF)

- IETF RFC 1422: "Privacy Enhancement for Internet Electronic Mail: Part II".
- IETF RFC 2693: "SPKI Certificate Theory".
- IETF RFC 3039: "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".

A.4.5 ANSI

- ANSI X9.30: "Digital Signature Standard, provides details of the Digital Signature Standard promulgated as FIPS 186".
- ANSI X9.45: "Authorization Certificates".
- ANSI X9.55: "Certificate Extensions for X9".
- ANSI X9.57: "Certificate Management techniques for public key certificates used in the financial sector".

A.4.6 US National Institute of Standards and Technology

- FIPS Pub 196: "Entity Authentication using Public Key Cryptography".
- NIST Spec Pub 800-15: "Minimum Interoperability Specifications for PKI Components (MISPC)".

A.4.7 RSA Public Key Cryptography Standards

- PKCS #6: "Extended Certificate Syntax, a syntax for extended certificates based upon X.509".
- PKCS #9: "Selected Attribute Syntax for PKCS #6 extended certificates, PKCS #7 digitally signed messages, and PKCS #8 private-key information".
- PKCS #10: "Certificate Request Syntax. describing a syntax for certification requests".

A.5 Smart Cards

A.5.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO/IEC 7816: "Identification cards - Integrated circuit(s) cards with contacts. A ten-part standard addressing the physical characteristics of smart cards. Details can be found at http://www.iso.ch/.
- ISO/IEC 10202: "Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards. An eight part standard which 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.

A.5.2 European Standards Committee - Information Society Standardization System (CEN/ISSS)

The following standards (European Norms) have been issued by CEN.

- EN 726: "Identification Card Systems - Telecommunications Integrated circuit cards and terminals. A seven part standard comprising":
  - Part 1: "Systems Overview".
  - Part 2: "Security Framework".
  - Part 3: "Application independent card requirements".
  - Part 4: "Application independent card related terminal requirements".
  - Part 5: "Payment Methods".
  - Part 6: "Telecommunications features".
  - Part 7: "Security Module".
- EN 1038: "Identification Card Systems, Telecommunications applications- integrated circuit(s) card payphone".
- ENV 1257: "Identification card systems - Rules for Personal Identification Number handling in intersector environments. A three part standards comprising":
  - Part 1: "PIN presentation".
  - Part 2: "PIN protection".
  - Part 3: "PIN verification".
- ENV 1284: "Identification card systems - Intersector rules for locking and unlocking of integrated circuit(s) cards".
- EN 1332: "Identification card systems - Man-machine interface. A four part standard comprising":
  - Part 1: "Design principles for the user interface".
  - Part 2: "Dimensions and location of a tactile identifier for ID-1 cards".
  - Part 3: "Key Pads".
  - Part 4: "Coding of user requirements for people with special needs".
- EN 1362: "Identification card systems- Device interface characteristics - classes of device interfaces".

- EN 1375: "Identification card systems- intersector integrated circuit(s) card additional formats -ID -000 card size and physical characteristics".
- EN 1387: "Machine readable cards- Health care applications - Cards: general Characteristics".
- EN 1545: "Identification Card Systems - surface Transport Applications. A two part standard comprising":
  - Part 1: "General data elements".
  - Part 2: "Transport payment related elements".
- EN 1546: "Identification card systems - Inter-sector electronic purse. A four part standard comprising":
  - Part 1: "Definitions, concepts and structure".
  - Part 2: "Security Architecture".
  - Part 3: "Data elements and interchanges".
  - Part 4: "Data objects".
- CR 1750: "Identification Card systems - Inter-sector messages between devices and hosts - Acceptor to acquirer messages".
- ENV 1855: "Identification card systems - Inter-sector messages between devices and hosts - Acceptor to enquirer messages".
- EN 1867: "Machine-readable cards - Healthcare applications - Numbering system and registration procedure for issuer identifiers".
- EN ISO/IEC 7810: "See ISO/IEC 7810 above".
- CR 13643: "Machine-readable cards - Healthcare applications - Logical data structures and concepts for different card technologies for use by patients in health applications".
- CR 13644: "Machine-readable cards - Healthcare applications - Logical organization of data on healthcare professional cards".
- CR 13875: "Identification card systems - Inter-sector thin flexible cards - Security features".
- CR 13909: "Identification card systems - Inter-sector thin flexible cards - Acceptance criteria".
- ENV 14062: "Identification card systems - Surface transport applications - Electronic fee collection. A two part standard comprising":
  - Part 1: "Physical characteristics, electronic signals and transmission protocols".
  - Part 2: "Electronic fee collection - Message requirements".

The following Workshop Agreements are available from CEN:

- CWA 14174: "Financial transactional IC card reader (FINREAD)". An eight part CWA standard comprising:
  - Part 1: "Business requirements".
  - Part 2: "Functional Requirements".
  - Part 3: "Security Requirements".
  - Part 4: "Architectural overview".
  - Part 5: "Download file format".
  - Part 6: "Definition of the virtual machine".
  - Part 7: "FINREAD card reader application programming interfaces (APIs)".

  - Part 8: "FINREAD client application programming interfaces (APIs)".

- CWA 13987: "Smart Card Systems - Interoperable Citizen Services - User Related Information (based on DISTINCT)". A three part CWA comprising:

  - Part 1: "Definition of User Related Information".

  - Part 2: "Implementation Guidelines".

  - Part 3: "Guidelines to Creating, Operating and Maintaining an Interoperable Network".

CEN is also working on the following smart card specifications (see the CEN web page http://www.cenorm.be/isss) for the latest status of these documents:

- CEN pr TS 1332-5: "Identification card systems - Man-machine - interface - Tactile identification of applications-embossed symbols for the differentiation of applications of ID1 cards".

- CEN pr TS IOPTA: "Identification card systems - Interoperable public transport applications - Ticketing applications".

- CEN pr TS 14062-3: Identification card systems - Electronic fee collection - Part 3: Application and security aspects".

- CEN pr TS 14062-4: "Identification card systems - Electronic fee collection - Part 4: Test procedures".

- EN ISO/IEC 7810: "Identification cards - Physical characteristics".

- EN 13343: "Identification card systems - Telecommunications IC cards and terminals - Test methods and conformance testing for EN 726-3".

  - Part 1: "Implementation Conformance Statement (ICS) proforma specification".

  - Part 2: "Test suite structure and test purposes (TSS and TP)".

  - Part 3: "Abstract test suite (ATS) and implementation for testing (IXIT) proforma specification".

- EN 13344: "Identification card systems - Telecommunications IC cards and terminals - Test methods and conformance testing for EN 726-4".

  - Part 1: "Implementation conformance statement (ICS) proforma specification".

  - Part 2: "Test Suite Structure and Test Purposes (TSS&TP)".

  - Part 3: "Abstract test suite (ATS) and implementation eXtra information for testing (IXIT) proforma specification".

- EN 13345: "Identification card systems - Telecommunications IC cards and terminals - Test methods and conformance testing for EN 726-7".

  - Part 1: "Implementation conformance statement (ICS) proforma specification".

  - Part 2: "Test suite structure and test purposes (TSS and TP)".

  - Part 3: "Abstract test suite (ATS) and implementation eXtra information for testing (IXIT) pro-forma specification".

Other CEN Activities:

- CEN Technical Committees 224, 251 and 278 are carrying out application specific work on smart cards in the areas of healthcare, transport and people with special needs.

- CEN/ISSS Workshop FINREAD validated a set of technical specifications produced by a consortium of banking interests for a secure IC card reader for bankcard payments and remote banking services delivered over the Internet and open networks. CEN/ISSS Workshop Embedded FINREAD is now extending the specification to card acceptance devices linked to mobiles, PDAs and set-top boxes. The FINREAD specifications are available from the CEN web site for downloading - see clause A.5 for details.

- A new CEN/ISSS Workshop was launched in September 2003 for European Electronic Authentication, to cover a functional architecture and required IAS (Identification, authentication and electronic signature) characteristics for a European Public Identity using smart cards and other aspects related to multi-application cards and user best practice. This will take the major results of the Smart Card Charter activity and collaborate with similar work in Japan and the US.

A.5.3 European Telecommunications and Standards Institute (ETSI)

ETSI is also carrying out a considerable amount of work under the Smart Card Project (EP SCP) approved in March 2000 to replace the SMG Technical Sub-Committee SMG9.

EP SCP provides a central focus for the standardization of a common Integrated Circuit (IC) card platform for 2G and 3G mobile communication systems. It also enables the participation of companies involved in standardization work in 3GPP, 3GPP", GAIT, T1P1, TR45 and other related activities.

The following lists technical reports issued and maintained by the smart card committee (EP SCP) and active work items. More information can be found on the SCP portal in the "Work Item Monitoring" window.

- ETSI TS 101 220 (V6.0.0): "Smart Cards; ETSI numbering system for telecommunication application providers (Release 6)".
- ETSI TS 102 124 (V6.0.0): "Smart Cards; Transport Protocol for UICC based Applications; Stage 1 (Release 6)".
- ETSI TR 102 151 (V6.0.0): "Smart Cards; Measurement of Electromagnetic Emission of SIM Cards (Release 6)".
- ETSI TS 102 221 (V3.6.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)".
- ETSI TS 102 221 (V4.5.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)".
- ETSI TS 102 221 (V3.5.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)".
- ETSI TS 102 221 (V4.4.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)".
- ETSI TS 102 221 (V3.0.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)".
- ETSI TS 102 221 (V3.1.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)".
- ETSI TS 102 221 (V4.0.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)".
- ETSI TS 102 221 (V3.2.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)".
- ETSI TS 102 221 (V4.1.0)): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)".
- ETSI TS 102 221 (V3.3.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)".
- ETSI TS 102 221 (V4.2.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)".
- ETSI TS 102 221 (V3.4.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)".

- ETSI TS 102 221 (V4.3.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)".
- ETSI TS 102 221 (V3.9.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)".
- ETSI TS 102 221 (V4.8.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)".
- ETSI TS 102 221 (V5.2.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 5)".
- ETSI TS 102 221 (V3.8.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)".
- ETSI TS 102 221 (V4.7.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)".
- ETSI TS 102 221 (V5.1.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 5)".
- ETSI TS 102 221 (V3.7.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)".
- ETSI TS 102 221 (V4.6.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)".
- ETSI TS 102 221 (V5.0.0): "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 5)".
- ETSI TS 102 223 (V4.3.0): "Smart cards; Card Application Toolkit (CAT) (Release 4)".
- ETSI TS 102 223 (V5.0.0): "Smart cards; Card Application Toolkit (CAT) (Release 5)".
- ETSI TS 102 223 (V4.0.0): "Smart cards; Card Application Toolkit (CAT);(Release 4)".
- ETSI TS 102 223 (V4.1.0): "Smart cards; Card Application Toolkit (CAT);(Release 4)".
- ETSI TS 102 223 (V4.2.0): "Smart cards; Card Application Toolkit (CAT) (Release 4)".
- ETSI TS 102 224 (V6.0.0): "Smart Cards; Security mechanisms for UICC based Applications - Functional requirements (Release 6)".
- ETSI TS 102 225 (V6.0.0): "Smart Cards; Secured packet structure for UICC based applications (Release 6)".
- ETSI TS 102 225 (V6.1.0): "Smart Cards; Secured packet structure for UICC based applications (Release 6)".
- ETSI TS 102 226 (V6.0.0): "Smart Cards; Remote APDU Structure for UICC based Applications (Release 6)".
- ETSI TS 102 226 (V6.1.0): "Smart Cards; Remote APDU structure for UICC based applications (Release 6)".
- ETSI TS 102 226 (V6.2.0): "Smart Cards; Remote APDU structure for UICC based applications (Release 6)".
- ETSI TS 102 226 (V6.3.0): "Smart Cards; Remote APDU structure for UICC based applications (Release 6)".
- ETSI TS 102 230 (V4.1.0): "Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification (Release 4)".
- ETSI TS 102 230 (V3.1.0): "Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification (Release 1999)".
- ETSI TS 102 230 (V4.0.0): "Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification (Release 4)".

- ETSI TS 102 230 (V3.2.0): "Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification (Release 1999)".
- ETSI TS 102 230 (V4.2.0: "Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification (Release 4)".
- ETSI TS 102 240 (V6.0.0): "Smart Cards; UICC Application Programming Interface and Loader Requirements; Service description (Release 6)".
- ETSI TR 122 907 (V3.1.3): "Universal Mobile Telecommunications System (UMTS); Terminal and smart card concepts (3G TR 22.907 version 3.1.3 Release 1999)".
- ETSI TS 101 220 (V5.1.0): "Smart Cards; ETSI numbering system for telecommunication application providers (Release 5)".
- ETSI TS 102 221: "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Releases 1999 to 5)".
- ETSI TS 102 222: "Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications (Release 1999)" compliant with ISO/IEC 7816.
- ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT) (Releases 4 and 5)".
- ETSI TS 102 224: "Smart Cards; Security mechanisms for UICC based Applications - Functional requirements (Release 6)".
- ETSI TS 102 225: "Smart cards; Secured packet structure for UICC based applications (Release 6)".
- ETSI TS 102 226: "Smart Cards; Remote APDU structure for UICC based applications (Release 6)".
- ETSI TS 102 230: "Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification (Releases 1999 and 4)" corresponding to the core specification in TS 102 221.
- ETSI TS 102 240: "Smart Cards; UICC Application Programming Interface and Loader Requirements; Service description (Release 6)".

SCP WG 1 work items:

- ETSI TR 102 242: "Smart Cards; Terminal - card interface; Considerations on robustness improvements".
- ETSI TS 102 221: "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 6)" (class D voltage).
- ETSI TR 102 151: "Smart Cards; Measurement of Electromagnetic Emission of SIM Cards".
- MI/SCP-00500: "Smart Cards; Support for Large Files on the UICC".
- MI/SCP-00501: "Smart Cards; Advanced UICC Communication".
- ETSI TS 102 124: "Smart Cards; Transport Protocol for UICC based Applications; Stage 1".
- DTR/SCP-010009: "Smart Cards; Architecture of the UICC".
- MI/SCP-010004: "Smart Cards; UICCng (Next Generation UICC)".
- RTS/SCP-010010: "Smart Cards; Update of TS 102 221 regarding smaller card size".

SCP WG 2 work items:

- ETSI TS 102 222: "Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications (Release 6)".
- RTS/SCP-020001: "Smart Cards; Update of TS 102 225 and TS 102 226 to GlobalPlatform 2.1".

SCP WG 3 work items:

- ETSI TS 102 241: "Smart Cards; UICC Application Programming Interface (UICC API) for Java Card (TM)".

SCP has established direct liaisons with the relevant bodies of all committees involved in elaborating the common platform. In particular, SCP has direct liaisons with ETSI TC SEC involved in the specification of security matters. In addition, SCP has liaison with CEN TC224. Other liaisons with regional and national bodies remain to be identified.

For further information on SCP liaison activities see:
http://webapp.etsi.org/Forawatch/HOME.ASP?TB=534&FIND=SEARCH_TB.

ETSI has also published numerous specifications regarding authentication for mobile telephony. The specifications may be downloaded from the ETSI web site (http://www.etsi.org).

A.5.4 Personal Computer Smart Card Workgroup

The Personal Computer Smart Card workgroup comprising Groupe Bull, Hewlett Packard, Microsoft, Schlumberger and Siemens Nixdorf (see http://www.pcscworkgroup.com/) has developed a specification to facilitate interoperability in a PC environment. The "PC/SC Specification 1.0" is in eight parts as follows:

- Part 1: "Introduction and Architecture overview".
- Part 2: "Interface Requirements for Compatible Smart cards and Interface Devices".
- Part 3: "Requirements for PC-Connected Interface Devices".
- Part 4: "IFD Design Considerations and Reference Design Information".
- Part 5: "ICC Resource Manager Definition".
- Part 6: "ICC Service Provider Definition".
- Part 7: "Application Domain/Developer Design Considerations".
- Part 8: "Recommendations for Implementation of Security and Privacy ICC Devices".

A.5.5 Smart Card alliance

The Smart Card Alliance is a US/European association of various organizations including representatives from government, the finance, computing and telecommunications, healthcare, retail and entertainment sectors. The alliance aim is to encourage the use of smart cards through education programs, market research, advocacy and open forums (see http://www.smartcardalliance.org).

Eurosmart is a joint project between Europe and Japan with the aim of reinforcing co-operation between Europe and Japan. In particular it has developed a series of specifications for electronic purse applications, a glossary of smart card security terms and a set of Common Criteria protection profiles for smart cards (see http://www.eurosmart.com).

A.5.6 e-Europe Smart Card (eESC) Initiative

The eEurope Smart Card (eESC) is an activity that was launched by the European Commission in 1999 in response to the eEurope initiative. The aim of eESC is to accelerate and develop the development of smart cards across Europe as the preferred method of access control to information society services. The activity is industry-driven but membership is open to developers and potential users of smart card based applications. Some 350 organizations have participated to the work.

The eESC have produced a detailed (50 documents in 11 volumes) a set of documentation called OSCIE (Open smartcard Infrastructure for Europe) with the basic aim of achieving an interoperable European smart card infrastructure based upon existing standards, workshop agreements including:

- ETSI/CEN Joint Workshops EESSII.
- ISSS Workshops eURI, FASTEST.

- FINREAD and Embedded FINREAD.
- Common Criteria for smart card security.
- NICSS Documents.
- US NIST GSC documents.

Part of the OSCIE, addressing Identification, Authentication and Digital signature, will be addressed in an additional CEN/ISSS workshop.

Moreover eESC has initiated some pilot projects to implement cross border interoperability of National Electronic ID cards for eGovernment and Health Insurance.

eESC has joined forces with NICSS and NIST to set up a Global Forum on interoperability of smart card based Identification, Authentication and Digital signature functionality. The outputs of this group will be fed into ISO SC 17.

Eurosmart is the umbrella organization for the smart card industry. It represents more than 90 % of the producers of cards and chips for smartcards, both memory chips and microprocessor chip. It is the official representative of industry in different IST projects like RESET, a FP5 roadmap project on R&D needs in the smart card domain for the next ten years and Smart Meji, a joint project between Europe and Japan with the aim of reinforcing co-operation between Europe and Japan in the domain of contactless cards. It also has developed a series of Common Criteria protection profiles for smart cards (see http://www.eurosmart.com). eESC TB 3 is the working arm in the smart card security domain.

The following specifications have been extracted from the eESC web site at http://www.eeurope-smartcards.org.

Volume 1, Application White papers:

- Part 1:
  - E-government White paper on smart card applications and Evolution.
  - Analysis of Developments.
  - Survey.
  - Survey on secure smart card based eGovernment applications.
- Part 2:
  - ePayments: Migration of EMV/CEPs. Status and roll out plans.
  - EMV Migration Synchronization in Europe.
  - ePurse situation in Europe.
  - EMV Country Summary.
  - EMV Migration (pointer to web-based information).
  - ePayments - Blueprint on Mobile Payments.
  - ePayments: Mobile payment business requirements.
  - Public transport: smart card transport applications and evolution.
  - Healthcare: Smart Card evolution in the health area.

Volume 2, Best Practice Manual including requirements for cost transparency and privacy code of conduct for multi-application IAS.

Volume 3, Global IAS interoperability framework:

- Part 1: Contextual and conceptual modelling.
- Part 2: Requirements for IAS functionality.

- Part 3: Recommendations for IOP specifications.
- Part 4: Deployment strategies for generic IAS.

Volume 4, Public electronic identity, electronic signature and PKI:

- Part 1: Electronic identity White Paper.
- Part 2: Study on legal issues in relation to the use of public ID (electronic identity).
- Part 3: Bionorm, Need for specifications and standardization to achieve Interoperability in the field of smart cards and biometrics.
- Part 4: Requirements Specification. Visual ID on smart card used as a travel document.
- Part 5: White Paper on PKI requirements.
- Part 6: PKI pre-inventory report.
- Part 7: Network Authentication module for Internet users - Electronic signature (Name-ES).
- Part 8: Requirements of terminal manufactures and convergence model for multiplatform access to services.
- Part 9: Telecom operators' requirements.

Volume 5, Multi-applications:

- Part 1: Legal Framework for multi-application cards and systems.
- Part 2: Current and Future Business models for multi-application systems.
- Part 3: Basic Multi-application technologies for cards and systems.
- Part 4: MAS prerequisites; Core Cross-sectorial Architecture for Interoperable Multi-application systems.
- Part 5: Integration of Multi-application systems.

Volume 6, Contactless Technology:

- Part 1: White paper requirements on the interoperability of Contactless cards.
- Part 2: White paper on Security and Threat Evaluation relating to Contactless cards.
- Part3: White paper on the Future roadmap for Contactless cards.
- Part 4: White paper on the Certification of Contactless cards.
- Part 5: Field Trials Specifications and guidelines for Contactless Card Systems.

Volume 7, generalized card Reader:

- Part 1: Generalized Card Reader (relation to FINREAD and embedded FINREAD CWAs).

Volume 8, Security and Protection Profiles:

- Part 1: The Application of Attack Potential to Smart Cards (Common Criteria Supporting Document.
- Part 2: The Application of CC to Integrated Circuits (Common Criteria Supporting Document).
- Part 3: ETR-lite for Composition (Common Criteria Supporting Document).
- Part 4: ETR-lite for Composition: Annex A Composite smart card evaluation - Recommended best practice (Common Criteria Supporting Document).
- Part 5: ST-lite (Common Criteria Supporting Document).
- Part 6: Guidance for smart card evaluation (Common Criteria Supporting Document).

Volume 9, Referenced Standards:

- Europe:
  - Executive Summaries and online pointer to EESSII standards and specifications.
  - Area K "Application Interface for smart cards used as secure signature devices, WD1 V012 Draft.
  - Summary and references to CEN/ISSS Workshop fastest.
  - Summary and references to FINREAD CWAs and CEN/ISSS Workshop.
  - Embedded FINREAD Business plan.
- Japan:
  - Japan's NICSS specifications.
  - Prerequisites.
  - Framework Scheme Overview.
  - Registration Operation Interface.
  - Operation System Interface.
  - Card Adapter Interface.
  - Card Interface Specification.
  - RW Common Card Interface.
  - Operation Guideline.
  - Contract and Covenants Example.
- USA:
  - USA GSA Specification NISTIR 6687/GSC-IS (V2.0).

Volume 10, eESC glossary of Smart Card terms.

A.5.6 US National Institute of Standards and Technology

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

A.5.7 RSA Public key Cryptography Standards

- PKCS #11: "Abstract Token Interface (Cryptoki) defines the interface between tokens when used as a cryptographic subsystem".
- PKCS #15: "Cryptographic Token Information Format Standard Background".

A.5.8 Internet Engineering Task Force

- IETF RFC 2808: "The SecurID(r) SASL Mechanism. SecurID is a hardware token card product for end-user authentication".

Annex B:
Standards for Confidentiality and privacy services

B.1 Encryption

B.1.1 Organization for Economic Co-operation and Development (OECD)

- OECD Guidelines for Cryptography Policy. Principles to be adhered to in the development of national policy on cryptography.

B.1.2 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO/IEC 9979: "Procedures for the Registration of Cryptographic Algorithms".
- ISO/IEC 8372: "Information processing - Modes of operation for a 64-bit block cipher algorithm".
- ISO/IEC 10736: "Transport Layer Security Protocol (TLSP)".
- ISO 100116 (2^{nd} edition): "Modes of operation for an n-bit block cipher algorithm (revision of 2^{nd} edition)".
- ISO/IEC 15946: "Information Technology - Cryptographic Techniques based upon elliptic curves". A four part standard comprising:
  - Part 1: "General Concepts".
  - Part 2: "Digital Signatures".
  - Part 3: "Key Recovery".
- FDIS 15946-4: "Digital Signatures giving message recovery".
- CD 15946-4: "Information Technology - Security Techniques - Cryptographic techniques based on elliptic curves - Part 4: Digital signatures with message recovery".
- CD 18031: "Information Technology - Security Techniques - Random bit generation".
- CD 18033: "Information Technology - Security Techniques - Encryption Algorithms" in four parts:
  - Part 1: "General".
  - Part 2: "Asymmetric Ciphers".
  - Part 3: "Symmetric Ciphers".
  - Part 4: "Stream Ciphers. (APEC 4.5.5)".
- ISO/IEC 11568: "Banking - Key Management (Retail)".
- ISO/IEC 8731: "Banking - Approved Algorithms for Message Authentication".
- ISO/IEC 10126: "Banking - Procedures for Message Encipherment (Wholesale)".
- ISO/IEC 13491: "Secure Cryptographic Devices".

B.1.3 European Telecommunications Standards Institute (ETSI)

The following confidentiality specifications have been issues by ETSI:

- ETSI ETS 300 840 (1998): "Telecommunications Security; Integrated Services Digital Network (ISDN); Confidentiality system for audiovisual services".
- ETSI TR 133 908 (V3.0.0): "Universal Mobile Telecommunications System (UMTS); Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms (3GPP TR 33.908 version 3.0.0 Release 1999)".
- ETSI TR 133 908 (V4.0.0): "Universal Mobile Telecommunications System (UMTS); Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms (3GPP TR 33.908 version 4.0.0 Release 4)".
- ETSI TS 135 201 (V4.0.0): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications (3GPP TS 35.201 version 4.0.0 Release 4)".
- ETSI TS 135 201 (V3.1.2): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications (3GPP TS 35.201 version 3.1.2 Release 1999)".
- ETSI TS 135 201 (V3.2.0): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications (3GPP TS 35.201 version 3.2.0 Release 1999)".
- ETSI TS 135 201 (V4.1.0): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications (3GPP TS 35.201 version 4.1.0 Release 4)".
- ETSI TS 135 201 (V5.0.0): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications (3GPP TS 35.201 version 5.0.0 Release 5)".
- ETSI TS 135 202 (V5.0.0): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification (3GPP TS 35.202 version 5.0.0 Release 5)".
- ETSI TS 135 202 (V3.1.2): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification (3GPP TS 35.202 version 3.1.2 Release 1999)".
- ETSI TS 135 202 (V4.0.0): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification (3GPP TS 35.202 version 4.0.0 Release 4)".
- ETSI TS 135 203 (V4.0.0): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data (3GPP TS 35.203 version 4.0.0 Release 4)".
- ETSI TS 135 203 (V3.1.2): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data (3GPP TS 35.203 version 3.1.2 Release 1999)".
- ETSI TS 135 203 (V5.0.0): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data (3GPP TS 35.203 version 5.0.0 Release 5)".
- ETSI TS 135 204 (V5.0.0): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data (3GPP TS 35.204 version 5.0.0 Release 5)".

- ETSI TS 135 204 (V3.1.2): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data (3GPP TS 35.204 version 3.1.2 Release 1999)".
- ETSI TS 135 204 (V4.0.0): "Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data (3GPP TS 35.204 version 4.0.0 Release 4)".
- ETSI EG 200 234 (V1.2.2): "Telecommunications security; A guide to specifying requirements for cryptographic algorithms".
- ETSI TS 133 105 (V3.2.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Cryptographic Algorithm Requirements (3GPP TS 33.105 version 3.2.0 Release 1999)".
- ETSI TS 133 105 (V3.3.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Cryptographic Algorithm Requirements (3GPP TS 33.105 version 3.3.0 Release 1999)".
- ETSI TS 133 105 (V3.4.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Cryptographic Algorithm Requirements (3GPP TS 33.105 version 3.4.0 Release 1999)".
- ETSI TS 133 105 (V3.5.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Cryptographic Algorithm Requirements (3GPP TS 33.105 version 3.5.0 Release 1999)".
- ETSI TS 133 105 (V3.6.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Cryptographic Algorithm Requirements (3GPP TS 33.105 version 3.6.0 Release 1999)".
- ETSI TS 133 105 (V3.7.0): Universal Mobile Telecommunications System (UMTS); 3G Security; Cryptographic Algorithm Requirements (3GPP TS 33.105 version 3.7.0 Release 1999)".
- ETSI TS 133 105 (V4.0.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Cryptographic Algorithm Requirements (3GPP TS 33.105 version 4.0.0 Release 4)".
- ETSI TS 133 105 (V3.8.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Cryptographic Algorithm Requirements (3GPP TS 33.105 version 3.8.0 Release 1999)".
- ETSI TS 133 105 (V4.1.0): "Universal Mobile Telecommunications System (UMTS); 3G Security; Cryptographic Algorithm Requirements (3GPP TS 33.105 version 4.1.0 Release 4)".
- ETSI ETR 234 (1995): "Security Techniques Advisory Group (STAG); A guide to specifying requirements for cryptographic algorithms".
- ETSI TCRTR 030 (1995): "Security Techniques Advisory Group (STAG); A guide to specifying requirements for cryptographic algorithms".

ETSI has also issued several documents on the subject of Law Enforcement. The following are extracted from http://portal.etsi.org/li/summary.asp:

- ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies".
- ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".
- ETSI ES 201 671: "Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic" (revised version).
- ETSI TR 101 943: "Telecommunications security; Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture".
- ETSI TR 101 944: "Telecommunications security; Lawful Interception (LI); Issues on IP interception".
- ETSI EG 201 781: "Intelligent Networks (IN); Lawful interception".
- ETSI EN 301 040: "Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface".

- ETSI TR 101 750: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; Studies into the Impact of lawful interception".
- ETSI TR 101 514: "Digital cellular telecommunications system (Phase 2+); Lawful interception requirements for GSM (GSM 01.33 version 7.0.0 Release 1998)".
- ETSI TS 101 507: "Digital cellular telecommunications system (Phase 2+); Lawful interception; Stage 1 (GSM 02.33 version 7.3.0 Release 1998)".
- ETSI TS 101 509: "Digital cellular telecommunications system (Phase 2+); Lawful interception; Stage 2 (3GPP TS 03.33 version 8.1.0 Release 1999)".
- ETSI TS 133 106: "Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful Interception Requirements (3GPP TS 33.106 version 3.1.0 Release 1999)".
- ETSI TS 133 107: "Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful Interception Architecture and Functions (3GPP TS 33.107 version 3.3.0 Release 1999)".

B.1.4 Internet Engineering Task Force (IETF)

The Internet Engineering Task Force has issued a large series of RFC standards and protocols relating to various aspects of encryption particularly in an Internet context.

Of particular note is RFC 2246 [10] which defines the IETF Transport Layer Security Protocol (TLS) for Transmission Layer Protocol (TCP).

See clause 6 of the APEC publication for a description of the other standards and protocols.

B.1.5 American National Standards Institute

- ANSI X9.17: "*Financial Industry Key Management (Wholesale)*". Key management for the use of the DES encryption system (equivalent to ISO/IEC 8732). [Withdrawn].
- ANSI X9.19: "*Financial Industry Message Authentication Code (Retail)*". Generation of a message authentication code using the DES encryption algorithm.
- ANSI X9.23: "*Data Encryption Standard (Wholesale).* Encipherment of financial transactions using the DES algorithm. [Withdrawn].
- ANSI X9.24: "*Financial Industry Key Management (Retail)*". Key management required for the use of the DES encryption system in the retail finance sector.
- ANSI X9.42: "*Diffie-Hellman Key Agreement*". Use of the Diffie-Hellman cryptographic technique to achieve key agreement.
- ANSI X9.43: "*Key Archiving and Retrieval*". Mechanisms to be used for their archiving and subsequent retrieval. [Unavailable].
- ANSI X9.44: "*Key Transport using RSA*". Exchange of confidentiality keys for subsequent symmetric encryption of messages. [Unavailable].
- ANSI X9.50: "*Certificate Management for Encryption Key Management*" [Unavailable].
- ANSI X9.52: "*Triple Data Encryption Algorithm*". Encipherment of financial transactions using the Triple-DES algorithm.

B.1.6 US National Institute of Standards and Technology

- FIPS Pub 46-2: "Data Encryption using the Data Encryption Algorithm (DEA)".
- FIPS Pub 74: "Guidelines for Implementing the Data Encryption Standard".

- FIPS Pub 81: "DES Modes of Operation".
- FIPS Pub 139: "Interoperability and Security Requirements for the Use of Data Encryption Standard (DES) in the Physical Layer of Data Communications".
- FIPS Pub 140-1: "Security Requirements for Cryptographic Modules. Note that FIPS Pub 140-2 supersedes FIPS Pub 140-1, but FIPS Pub 140-1 remains valid for former evaluations".
- FIPS Pub 140-2: "Security Requirements for Cryptographic Modules".
- FIPS Pub 141: "Interoperability and Security Requirements for the Use of Data Encryption Standard with CCITT Group 3 Facsimile Equipment".
- FIPS Pub 197: "Advanced Encryption Standard (AES)".
- NBS Spec Pub 500-61: "Maintenance Testing for the Data Encryption Standard".
- NIST Spec Pub 800-20: "Modes of Operation Validation System for the Triple Data Encryption Algorithm".
- NIST Spec Pub 800-2: "Public-Key Cryptography survey (1988-1990)".
- NIST Spec Pub 800-17: "Modes of Operation Validation System (MOVS): Requirements and Procedures. 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 and the Escrowed Encryption Standard".

B.1.7 RSA Public Key Cryptography Standards

- PKCS #1: *RSA Encryption and Signature*. Encryption of data using the RSA public-key cryptosystem and in the construction of digital signatures and digital envelopes as described in PKCS #7.
- PKCS #3: *Diffie-Hellman method for implementing key agreement in protocols for establishing secure connections, such as those proposed for OSI's transport and the network layers*.
- PKCS #5: *Password-based Encryption method for the encryption of private keys using a secret key derived from a password*.

B.2 Public Key Infrastructure

See annex C (Trust Services) for standards related to Public Key Infrastructures.

Annex C:
Standards for Trust Services

C.1 Electronic signatures

C.1.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO 9796: "Information technology - Security techniques - Digital signature schemes giving message recovery". A three part standard comprising:
  - Part 1: "Void".
  - Part 2: "Integer Factorization based mechanisms".
  - Part 3: "Discrete Logarithm based mechanisms".
- ISO/IEC 15945/ITU-T Recommendation X.843: "Information technology - Security techniques - Specification of TTP services to support the application of digital signatures".
- ISO/IEC 14888: "Information technology - Security techniques - Digital signatures with appendix". Standards for the creation and verification of a digital signature using asymmetric cryptographic techniques in three parts:
  - Part 1: "General".
  - Part 2: "Identity-based mechanisms".
  - Part 3: "Certificate-based mechanisms".
- ISO/IEC 15946-2: "Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures".
- CD 15946-4: "Information Technology - Security Techniques - Cryptographic techniques based on elliptic curves - Part 4: Digital signatures with message recovery".
- ISO/TC215 N266: "Health informatics - Security requirements for archiving and backup electronic health records".

C.1.2 European Standards Committee- Information Society Standardization System (CEN/ISSS)

The following is a list of CEN Workshop Agreements (CWAs) relating to Electronic Signatures.

- CWA 14168:2002: "E - Secure Signature Creation Devices "EAL4"".
- CWA 14169:2002: "E - Secure Signature Creation Devices "EAL4+"".
- CWA 14170:2001: "E - Security Requirements for Signature Creation Applications".
- CWA 14171:2001: "E - Procedures for Electronic Signature Verification".
- CWA 14355:2002: "E - Guidelines for the implementation of Secure Signature-Creation Devices".
- CWA TBA (work in progress): "Application Interface for SmartCards used as Secure Signature Creation Devices".

- CWA 14172-n:2001: "E - Conformity Assessment Guidance".
- CWA 14172-1:2001: "E - General".
- CWA 14172-2:2001: "E - Certification Authority services and processes".
- CWA 14172-3:2001: "E - Trustworthy systems managing certificates for electronic signatures".
- CWA 14172-4:2001: "E - Signature Creation Applications and Procedures for Electronic Signature Verification".
- CWA 14172-5:2001: "E - Secure signature creation devices".

Additionally, the following further parts are under consideration, but no formal commitment has yet been made to their development:

- CWA 14172-5: "Secure signature creation devices (for Qualified Certificates)".
- CWA 14172-6: "Certification Authority services and processes (for non-Qualified certificates)".
- CWA 14172-7: "Secure signature creation devices (for non-Qualified Certificates)".
- CWA 14172-8: "Time-Stamping Authorities".
- CWA 14172-9: "Cryptographic Modules for CSP Signing Operations".
- CWA 14365: "Guide on the Use of Electronic Signatures".

C.1.3 European Telecommunications Standards Institute (ETSI)

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 following is a list of relevant publications, details can be found in clause 9.4 of the APEC report [4]:

- ETSI TS 101 733 (V1.3.1): "Electronic signature formats" based upon Internet specification RFC 2630.
- ETSI TS 101 903 (V1.1.1): "XML Advanced Electronic Signatures (XAdES)" developed in close liaison with the W3C, to allow easy insertion into the W3C framework for XML digital signatures.
- ETSI TS 101 456 (V1.2.1): "Policy requirements for certification authorities issuing qualified certificates".
- ETSI TR 102 045 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model".
- ETSI TR 102 041: "Signature Policies Report".
- ETSI TR 102 045: "Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model".
- ETSI SR 002 176 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures".

C.1.4 International Telegraph and Telephone Consultative Committee (CCITT) of the International Telecommunications Union (ITU)

- ITU-T Recommendation X.509: Directory Authentication Framework standard adopted by ISO/IEC as ISO/IEC 9594-8.

C.1.5 Internet Engineering Task Force (IETF)

The IETF have issued a vast number of RFCs relating to digital signatures. See clause 6 of the APEC report [4] for details. The following ones are of particular note since they relate to policy issues.

- IETF RFC 3125: "Electronic Signature Policies", and rules for the creation and validation of electronic signatures based on the signature policy defined in TS 101 733 (V.1.2.2).
- IETF RFC 3126: "Electronic Signature Formats for long term electronic signatures". As an extension of RFC 2630 and RFC 2634. Equivalent to TS 101 733 (V.1.2.2).

C.1.6 RSA - Public Key Cryptography Standards

See annex B (Confidentiality and Privacy Services) for relevant Public Key Cryptography standards.

C.1.7 American National Standards Institute

- ANSI X9.30: "*Digital Signature Standard*". Details of the Digital Signature Standard promulgated as FIPS 186.
- ANSI X9.31: "*RSA*". Details of the Rivest-Shamir-Adleman (RSA) public key system for generating digital signatures using various hash algorithms MD2, MD4, MD5, SHA, MDC-2.
- ANSI X9.62: "*Elliptic Curve Digital Signature Algorithm*".

C.1.8 US National Institute of Standards and Technology

- FIPS Pub 186: "Digital Signature Standard (DSS)".

C.2 Public Key Infrastructure

C.2.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO/IEC TR 14516 (2002)/ITU-T Recommendation 842 (2000): "Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services".

C.2.2 European Telecommunications Standards Institute (ETSI)

- ETSI EG 201 057 (V1.1.2): "Telecommunications security; Trusted Third Parties (TTP); Requirements for TTP services".
- ETSI TR 102 030 (V1.1.1): "Provision of harmonized Trust Service Provider status information".

C.2.3 US National Institute of Standards and Technology

- NIST Spec Pub 800-32: "Introduction to Public Key Technology and the Federal PKI Infrastructure".

C.2.4 Internet Engineering Task Force (IETF)

- IETF RFC 2510: "Internet X.509 Public Key Infrastructure Certificate Management Protocols".

- IETF RFC 2528: "Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates".
- IETF RFC 2559: "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2" for embedding S-HTTP negotiation parameters in HTML documents.
- IETF RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP". Describes a syntax for securing messages sent using the Hypertext Transfer Protocol (HTTP) which forms the basis for the World Wide Web.
- IETF RFC 2585: "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP".
- IETF RFC 2587: "Internet X.509 Public Key Infrastructure LDAPv2 Schema" to support PKIX in an LDAPv2 environment, as defined in RFC 2559.
- IETF RFC 2692: "SPKI Requirements". 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.
- IETF RFC 3029: "Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols".
- IETF RFC 3039: "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".

C.3 Hash functions

C.3.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO/IEC 10118: "*Hash Functions*". A four part standard comprising:
  - Part 1: "General Concepts".
  - Part 2: "Hash functions using an n-bit block cipher".
  - Part 3: "Dedicated hash functions (under revision)".
  - Part 4: "Hash functions using modular arithmetic".

C.3.2 Internet Engineering Task Force (IETF)

- IETF RFC 3174: "US Secure Hash Algorithm 1 (SHA1)" based upon FIPS 180-1.
- IETF RFC 1319: "The MD2 Message-Digest Algorithm".
- IETF RFC 1320: "The MD4 Message-Digest Algorithm".
- IETF RFC 1321: "The MD5 Message-Digest Algorithm".

C.3.3 American National Standards Institute

- ANSI X9.30: "*Digital Signature Standard*". Specifies the Digital Signature Standard promulgated as FIPS 186 including the Digital Signature Algorithm (DSA), the Secure Hash Algorithm (SHA), and the management of certificates to support DSS.

C.3.4 US National Institute of Standards and Technology

- FIPS Pub 180: "Secure Hash Standard.
- NIST Spec Pub 800-2: "Public-Key Cryptography". A state-of-the-art survey of public-key cryptography circa 1988-1990 including a summary of digital signatures and hash functions.

C.4 Time-stamping

C.4.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO/IEC 18014: "Information Technology- Security techniques - Time stamping services".
- FDIS 18014- 2: "Information Security - Security Techniques - Time stamping services Part 2 Mechanisms producing independent tokens".
- CD 18014-3: "Information Security - Security Techniques - Time stamping services Part 3 Mechanisms producing linked tokens".

C.4.2 European Standards Committee- Information Society Standardization System (CEN/ISSS)

- CWA 14172-8: (work in progress). "*Time-Stamping Authorities*".

C.4.3 European Telecommunications Standards Institute (ETSI)

- ETSI TS 102 023 (V1.1.1): "Policy requirements for time-stamping authorities in support of Qualified Certificates".
- ETSI TS 101 861 (V1.2.1): " Time stamping profile". Defines how the Internet specification for time-stamping may be used to support advanced electronic signatures to provide long term validity as defined in TS 101 733.

C.5 Non-repudiation

C.5.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO/IEC 13888: "Non-Repudiation". A three part standard comprising:
  - Part 1: "General Concepts".
  - Part 2: "Mechanisms using symmetrical techniques".
  - Part 3: "Mechanisms using asymmetric techniques".

C.6 Key management

C.6.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO/IEC 11770: "Key Management": A four part standard comprising:
  - Part 1: "Framework".
  - Part 2: "Mechanisms using symmetric techniques".
  - Part 3: "Mechanisms using asymmetric techniques".
  - Part 4: "Mechanisms using weak secrets".

Annex D:
Standards for Business Services

There are no internationally recognized standards in this area though national and industry specific guidelines exist.

Annex E:
Standards for Network Defence Services

E.1 Anti-virus

E.1.1 US National Institute of Standards and Technology

- NIST Spec Pub 500-166: "Computer Viruses And Related Threats: A Management Guide".
- NIST Spec Pub 800-5: "A Guide To The Selection Of Anti-Virus Tools And Techniques".

E.2 Firewalls

E.2.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- PDTR 15446: "Information Security - Security Techniques - Guide for production of protection profiles and security targets including annexes for firewalls".

E.2.2 Internet Engineering Task Force

- IETF RFC 2588: "IP Multicast and Firewalls". Describes how a Firewall may be configured to address the issues around the traversal of multicast traffic across a Firewall.
- IETF RFC 2647: "Benchmarking Terminology for Firewall Performance".
- IETF RFC 2979: "Behaviour of and Interoperability Requirements for Internet Firewalls".
- IETF RFC 3093: "Firewall Enhancement Protocol (FEP) - Proposed methodology to layer any application layer Transmission Control Protocol/User Datagram Protocol (TCP/UDP) packets over the HyperText Transfer Protocol (HTTP) protocol".

E.2.3 US National Institute of Standards and Technology

- NIST Spec Pub 800-10: "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls".
- NIST Spec Pub 800-41: "Guidelines on Firewalls and Firewall Policy".
- NIST Spec Pub 800-46: "Security for Telecommuting and Broadband Communications including requirements for home office systems".

E.3 Intrusion detection

E.3.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO/IEC TR 15947: "Information Technology-Security techniques - Framework for intrusion detection".
- WD 18043: "Guidelines for the selection, deployment and operations of intrusion detection systems (IDS)".

E.3.2 US National Institute of Standards and Technology

- NIST Spec Pub 800-31: "Intrusion Detection Systems (IDS) - A primer".

E.4 General Network Security

E.4.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- WD 18028: "IT Network Security". A four part standard comprising:
  - Part 1: "Network Security".
  - Part 2: "Network Security Architecture".
  - Part 3: "Securing communications between networks using security gateways".
  - Part 4: "Remote Access".
- WD 18044: "Information Security Incident Management".

Annex F:
Standards for Assurance services

F.1 Information security management and risk assessment

There are numerous international and industry sector standards and national guidance documents on information security management and risk assessment:

- OECD: "Guidelines for the Security of Information Systems".
- ISO/IEC TR 13335: "Information Technology - Guidelines for the management of IT security (GMITS)". A five-part standard comprising:
  - Part 1 "Concepts and models for IT security" (under revision).
  - Part 2: "Managing and Planning IT security" (under revision and being merged with Part 1).
  - Part 3: "Techniques for the management of IT security", this provides guidance and methods for risk assessment.
  - Part 4: "Selection of safeguards", this provides risk management guidance on the selection of safeguards.
  - Part 5: "Management guidance on network security".
- CD 13335-1: "Management of Information and communication technology security; Part 1: Concepts and models for information and communications technology security management".
- ISO/IEC TR 13335-2: "Management of Information and communication technology security; Part 2: Techniques for information and communications technology security risk management".
- ISO/IEC 17799 (2000): "Information technology - Code of practice for information security management".
- WD 17799: "Code of practice for information Security Management (revision)".
- NP 19791: "Security Assessment of operational systems".
- IS 21827: "Systems Security Engineering - capability Maturity Model (SSE-CMM)".
- ISO Guide 73 (2002): "Risk management - Vocabulary - Guidelines for use in standards".
- BS 7799-2 (2002): "Information security management systems - Specification with guidance for use - Annex B provides implementation guidance for the risk assessment, risk treatment and risk management processes defined in the main body of Part 2".
- Bundesamt fur Sicherheit in der Informationstechnik (BDI): IT Baseline Protection Profile.
- Financial Services Authority (FSA) CP 142: Operational risk systems and controls.
- AS/NZS 4360: Risk Management. A generic guide for establishing and implementing a risk management process.
- SAA/SNZ HB 231: "Information Security Risk Management Guidelines. Guidance for the establishment and implementation of a risk management process for information security risks".
- SAA/SNZ HB 240: "Guidelines for managing risk in outsourcing utilizing the AS/NZS 4360 process. Guidance for managing risks, which arise when organizations outsource elements of their business".
- GAO/AIMD-00-33: "Information Security Risk Assessment - Practices of Leading Organization".

- Information Assurance Guidelines for the Commercial Sector: 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.
- MG-2: A Guide to Security Risk Management for Information Technology System. 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.
- MG-3: A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems. Produced by Government of Canada, Communications Security Establishment (CSE), this provides additional guidance for system designers on the technical factors associated with performing risk assessments and selecting appropriate safeguards.
- NIST Spec Pub 800-30: Risk Management Guide for Information Technology Systems.
- 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.
- 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).
- 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.

F.2 Accreditation and certification

F.2.1 European Committee for Standardization (CEN) and International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO/IEC 17025: "General Requirements for the Competence of Calibration and Testing Laboratories".
- EN 45011: "General Requirements for Bodies Operating Product Certification Systems (ISO/IEC Guide 65)".
- EN 45012: "General Requirements for Bodies Operating Assessment and Certification/ Registration of Quality Systems (ISO/IEC Guide 62)".
- EN 45003: "Calibration and testing laboratory accreditation systems -- General requirements for operation and recognition (ISO/IEC Guide 58)".
- EN 45010: "General Requirements for Assessment and Accreditation of Certification/Registration Bodies (ISO/IEC Guide 61)".
- ISO/IEC Guide 7 (1994): "Guidelines for drafting of standards suitable for use for conformity assessment".
- ISO/IEC Guide 22 (1996): "General criteria for supplier's declaration of conformity".
- ISO/IEC Guide 23 (1982): "Methods of indicating conformity with standards for third-party certification systems".
- ISO/IEC Guide 27 (1983): "Guidelines for corrective action to be taken by a certification body in the event of misuse of its mark of conformity".
- ISO/IEC Guide 28 (1982): "General rules for a model third-party certification system for products".

- ISO/IEC Guide 67 (1999): "Fundamentals of product certification - Desciption of various types commonly in use".
- ISO/IEC Guide 68 (2002): "Arrangements for the recognition and acceptance of conformity assessment results".
- ISO/IEC DIS 17000: "Conformity assessment - General Vocabulary".
- ISO/IEC WD PAS 17001: "Conformity Assessment - impartiality and related bodies - Principles and requirements".
- ISO/IEC WD PAS 17002: "Conformity Assessment -Confidentiality - Principles and requirements".
- ISO/IEC WD PAS 17003: "Conformity Assessment - Complaints and appeals - Principles and requirements".
- ISO/IEC TR 17010 (1998): "General Requirements for bodies providing accreditation of inspection bodies".
- ISO/IEC DIS 17011: "General Requirements for bodies providing assessment and accreditation of conformity assessment bodies".
- ISO/IEC 17020 (1998): "General criteria for the operation of various types of bodies performing inspection".
- ISO/IEC CD 17021: "Conformity assessment - General criteria for bodies providing assessment and certification for management systems".
- ISO/IEC 17024 (2003): "Conformity assessment - General requirements for bodies operating certification of persons".
- ISO/IEC 17025 (1999): "General requirements for the competence of testing and calibration laboratories".
- ISO/IEC WD 17025: "General requirements for the competence of testing and calibration laboratories".
- ISO/IEC FDIS 17030: "Conformity assessment - General requirements for third-party marks of conformity".
- ISO/IEC CD 17040: "General requirements for peer assessment of conformity assessment bodies".
- ISO/IEC DIS 17050-1: "Conformity assessment - Suppliers declaration of conformity - Part 1: General Requirements".
- ISO/IEC DIS 17050-2: "Conformity assessment - Suppliers declaration of conformity - Part 2: Supporting documentation".
- ISO/IEC Guide 43-1 (1997): "Proficiency testing by inter-laboratory comparisons - Part 1: Development and operation of proficiency testing schemes".
- ISO/IEC Guide 43-2 (1997): "Proficiency testing by inter-laboratory comparisons - Part 2: Selection and use of proficiency testing schemes by laboratory accreditation bodies".
- ISO/IEC Guide 53 (1988): "An approach to the utilization of a supplier's quality system in third party product certification".
- ISO/IEC Guide 60 (1994): "ISO/IEC Code of good practice for conformity assessment".
- ISO/IEC CD Guide 60: "ISO/IEC Code of good practice for conformity assessment".
- ISO 19011 (2002): "Guidelines for quality and/or environment management system auditing".
- EA 7/03: "EA Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems".
- CWA 14172: "EESSI Conformity Assessment Guidance (5 parts)".
- ISO/IEC 15408: "Information Technology - Security techniques -Evaluation criteria for IT security. Used for evaluation and certification of security properties of IT products and systems".

- BS 7799-2: "Information security management systems - Specification with guidance for use. Used for certification of Information Security Management Systems".

F.3 Evaluation

F.3.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC) and European Committee for Standardization (CEN)

- ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security". A three-part standard, the Common Criteria (CC), is provided for use as the basis for evaluation of security properties of IT products and systems. It comprises:
  - Part 1: "Introduction and general model: Introduces the Common Criteria".
  - Part 2: "Security functional requirements: Establishes a set of security functional components as a standard way of expressing the security functional requirements for Targets of Evaluation (TOEs)".
  - Part 3: "Security assurance requirements: Catalogues the set of assurance components, families, and classes".
- CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".
- CWA 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP)".
- CWA 14167-3: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)".
- CWA 14168: "Secure Electronic Signature Devices, version EAL4".
- CWA 14169: "Secure Electronic Signature Devices, version EAL4+".
- CWA 14170: "Security Requirements for Signature Creation Applications".
- CWA 14171: "Procedures for Electronic Signature Verification".
- CWA 14365-1: "Protection Profile - Software Signature-Creation Device SCDev-PP".
- ISO/IEC WD 19790 Security requirements for cryptographic modules - Based on FIPS 140-2.
- ISO/IEC NWI 17972 A framework for security evaluation of biometric technology.
- ISO/IEC PDTR 15446: "Information Security - Security Techniques - Guide for production of protection profiles and security targets".
- ISO/IEC 15292: "Protection Profile Registration Procedures".PDTR 15443: "Information Security - Security Techniques - A framework for IT assurance". A three part standard comprising:
  - Part 1: "Overview and Framework".
  - Part 2: "Assurance Methods".
  - Part 3: "Analysis of assurance methods".
- ISO/IEC 21827 (2002): "Systems Security Engineering - capability Maturity Model".

- ISO/IEC WD 18045: "Information Security - Security Techniques - Methodology for IT security evaluation (CEM)". Specifies ISO/IEC 15408 Evaluation Criteria for IT Security. It supports the consistent and therefore predictable evaluation work performed by IT Security Evaluation Facilities (ITSEFs) around the world, performing IS 15408 evaluations.

F.3.2 US National Institute of Standards and Technology

- FIP Spec pub 102: "Guideline for Computer Security Certification and Accreditation".
- FIPS Pub 140-2: "Security Requirements for Cryptographic Modules". 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. Supersedes FIPS Pub 140-1.

F.3.3 US National Computer Security Centre

- NCSC-TG-029: "Introduction to high level Certification and Accreditation Concepts".

F.3.4 US National Computer Security Centre

- NCSC-TG-002: "Trusted Product Evaluations - A Guide for Vendors".

Annex G: Standards for Microprocessor Control of Domestic Equipment

G.1 International Organization for Standardization and Electrotechnical Commission (ISO/IEC)

- ISO/IEC 15045-1: "Information technology - Home Electronic Systems (HES) gateway - Part 1: A Residential Gateway model for HES".

ISO/IEC JTC1 SC25 WG1 is starting to work on a standard for aspects of security as they impinge on the home-based user of home electronic systems and equipment. Input to the sub group that will be developing the present document will be welcomed.

G.2 Other work

A significant amount of work has been carried out on behalf of the UK Department for Trade and Industry (DTI) ("The Application Home Initiative") and a report produced:

- The Application Home Initiative. *Survey and Recommendations for al standards, protocols and related requirements of Home Systems*. (A report available from (http://www.theapplicationhome.com) or from Telemetry Associates Ltd., Church Farm Barn, Rickinghall, Diss, Norfolk, UK IP22 1EC).

History

Document history		
V1.1.1	December 2003	Publication