Network and Information Security Standards Report

in support of the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions:

A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"

Issue 6.2, 4 June 2007

FINAL VERSION

Version History

Version	Date	Changes
Version 1	October 2003	Original Version
Version 1.1	24th May 2006	Version 1.1 was created based on the resolution of comments agreed at the meeting on the 11th April 2006, contained in the Disposition of Comments. All changes have been marked for easy identification.
Version 1.2	23rd June 2006	Version 1.2 was created based on the discussions held at the Project Team meeting on the 30th May 2006 and the NISSG meeting on the 31st May 2006. All changes have been marked for easy identification.
Version 2.0	16th July 2006	Version 2.0 was created based on the discussions held at the Open meeting on the 28th June 2006, and some additional input that was sent to the editors after the meeting.
Version 2.1	10th September 2006	Version 2.1 was created for the ISSS Meeting on the 19th September, and incorporates all comments received after the Open meeting on the 28th June 2006.
Version 3	15th October 2006	Version 3.0 was created based on the comments that have been received so far and will be discussed at the Open Meeting on 25th October.
Version 3.1	28th October 2006	Version 3.1 was created based on the discussions held at the Open Meeting on 25th October 2006 and includes all comments that have been made prior to and at that meeting.
Version 4.0	26th November 2006	Version 4.0 was created based on the comments received after the Open Meeting on 25th October 2006, up to 24.11.2006. This version is sent to the Project Team for final proof-reading.
Version 4.1	26th December 2006	Version 4.1 of the NIS Report was created based on Version 4.0 and includes all comments that have been made by the Project Team after a final proof-read.
Version 4.9	7th February 2007	Version 4.9 of the NIS Report was created following the Open Meeting in Sofia Antipolis, and all comments that were discussed there have been addressed in this draft. The purpose of this draft is to give the Project Team to review the text and to provide feedback for the final version.
Version 5.0	25th February 2007	Version 5.0 was created based on some final feedback from several sources, not yet including the Project Team feedback.
Version 5.1	28th February 2007	Version 5.1 was created following the feedback from the Project Team, based on Version 5.0.
Version 6.0	31st March 2007	Version 6.0 is the Final version of the NIS Report and has been created based on the comments received on Version 5.1 and their resolution, which was agreed at the NISSG meeting on the 21st March.
Version 6.1	24th April 2007	Version 6.1 contains guidelines to SMEs in some other languages than English (Italian not yet included)
Version 6.2	4 June 2007	Version 6.2 contains also the Italian guidelines to SMEs - it is this version which is made available as web-pages from the web.

Executive Summary

Communication from the Commission COM (2006) 251

The Communication from the Commission COM (2006) 251 states: "*The availability, reliability and security of networks and information systems are increasingly central to our economies and to the fabric of society*". This report is in support of the objectives in COM(2006) 251 and provides an overview of existing standards in the area of NIS, and makes recommendations for standards-related actions to be carried out by the European Standards Organizations, industry standards groups and related bodies.

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

- **Technology - diversity, openness and interoperability:** There are many different and diverse network and information security problems related to technology, and the standardization organizations have produced a large set of standards that can be used to help protect against these security problems. One aim of this report is to highlight the standards that do exist in relation to specific security areas.
- **People – culture of security and trust**: The effectiveness of any network and information security measure is dependent on the end user complying with the requirements of the security measure and applying it accordingly. Also users and management need to be aware that a lack of adequate initial investment in security may result in more costly recovery measures later should security be compromised. Consequently a culture of security should be developed in the organization/user population. This will also demonstrate trustworthiness to business partners and customers.
- **Best Practices – information security management**: There are many best practices available that are well-tested and can be applied by any organization to make their systems more secure. These best practices can be further enhanced by gaining a good understanding of the security risks and then tailoring the best practices to the particular needs of the organization. In addition, security management can be applied to maintain the level of security achieved and to be able to make improvements, where necessary.

Another area where awareness is important is the Small and Medium Enterprises and Home users. Home users and many Small and Medium Enterprises are using the Internet for the purposes of e-commerce, information and entertainment. These users often have neither the expertise nor the awareness to apply appropriate security measures consistently in order to prevent network and information security breaches. Annex 2 provides an overview on existing guidelines for SMEs to keep products and services secure, together with hyperlinks to where this information is available.

About this Report

The aim of this report is to respond to the Communication COM(2006) 251 by providing an overview of existing standards in the area of Network and Information Security (NIS). This report considers NIS in the context of the security issues arising in global electronic business and the secure information society, with the aim to provide a secure, reliable and trustworthy infrastructure for carrying out electronic business and communications in "cyberspace", and to encourage growth of e-business and other electronic applications in Europe.

The report does not address all aspects of network security but essentially those that relate to the user and provider of e-business services, the issue of identifying and reducing cybercrime, electronic communication, and application areas, such as e-health, with a focus on stakeholders, such as security experts and bodies representing end users (in the following referred to as 'stakeholder') and their requirements.

This report provides the stakeholders with an overview of existing security standards and future standardization requirements in the area of NIS. The report identifies typical network and information security related threats, together with the standards and solutions that help to protect against these threats. These standards are also included in an online database, which is being developed in collaboration with ITU-T and ENISA and allows searching for topics and particular standards bodies. The report also addresses new developments and trends in the technological environment.

The areas for which existing standards have been identified are:

- Registration, authentication and authorization services;
- Confidentiality and privacy services;
- Trust services;
- Network and information security management systems and services; and
- Assurance services.

Target Audience

This report is intended to be used by organizations with an interest in information security standards and guidelines; these organizations may represent stakeholders, small and medium-sized enterprises (SMEs) or large organizations, may be governments or may be public interest bodies.

1 Introduction

This report is issued in support of the objectives from COM(2006) 251 Communication from The Commission to The Council, The European Parliament, The European Economic and Social Committee and the Committee of the Regions; A strategy for a Secure Information Society – "Dialogue, partnership and Empowerment"

An overview of this Communication follows:

The Communication "i2010 – A European Information Society for growth and employment"[1], highlighted the importance of network and information security for the creation of a single European information space. The availability, reliability and security of networks and information systems are increasingly central to our economies and to the fabric of society. The purpose of the present Communication is to revitalize the European Commission strategy set out in 2001 in the Communication "Network and Information Security: proposal for a European Policy approach"[2]. It reviews the current state of threats to the security of the Information Society and determines what additional steps should be taken to improve network and information security (NIS).

Drawing on the experience acquired by Member States and at European Community level, the ambition is to further develop a dynamic, global strategy in Europe, based on a culture of security and founded **on dialogue, partnership and empowerment**.

In tackling security challenges for the Information Society, the European Community has developed a three-pronged approach embracing: specific network and information security measures, the regulatory framework for electronic communications (which includes privacy and data protection issues), and the fight against cybercrime. Although these three aspects can, to a certain extent, be developed separately, the numerous interdependencies call for a coordinated strategy. This Communication sets out the strategy and provides the framework to carry forward and refine a coherent approach to NIS.

The regulatory framework for electronic communications, the review of which is underway, includes security-related provisions. In particular, the Directive on Privacy and Electronic Communications[3] contains an obligation for providers of publicly available electronic communications services to safeguard the security of their services. Provisions against spam[4] and spyware[5] are laid down.

The aim of this report is to respond to the Communication COM(2006) 251 by providing an overview of existing standards in the area of NIS, 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 Communication.

The identified existing standards are listed in a database on a Web site [Web-Site 1], which is developed in collaboration with ITU-T and ENISA. This database allows an interactive

1 COM(2005) 229 final of 1.6.2005.
2 COM(2001) 298 final of 6.6.2001.
[3] Directive 2002/58/EC
[4] Or unsolicited commercial communications.
[5] Spyware is tracking software deployed without adequate notice, consent, or control for the user.

search for standards dealing with particular security topics and for standards that have been issued by a specific standards body.

Recommendation 1 NISSG should collaborate with ITU-T and ENISA to complete the database of standards as described above. This include a suitable design of the database that supports the aims of this NIS-Report, and of a mechanism that ensures that updates are made in a suitable timeframe to ensure topicality of this database. The collaboration of NISSG, ITU-T and ENISA should be made visible on the Web site on which this database is published.

Suggested responsibility: NISSG Secretariat

Priority: High

Deadline and Timeframe: The development of this database has started already and will be completed within the next months. This database should be published as soon as possible to support the NIS-Report.

2 Threats referred to in COM(2006) 251

The Communication COM(2006) 251 highlights several threats and risks to NIS, and discusses a suggested way towards a secure information society. This section explains how this report supports the Communication, and how the various sections in this report relate to the issues raised in the Communication.

The following threats and security related issues were explicitly mentioned in the Communication, in addition to the general requirement for a secure network and information infrastructure:

- Malware, including malicious software, spam, spyware, phishing, etc.:
  The protection against malware relies on the integrated application of different security controls; see Threat T3 in Section 5.
- Mobile devices:
  The use of mobile devices might be subject to a number of threats, such as interception (see Threat T1), unauthorized access to the content of the communication (see Threat T2), malicious software (see Threat T3), illegal content decryption (see Threat T6), or disruption of services (see Threat T8). See Threats T1, T2, T3, T6 and T8 in Section 5 for further consideration.
- Future developments:
  The Communication mentions explicitly the security issues that relate to the increased use of intelligent devices, such as RFID. This report discusses the security issues related to RFID in Section 12.1, and next generation networks are considered in Section 12.2.
- Raising awareness
  COM (2006)251 refers to "best practices to improve awareness among SMEs and citizens of the need to address their own specific NIS challenges and requirements as well as their ability to do so." This report provides in Annex 2 an Overview of Information for SMEs regarding NIS.
- Importance of NIS:
  The Communication also states "*A breach in NIS can generate an impact that transcends the economic dimension. Indeed, there is a general concern that security*

problems may lead to user discouragement and lower take-up of ICT, whereas availability, reliability and security are a prerequisite for guaranteeing fundamental rights on-line." The aim of this report is to highlight the existing standards that can be used to achieve NIS, and also to make recommendations for future standards and solutions that are needed to make a further step towards a secure information society.

- Critical infrastructures:
  COM (2006)251 points out that "because of increased connectivity between networks, other critical infrastructures (like transport, energy, etc.) are also becoming more and more dependent on the integrity of their respective information systems." The NIS report addresses issues that are related to critical infrastructures in Section 11.3.

3 Scope and Content of this Report

3.1 Definitions

According to the 2001 Communication from the Commission [2], Network and Information Security (NIS) is defined as:

NIS: 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.

This report also uses the following terms:

Authenticity: the property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information [7]

Availability: the property of being accessible and usable upon demand by an authorized entity [7]

Confidentiality: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes [7]

Integrity: the property of safeguarding the accuracy and completeness of assets [7]

3.2 Scope of this report

This report considers Network and Information Security in the context of the security issues arising in global electronic business and the secure information society, as outlined in [1]. The NIS-related security issues of electronic business and communications within the scope of this report are addressed in Sections 4 to 10 below.

In addition to these issues, there are other important topics that relate to NIS, but are not within the scope of this report; these topics are discussed in Section 11, and NIS-related new developments are discussed in Section 12.

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

3.3 Context of this report

In the context of this report, e-business means 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, the issue of identifying and reducing cybercrime, electronic communication, and application areas, such as e-health. To help understand the scope of this report, reference should be made to the security architecture described in the ITU-T report COM D79 [8], Security Architecture for Systems Providing End-to-End Communications.

In essence the NIS report addresses those security issues arising in the "Stakeholder 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 European Standards Organizations and other such bodies are largely not relevant.

In view of the fact that electronic business, communications and applications may traverse national boundaries and, where the Internet is concerned the communications path is unpredictable, the stakeholder should be sure that security measures for the applications used 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 networks. The use of Virtual Private Networks (VPNs), wireless LANs and 3G networks is also considered, as it is likely that any electronic transaction or communication may utilize one or more of these types of networks. Thus it is crucial that the various protocols (including security protocols) should be interoperable over these networks wherever required to establish and maintain the end-to-end communications path as well as conduct the electronic transaction or use e-applications.

4 User Requirements

Roles and responsibilities should be carefully separated. The users of equipment, whoever they are, cannot escape responsibility for the correct installation and use of their equipment. Manufacturers are responsible for the incorporation of security features but cannot be held responsible for their correct use. However, the usability of the security features of the product need to be designed so that the stakeholder can be expected to use these features. In addition, stakeholders should 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.

4.1 Home Users

The home user today typically has a single PC and uses a single gateway (to the public Internet). Often, there is a wireless network connected to this gateway.

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

4.1.1 Home Working

There is a significant growth in the 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.

4.1.2 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.

4.1.3 Microprocessor control of Domestic equipment

There is a significant growth in the use of home devices – such as heating systems, refrigerators, alarm systems, ovens – containing embedded microcontrollers that can be accessed remotely. Therefore, there is a requirement for the home user to control such systems using personal computers in the home. Additionally it is 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. In addition, there is the CEN SmartHouse project, which has the overall objective to grow and sustain convergence and interoperability of systems, services and devices for home users that will provide an increased functionality, accessibility, reliability and security.

4.1.4 eHealth

In addition to the requirements of home users and home workers as described above, eHealth (see also Section 11.2) establishes other security relevant scenarios such as home care. In this context, privacy and safety (health and life) might be endangered by attacks to integrity of information and actions.

4.1.5 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 might not always be able to protect the integrity and confidentiality of their personal information. Online suppliers of products and services and ISPs should be encouraged to provide basic security services to assist their customers (e.g. firewalls and malware detection). Default settings of devices should be so that a minimum level of security is provided (e.g. the firewall of a wireless router must be in the "on" state by default.). Although not removing a home 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. The Research and Testing study commissioned by ANEC for the standards possibilities for Internet filtering software to protect children on-line is of relevance here. The purpose of the study was to investigate to what extent unsolicited commercial communication (Spam) and Internet content filters should be testable and comparable in order to help consumers with their choice. The ANEC report may be found at [Web-Site 35]. CEN BT has created BT/WG 194 to define the scope of one or more potential deliverables in relation to Internet filtering and anti-spam measures.

e. 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.

f. The home worker will need to be provided by his employer with ready-to-use systems with good security, such as VPNs or a secure file transport capability.

g. 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 is 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. Consideration should be given as to whether users should be provided with facilities to enable them to evaluate the level of protection provided by their applications

Note that the legal aspects on the 'interception' for the purposes of Anti-Spam and Anti-Virus handling is under scrutiny at the International level in the International Working Group for Data Protection on Telecommunications.

4.2 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.

4.2.1 The SME as a user of e-business services

An example is an organization that uses an Internet-based trading service, provided by an e-business service provider, to source raw materials or office supplies.

The typical SME will share some of the concerns of the home user (see above). However the SME will also hold personal data relating to its employees, commercial data relating to trading partners business critical data such as customer lists, contract information etc. In its

relation with the ISP or e-business service provider, it should be clear to the SME, what data the ISP or e-business service requires from it and how it will protect that data. A loss of confidentiality, integrity or availability of this data (to the SME) 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. Typically, these types of arrangements should be stated in a service level agreement between the SME and ISP or e-business service provider.

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. However, with a steadily increasing number of Internet security threats and vulnerabilities, it cannot be expected that every SME will be able to keep up to date with these developments. Therefore, depending on the size and type of activity of the SME, the SME either has sufficient internal experience and knowledge to resolve these security issues (an SME IT operator for example) itself or should otherwise have access to external specialist IT security support. Annex 2 includes several Web sites where SMEs can find further information about network and information security.

The SME trade bodies UEAPME and NORMAPME have started a new network that aims to represent the European IT-SMEs (suppliers and service providers). This network seeks to accelerate the adoption of eBusiness solutions by SMEs in Europe by providing the eBusiness tools and the means to the IT-SMEs and small eBusiness-enablers, with the aim to achieve a significantly higher use of ICT & eBusiness as the standard medium for doing business between SMEs, their large business partners and the governments. It seeks recognition from the European political leadership of the important role that IT-SMEs and small eBusiness-enablers play. Members of this network are important implementers of security systems at SMEs and some also are themselves active programmers in that area. They can also help in the education and awareness programs.

4.2.2 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. The SME may also be perceived by its customers as having some responsibility for security for the transaction path between the SME and the customer; it is therefore very important that the customers can make their own security assessments.

4.2.3 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 ISP and/or e-business provider should define for the SME user the extent of the ISP or e-business provider's responsibility for the protection of the confidentiality and integrity of commercially sensitive data belonging to the SME and how it intends to discharge that responsibility. This allows the SME to make an informed choice whether or not he should apply additional security measures.

This could be settled in a service level agreement (SLA) between the SME and the ISP or e-business service provider.

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. Although these products should be easy to use, they should also provide a means to evaluate the level of protection offered, and provide a clear indication of what is required for a secure implementation. Note that the legal aspects of Anti-Spam and Anti-Virus are being addressed - see section 11.

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.

4.3 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) and various other communication facilities. In the context of this report "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.

4.3.1 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.

Recommendation 2 All users of standards, home users, SMEs or medium to large organizations, will benefit from improved collaboration and coordination of standardization activities. Such collaboration can be achieved be aligning and agreeing upon roadmaps, vocabulary and approaches used by the various standardization bodies.

Suggested responsibility: ICTSB should consider this issue.

Priority: Medium

Deadline and Timeframe: This harmonization of standardization activities should start as soon as possible and continue over time.

5 General Threats to Network and Information Security

The assets of the e-business services and other electronic services should be protected in order to preserve the authenticity, confidentiality, integrity and availability of the service. The assets of these electronic services are:

- The data of organizations and citizens using electronic service.
- The assets of the electronic business or activity service itself (e.g. systems, networks, information).
- Data and information related to the remote control of networked home based equipment and systems.
- User authentication credentials.

A user's safety, health, reputation and money are also important assets.

The threats to the assets of the e-business services and other electronic services are described below; they have been ordered into two categories (system and application threats and infrastructure threats) to illustrate the different types of threats and assets that might be affected by these threats:

System and Application Threats

T1. Electronic communication can be intercepted and data copied or modified. This can cause damage through invasion of the privacy of individuals or through the exploitation of data intercepted; the modification of intercepted data could also threaten the health and life of patients.

T2. Unauthorized access into computer and computer networks is usually carried out with malicious intent to copy, modify or destroy data and extends to systems and automatic equipment in the home or to mobile devices such as mobile phones, PDAs, etc.

T3. Malicious software, such as viruses, can disable computers or mobile devices, delete or modify data or reprogram equipment. Some recent virus attacks have been extremely destructive and costly. Recent attacks are targeted and designed for financial gain.

T4. Misrepresentation of people or entities can cause substantial damages, e.g. customers may download malicious software from a website masquerading as a trusted source , people might be subject to identity theft, phishing might be used to receive confidential information, contracts may be repudiated, and confidential information may be sent to the wrong persons.

T5. Unforeseen and unintentional security incidents, such as hardware or software failures, human error, unexpected behaviour from users, or natural disasters (floods, storms, and earthquakes) can result in loss of or damage to assets.

T6. Illegal content decryption and/or copying and/or forwarding on the Internet threaten copyrights and content distribution services on a more and more large scale.

Infrastructure Threats

T7. External threats to the supply and provisioning of services at the national or international infrastructure level. This includes supply of services such as those relating to telecoms and networks, medical and healthcare, financial, transport, utilities (e.g. water, electricity and gas), emergency facilities (e.g. police, fire fighting) and food supply chain. The threats to the services include natural disasters, acts of terrorism, strikes and other disruptive activities, arson and other criminal incidents and epidemics (e.g. SARS, bird flu).

T8. Disruptive attacks on the Internet have become quite common and the telephone network, both fixed and mobile, also becomes more and more vulnerable, due to their transition to internet technologies (i.e. VoIP)). These attacks include VoIP spamming, denial of service (DoS) and distributed denial of service (DDoS) attacks. These attacks can also influence the national and international infrastructure mentioned in T7.

The threats T1 to T8 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 controls covered in sections 6 to 10 inclusive. For the purposes of this report, the security services are defined as follows[6].

a. **Registration, Authentication and Authorization 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. The service also includes the authentication of all entities other than a person, such as organizations, systems, devices, applications/services, or components

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. These

[6] 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.

services might also provide anonymization and pseudonymization, as well as directory services.

d. **Network and Information Security Management Services**. These services are required to ensure that appropriate management controls, processes and procedures are in place in addition to the technical security measures to protect the system and network infrastructure. The security controls in this section include policies, organizational controls, controls to achieve asset management, human resources security, physical security, controls to achieve operational and communications controls, controls against malicious code, the secure design and configuration of applications, incident management and business continuity.

e. **Assurance Services**. These services provide e-business users with confidence that all technical (hardware and software applications) and non-technical (physical, personal and procedural) security measures have been designed, configured and are being operated in a secure manner in accordance with the relevant standards, and provide protection against the assessed risk to the services. Following a process of independent audit or evaluation, the result can be an improved security management system or a more secure product; this might also be indicated by a certificate[7].

The following table shows the relationship between threats T1 to T8 and the set of security services defined above (note that assurance services are not included in the table because they aim at defining what confidence can be placed in the security measures contained in the other sections):

Threat	**Security Services**			
	Registration, Authentication and Authorization	Confidentiality and Privacy	Trust	Network and Information Security Management
T1		**X**		**X**
T2	**X**	**X**		**X**
T3				**X**
T4	**X**		**X**	
T5				**X**
T6				**X**
T7				**X**
T8				**X**

In order to protect the network and information systems that form the basis of the e-business service, the threats to the service should be countered by a number of technical, policy or

[7] Note that 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.

procedural security measures. The following sections of the report describe these security measures under the high level security services defined in the previous section and contain relevant recommendations. In addition, the existing standards that relate to these services are contained in a database that can be accessed on [Web-Site 1]; this Web-site also allows a search for particular security services. The services in this report are:

Section 6: **Registration, Authentication and Authorization Services**;

Section 7: **Confidentiality and Privacy Services**;

Section 8: **Trust Services**;

Section 9: **Network and Information Security Management Services**;

Section 10: **Assurance Services**.

Recommendation 3 All users of standards should be aware of any progress made within the standardization bodies and in research on the above mentioned services.

Suggested responsibility: NISSG Secretariat (for the current report), ICTSB (for the future report), and ENISA and ITU-T (for the database, see Recommendation 1).

Priority: Medium

Deadline and Timeframe: The present report is placed online (the reference *to the Web site needs to be added*). A new version of this report should be envisaged in 2010. The online database (see Recommendation 1) gives an overview of the standards work in existence and under development.

6 Registration, Authentication and Authorization Services

It is of paramount importance that effective and secure registration, authentication and authorization services are put in place in an e-business environment, since registration, authentication, and authorization represent one of the "front lines" in the defence of the e-business services and data. For the purpose of this report the definitions of "authentication", "registration" and "authorization" are taken from *e-Government Strategy Framework Policy and Guidelines* [4]:

- **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 information 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 of his virtual identity is the true owner of the information supplied during the registration process by means of a password or biometric for instance.

- **Authorization** Authorization is the granting of rights to access services, information and resources.

6.1 Registration, Authentication and Authorization Processes

In the context of this document, registration and authentication services comprise the following processes:

a. Effective user registration

b. Effective user identification;

c. Effective user authentication;

d. Effective authorization/access control;

e. Effective user management.

6.1.1 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 Registration Authority may be involved in operating the registration process.

6.1.2 Effective User Identification

The aim of user identification is to determine the appropriate user information for the service required. This includes information used for authentication.

Note that in some cases it may be necessary to protect the real world identity of the individual for privacy and provide pseudonymous or anonymous identity. In this case, proper authentication is no less important (see section 6.1.3 below).

6.1.3 Effective User Authentication

The aim of user authentication is to ensure that access to the service is only granted to individuals or pseudonyms whose registration information has been validated. The claimed user identity can be verified e.g. by a **digital certificate**, and **passwords**, **biometrics** or **smartcards**.

6.1.4 Effective User Authorization/Access Control

Authorization refers to the granting of permission to a user to access an e-business system, e-business service, network, application or file; access control is the means by which the access is restricted to authorized users. User authorization defines the user's privileges to access objects such as systems, applications or single information objects. It also defines the function the user is permitted to perform.

Authorizations can be directly or indirectly assigned to the single user. A typical example of direct assignment are the use of **access control mechanisms, like access control lists (ACL)** and **firewalls** that will help prevent all unverified users (including "hackers") from gaining unauthorized access (these matters are dealt with in section 9 on Network and Information Security Services). In the case of indirect assignment, the rights are assigned to roles, which themselves can be assigned to users. A user can have many roles. These mechanisms are typically called Role Based Access Control (RBAC). Access control in an RBAC system is

based on the existence of different roles. The permissions to perform certain operations are assigned to specific roles. RBAC access control mechanisms have gained acceptance and a number of organizations have developed, or are currently developing RBAC standards for specialized domains, in addition to general purpose RBAC standards. As an example of these specific domains, it is interesting to note that RBAC has a natural fit with many health care applications. Standards are being developed under the HL7 Standards Development Organization (see also Section 11.2). RBAC based systems are also used to secure the networks and applications that control power plants, manufacturing facilities and other process control systems (see also Section 11.3). More information on RBAC can be found on web site [Web-Site 37].

Authorization may utilize software-based access control mechanisms operating at a service, file or record level. Examples of software based access control mechanisms are access control lists and attribute or authorization certificates where access permissions are held in digital certificates. In the Web Services world, SAML (Security Assertion Markup Language) assertions can also be used to carry attribute statements (attributes are used during the authorization decision process) and authorization decision statements. Also in the Web Services world, XACML (eXtensible Access Control Markup Language) can be used for representing authorization and entitlement policies. XACML also has a "Core and hierarchical role based access control profile", which makes XACML appropriate for implementing an RBAC system.

6.1.5 Effective User Management

The aim of user management is to control and maintain user profiles in order that service users may access those parts of the user profile that are necessary to carry out their e-business activities. User authentication and access control (by using authorization attributes, or role based access) should be used to manage user access in accordance with the user profiles. The user profile information may be stored centrally or distributed, but in any case, it should be stored in a secure way (preferably encrypted) so that user authentication and authorization is necessary before disclosure of the user profile information.

6.1.6 User Management in Healthcare

In healthcare, user registration, identification and authentication are in place or in preparation across Europe.

In the context of identification of patients, the European Electronic Health Insurance Card (EEHIC) is the dominant project, regardless of the different approaches for patient identification isolated for health purposes or combined with citizen functionalities. An EEHIC standard has been announced.

In the context of identification of health professionals, a harmonized approach is applied, based on CEN ENV 13729 "Health informatics – Strong authentication using microprocessor cards", which is currently under revision to become an European standard.

In integrated health care arrangements, the identification and authentication of all entities involved is required. This includes users, organizations, systems, devices, applications, components and single object taking part in communication and co-operation.

The harmonized and standardized approach applied for identification (see above) has also been announced for authentication of patients, citizens and health professionals. In addition, there are national health telematic platform programmes.

6.2 Security Measures

6.2.1 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, or using a hardware device.

Another alternative to username/password authentication providing better protection is the use of "Password Authenticated Key Agreement", which is an interactive method for two or more parties to establish cryptographic keys allowing for relatively simple passwords. With password authenticated key agreement, a user logs into a remote server using his user name and password. The communication between user and server is protected in such a way that no information about the password can be obtained. Furthermore, the server is aware of all login attempts, so excessive password attempts can be blocked. This implies that man in the middle attack and exhaustive password search are impossible, even with direct access to the server.

An implementation of password authenticated key agreement is proposed under the Secure Remote Password (SRP) scheme. It is proposed for use with the Transport Layer Security (TLS) protocol. Details can be found in the IETF RFC "RFC 2945: SRP Authentication and Key Exchange System".

Recommendation 4 Promote the use of SRP in website authentication for all applications and highlight to all parties involved (users, content providers and developers) that usercode and password, even when encrypted over TLS, is not secure enough for financial and other high security applications.

Suggested responsibility: Standards bodies, industry, Member States, and the Commission

Priority: Medium

Deadline and Timeframe: This activity should start within the next year, because passwords are used more and more often every day, and a standard secure alternative is not available.

6.2.2 Biometrics

In some cases the use of biometric methods on their own may offer a convenient and practical alternative to authenticate or verify individuals. As with all technologies, biometrics, too, have their own specific vulnerabilities. Biometrics 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. Any biometric system has a FAR (False Acceptance Rate) and a FRR (False Rejection Rate) dependent on the "margin of error". However, this margin of error may allow an unauthorized user to gain access to the system. Other biometric vulnerability is spoofing (e.g. of signature, voice recording, or fake finger using the residual image left behind on a fingerprint reader).

Identification using biometrics is prone to error as soon as the number of users becomes high. It is not recommended to use biometrics alone for identification in a secure environment.

Nevertheless, Biometric 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).

Biometric technology involves a probabilistic comparison process that cannot guarantee unique verification of individuals. The ability to discriminate between individuals depends on the modality used (e.g. face, fingerprint, iris) as well as the implementation details and is typically expressed in terms of the FAR. FAR can be used to denote the discrimination ability and the values can range from hundreds to millions.

With passwords and smartcards, regardless of their technical security, there is no guarantee that the presenter is the rightful owner. Biometric authentication is however constrained by the performance limitations (i.e. FAR) and any underlying vulnerabilities (e.g. spoofing and capture/replay attacks). These have to be assessed through security evaluation to determine the residual risks, in the same way as for vulnerabilities of password and smartcard based authentication mechanisms. Because the vulnerabilities of the various biometric mechanisms tend to lie in different areas, the combination of several mechanisms can be a powerful tool to provide much stronger overall assurance of true authentication. The security provided by a biometric system should be evaluated, taking account of the security requirements of the application(s) where its use is intended.

If a large number of biometric devices are used to measure biometric properties, these devices might not be owned by the party that relies on the biometric authentication. In this case, it might be necessary for the devices to prove their identity and proper operation. These issues are currently not well addressed in the literature.

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, such as ISO/IEC JTC 1 SC 27 and SC 37, work on biometrics is also being carried out in several national and international groupings.

In Europe, the CEN/ISSS Focus Group on Biometrics aims to support the interchange of knowledge and understanding among European national standards bodies in support of an effective participation in JTC 1/SC 37 and to provide a forum for more detailed consideration of European requirements.

Recommendation 5 A specific biometric profile for cross-border interoperability of biometrics applicable to e-Identity should be developed and promoted. International committees address identity and security without consideration of European specific needs because at international level, there are no configurations implying multiple Member States. The profile should address specifically the issues of FAR/FRR discrimination and data protection particularly in regard to European Directives and the recommendations of the Data Protection European Committee (Article 29), which this report has identified as an essential issue for wide public acceptance.

Suggested responsibility: CEN ISSS Focus Group on Biometrics

Priority: High

Deadline and Timeframe: Identification of the requirements for this profile should start as soon as possible, and this activity should continue as long as it is necessary to support the inclusion of European needs.

Recommendation 6 Conformance and interoperability mechanisms, both for applications and sensors, should be promoted in order to reach security evaluated interoperable solutions between Member States.

Suggested responsibility: CEN ISSS Focus Group on Biometrics

Priority: Medium

Deadline and Timeframe: This activity should start within the next months, to ensure that these conformance and interoperability means can be built in applications and sensors and to achieve interoperable solutions.

6.2.3 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.

6.2.4 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. Smart cards 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.

Smart cards can provide a good solution for authentication and payment, where the card is used in a controlled environment and the card holder is not treating the card as a trusted / signature token. If the card 'signs' a message in this context, it is a card signature and not a user signature (i.e. the certificate and public key belong to the card). However, they are quite unsuitable as trusted tokens for electronic signature because they have no trusted human interface (display, keyboard).

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.

There are strong synergies among standardization groups at International (ISO/IEC JTC 1/SC 17, SC 27, SC 37) and European level (CEN/TC 224, CEN/ISSS FG Biometrics):
The SC 17 (card oriented) working groups are improving the physical & electrical characteristics (cycle duration, new electrical tests particularly for contactless cards) with a high impact on the travel documents work related to the ICAO specifications. Regarding particularly the epassport application, the work refers to the SC 37 (biometrics oriented) works (biometrics data interchange format, CBEFF, etc.). All the security aspects for the use of the biometrics, Authentication context and Security evaluation, have been developed within the SC 27 (Security techniques oriented).

At a European level, CEN/TC 224 (card and electronic signature oriented) is developing a specification for a European Citizen Card (ECC) which could be the technical reference for the Schengen passport and European third country resident card (and, if needed, at national level for an eID card). The work refers to the International standards (physical and electronic card characteristics, biometrics and its use).

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, Eurosmart, and the ISCI (International Security Certification Initiative). Other activities include the ETSI SCP Smart Card Platform [Web-Site 41] and TSG CT WG6 (Smart Card Application Access) at [Web-Site 42].

7 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 TETRA, TISPAN and 3GPP.

7.1 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[8], destination etc., see [Web-Site 7].

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 section 6). However, this section 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 **media disposal and re-use** procedure to prevent the accidental release of sensitive information to unauthorized individuals.

c. **Privacy** preserving measures.

7.2 Encryption of stored information

There are many stand-alone consumer-oriented PC-based products available for encrypting stored information. Unfortunately these might be 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. Note that TLS/SSL and PGP are not effective for the encryption of stored information.

Personal key management is best handled using a personal key ring. The user should have the option to store all his keys under a general password in his key ring, together with the passwords used for authentication of services.

7.3 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) provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (by using digital signatures), and data confidentiality (by using encryption). S/MIME version 3.1 is described in RFC3850 through RFC3852.

Messages are encrypted using symmetric encryption but use an asymmetric (public key) mechanism to exchange the content encryption (and decryption) key. 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.

Conformant applications using S/MIME v3.1 should support the Triple DES, RC2 and AES standards for symmetric encryption of their content. Today, AES is preferred over Triple DES for two reasons: (i) AES is widely believed to be faster than Triple DES and of comparable security. (ii) AES is also believed to have comparatively low memory requirements, which makes it suitable for use in mobile or embedded devices. This is why the IETF SIP (Session Initiation Protocol) have updated their SIP RFC (RFC3261) in RFC3853 (S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)) to require the use of AES for S/MIME.

[8] Note that protection of origin information will not be appropriate in the case of emergency services

The content decryption key is also encrypted (and sent from the sender to the receiver) either with the Rivest-Shamir-Adleman encryption algorithm (RSA) (see RFC3447) or using Diffie-Hellman in ephemeral-static mode (RFC2631). With respect to signature algorithms, conformant applications, using S/MIME v3.1 should support the Digital Signature Algorithm (DSA) that is defined in FIPS Pub 186, or the RSA signature algorithm defined in RFC3447.

Other products such as Pretty Good Privacy (PGP), first created by Phil Zimmermann in 1991, are also widely used but have not been published as an official standard. However, the IETF OpenPGP working group has created the OpenPGP proposed standard in RFC2440, and is currently working on a new version of this RFC. Because there was already a significant installed base of PGP users, the working group only considers compatibility and interoperability issues to avoid disenfranchising the existing community of PGP users. The main issue surrounding the use of products such as PGP is the lack of a standard infrastructure for key distribution.

ETSI TC ESI has started some activities on a Registered EMail (REM) framework. The aim is not only to provide email encryption services, but also integrity, time stamping and non-repudiation.

Recommendation 7 Identify solutions providing secure E-mail that can be routed through a company firewall.

Suggested responsibility: ETSI TC ESI (if this is not within the scope of the current programme of work, ETSI TC ESI can refer to another group that is dealing with this issue)

Priority: Medium

Deadline and Timeframe: This activity should start within the next year, since the need for strongly protected email is already there.

7.4 Network Encryption

Securing the communication between two entities can be done at different layers in the protocols stack. The choice of layer depends on the type of communication between the entities and on the security requirements of the application.

One option is to provide security at the lowest layer in the protocol stack if we want to secure all communication between two entities. The industry standard network layer protocol for the Internet is the Internet Protocol (IP) standard. IPsec provides security for the IP protocol. The security services offered by the IPsec protocol are mainly: secure authentication of the end-nodes, confidentiality and integrity protection of the data communication.

Many applications make use of the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) as transport protocol. TCP is used to communicate between client and server in a client/sever environment and supports applications such as HTTP, electronic mail or file transport (FTP). These applications can secure their own communication by using the Transport Layer Security (TLS) protocol, which runs on top of TCP. The security services offered by TLS are: secure authentication of the end-nodes, confidentiality and integrity protection of TCP-based communication. Recently, also the DTLS protocol, to be used as security layer on top of UDP, has been specified within IETF (in RFC4347). The DTLS protocol is based on the Transport Layer Security (TLS) protocol and provides equivalent security guarantees.

More complex applications are realized in the form of Web Services. Web Services communications is based on the Simple Object Access Protocol (SOAP). SOAP messages are (mainly) transported over HTTP. Using TLS to secure this SOAP message transport only results in a point-to-point (or hop-by-hop) security model. End-to-end protection of Web Services communications is provided by securing the SOAP communication. The Web Services Security specifications describe the security mechanisms that are available to protect SOAP communication.

For a more detailed consideration of network encryption, please refer to Annex 1.

7.5 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 delivered algorithm specifications to the Third generation Partnership Project (3GPP) for the protection of confidentiality and integrity of information transmitted over third generation (3G) cellular communication systems.

ISO has specified a list of encryption algorithms divided into two families: stream ciphers and block ciphers. The detailed information can be found in the following standards:

- ISO/IEC 18033-3: *Encryption algorithms – Part 3: Block ciphers*.
- ISO/IEC 18033-4: *Encryption algorithms – Part 4: Stream ciphers*.

At european level, ECRYPT - European Network of Excellence for Cryptology is a 4-year network of excellence. ETSI has defined a list of hash functions and a list of signature schemes, the recommended combinations of hash functions and signatures schemes in the form of "signature suites", and the symmetric algorithms and protocols to be used to construct a secure channel between an application and a signature creation device. This list can be found in:

- TS 102 176-1 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
- TS 102 176-2 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices

One particularly important part of the ECRYPT project is the *eSTREAM* project (see [Web-Site 20]). The aim of eSTREAM is to promote the development of new stream cipher primitives. Stream ciphers form a sub-class of symmetric encryption techniques and while there are many in commercial use, as a field it has not benefited from the existence of open standards in the same way as block ciphers.

As research is ongoing on determining the strength, and finding weaknesses in existing cryptographic algorithms, research is also needed in new and improved cryptographic algorithms, also taking into account that these algorithms might run on resource constrained devices.

Recommendation 8 NIST is currently developing a new hash standard. Activities in Europe should follow this development and join the effort.

Suggested responsibility: ETSI SAGE to consider developing a liaison statement, and possibly 7 Framework Programme for Research and Development

Priority: High

Deadline and Timeframe: The timeline of the NIST hash standard is so that the new hash function is announced at the end of 2011.

7.6 Privacy

Protection of privacy is an important aspect of network security, from the standpoint of the user. For some applications, such as electronic voting, privacy and authentication are the most important security aspects of the application

On the other hand, there are circumstances where security measures reduce privacy, e.g. a company monitoring system user activities. It is recommended that security measures are implemented in such a way that privacy reduction is kept to a minimum, and in case of the example, any such monitoring should comply with appropriate legal requirements such as the Data Protection Act.

Storage of personal information, if necessary, should be protected so that only authorized users of the database can access it and only when necessary. Personal information that is not necessary for the service should not be stored. By EU law (Directive 95/46/EC), personal information should be verifiable by the owner of the information.

There are two initiatives that address the problem of identity and privacy protection. The Liberty Alliance (see [Web-Site 8]) consortium "is committed to developing an open standard for federated network identity that supports all current and emerging network devices." The Platform for Privacy Preferences Project (P3P, see [Web-Site 9]), "is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit."

Recommendation 9 Today, many Web sites and web applications collect user sensitive data. It is unclear how well these web sites protect this end-user data. More research is necessary on end-user privacy preserving technologies.

Suggested responsibility: CEN ISSS Workshop on Data Privacy, for further consideration of this recommendation

Priority: High

Deadline and Timeframe: Privacy preserving techniques should be readily available in a short time frame.

Recommendation 10 With respect to identity management, competing solutions and standards exist (i.e. the specifications of the Liberty Alliance Project and specifications from W3C and OASIS). These different standards will hinder interoperability. Synchronization between these standardization efforts is recommended.

Suggested responsibility: ISO/IEC JTC1 SC 27

Priority: High

Deadline and Timeframe: Work on synchronization of the specifications of different standardization bodies should start as soon as possible.

Recommendation 11 It is recommended that international standardization bodies, like ISO, ITU-T, ETSI, or 3GPP should further develop work on end-user (data) privacy protection and identity management, based on current activities from Liberty Alliance Project, W3C and OASIS.

Suggested responsibility: ISO/IEC JTC1 SC 27, ITU-T, ETSI, and 3GPP

Priority: High

Deadline and Timeframe: The respective standardization bodies should start Privacy and Identity management activities now.

Recommendation 12 The implications on user privacy of new security services such as Biometrics techniques, RFID or others should be analyzed in order to reach common understanding and recommendations between Member States.

Suggested responsibility: ICTSB and Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data (as far as policy issues are concerned)

Priority: High

Deadline and Timeframe: This activity should start within the next months, to ensure that new security solutions meet the privacy requirement of each state.

7.7 Media Disposal and Re-use Policy

A media 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, computers or storage media are released for disposal without securely erasing or overwriting their content. 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.

There are already many guidelines and recommendations available for adequate media sanitization. In addition, several companies and government agencies (e.g. NIST or the German Information Security Agency) offer consultancy and products to securely delete media for re-use or disposal. Some tools are even freeware.

8 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 to support that fact. They ensure that commitments 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.

8.1 Trust Service Processes

In the context of this document, trust services comprise the following processes:

a. Key Management

b. Non-Repudiation.

c. Trusted Commitment Service.

d. Content 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 notarisation services (the IETF LTANS (Long-Term Archive and Notary Services) working group considers these issues).

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

8.1.1 General Key Management

The essential part of every cryptographic system is 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 secret keys, public keys and certificates.;

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 this document but can be found at [Web-Site 13]).

Key management is treated in detail in ISO 11568: Banking -- Key management (retail), and also in ISO/IEC 11770, which is a four part standard comprising Part 1: Framework, Part 2:

Mechanisms using symmetric techniques, Part 3: Mechanisms using asymmetric techniques and Part 4: Mechanisms based on weak secrets.

There is a significant difference in key management techniques for symmetric key systems and public key systems. Secret key management is key management of secret keys, where the involved parties share the same key value. Often, the key value is distributed as an encrypted value under another key, normally called *transport key*.

Detailed treatment of secret key management can be found in Part 2 of ISO 11568 and in Part 2 of ISO/IEC 11770.

8.1.2 Public Key Management

Public key management is key management of public keys. Since a public key pair consists of two parts that have different security requirements, public key management is more complicated yet has more possibilities than secret key management. Detailed treatment of public key management can be found in Part 4 of ISO 11568 and in Part 3 of ISO/IEC 11770.

Management of public keys is normally handled by a public key infrastructure (PKI). A PKI allows secure distribution of the public key part among parties that have no previous contact by including the key together with the owner's identifier in a certificate signed by a root key that is trusted. Maintaining a PKI requires the secure distribution, revocation and replacement of the root keys.

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 and generation of certificates to prove this.

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 and, where appropriate, the provision of facilities for access to keys for law enforcement purposes (key escrow). This is not applicable for signature keys.

g. Revocation of stolen keys.

It is important that users can use the PKI to verify the validity of a given certificate to find out information about the owner. Very sensitive applications will even require the possibility to check that certificate validity online. Fraud using fake certificates is just beginning, and is expected to grow in the near future. Examples of fraud include the use of fake certificates as a result of delays in the revocation of old certificates, or where the identification of a user has not been properly established at the time a certificate is issued.

Various groups such as the IETF PKIX WG, NIST, The Open Group and national governments, are developing PKI standards. There are also many commercial PKI products in the market place.

ETSI and CEN co-operated on the European Electronic Signature to provide Europe with a reliable electronic signatures framework to enable electronic commerce and support the

eSignature EC Directive. Current challenges are eInvoicing and Registered Email (REM) being undertaken. International collaboration is being undertaken with Certificate Policy mapped and aligned with US policy and the XML Signature Standard adopted in Japan

However it should be noted that many end users find PKI products difficult to understand (lack of adequate, basic documentation) and to use (poor user interfaces).

Recommendation 13 Further information and education of all users of certification services about the use of certificate is needed. All ICT stakeholders should cooperate in editing clear guidelines for the users on the advantages and risks related to certificates.

Suggested responsibility: ENISA

Priority: Medium

Deadline and Timeframe: End 2008

8.1.3 Non-Repudiation

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

- Non-repudiation of creation. Providing proof that the originator created the message.
- Non-repudiation of delivery. Providing proof that the intended recipient received the message and recognized the content
- Non-repudiation of knowledge. Providing proof that a recipient took account of the message contents
- Non-repudiation of origin. Providing proof that the originator created and sent the message
- Non-repudiation of receipt. Providing proof that the intended recipient has received the message.
- Non-repudiation of sending. Providing proof that the originator did send the message
- Non-repudiation of submission. Providing proof that a delivery authority accepted the message for transmission
- Non-repudiation of transport. Providing proof that a delivery authority has delivered the message to the intended recipient.

Measures which support non-repudiation services 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.
- **Smart cards** may be used as signature creation devices to carry public and private keys and **digital certificates**.

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** (see 8.1.2 above).

The standard that describes non-repudiation mechanisms is ISO/IEC 13888; this is a three part standard comprising Part 1: General, Part 2: Mechanisms using symmetric techniques and Part 3: Mechanisms using asymmetric techniques.

8.1.4 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.

8.1.5 Content Integrity

The aim of a content 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:

- For protection against non-malicious events, such as accidental corruption, simple **checksums** may be adequate.
- For protection against malicious attacks **digital signatures** (see also 8.2.1 below) should be used. Such a signature consists of a signed hash of the message that is appended to the transaction by the originator and is verified by the recipient. A PKI may be used to support an electronic signature regime.

8.2 Security Measures

8.2.1 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. This report 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 or en-route by other parties. 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 and compares it to the hash of the message to prove origin and integrity.

On 1999-12-13 the European Commission published Directive 1999/93/EC to provide a Community framework for electronic signatures (Dir.1999/93). Details can be found at [Web-Site 10]. 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.

CEN/ISSS has developed documents through the operation of an open technical Workshop "CEN/ISSS Workshop on Electronic Signatures (E-SIGN), created specifically for this purpose. Documents developed and approved by this process are CEN Workshop Agreements (CWAs). After the closure of this workshop, the maintenance of some CWAs has been appointed to CEN/TC 224 (Machine readable cards, related device interfaces and operations), and ETSI TC ESI. Further information is available from [Web-Site 12].

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. Further information is available from [Web-Site 32].

Under a Commission Decision of 14 July 2003, two CEN Workshop Agreements (CWA 14167-1 and CWA 14167-2) 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) in a separate list of the generally recognized standards in compliance with Annex III of the Directive.

In the United States, The Digital Signature Algorithm (DSA) was proposed by the NIST in August 1991 for use in their Digital Signature Standard (DSS), specified in FIPS 186 [Web-Site 38], adopted in 1993. A minor revision was issued in 1996 as FIPS 186-1 [Web-Site 39], and the standard was expanded further in 2000 as FIPS 186-2 [Web-Site 40].

8.2.2 Hash Functions

A hash function is a function which compresses strings of bits (input string) to fixed length strings (output string) such that it is infeasible to find two different input strings yielding the same output string. This implies that:

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

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

c. most importantly, if the output string value of a given input string has the correct value, the input string should also be correct.

8.2.3 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 a three part standard comprising Part 1: Framework, Part 2: Mechanisms producing independent tokens and Part 3: Mechanisms producing linked tokens. ETSI have also produced ETSI TS 102 023 v1.2.1 *Policy requirements for time-stamping authorities*.

8.3 Harmonization of Trust Services

ETSI and CEN via the European Electronic Signature Standardization Initiative (EESSI) did undertake work on the harmonization of trust service provider services. EESSI was created in 1999 by Information and Communications Technologies Standards Board (ICTSB) to co-ordinate the standardization activity in support of the implementation of Directive 1999/93/EC on electronic signature. Standardization activities were carried out in the CEN/ISSS E-sign workshop and the ETSI TC SEC/ESI. The references to the required standards were published in the Official Journal in July 2003. These standards are part of a longer set of specifications defined by EESSI and included in their work programme. With the publication of this full set of standards, EESSI has fulfilled its mandate and consequently ICTSB decided to close EESSI in October 2004. Further information regarding EESSI can be found at [Web-Site 11], and now NISSG is responsible to coordinate these activities.

However, note that standardization work in this area is still ongoing, even though it is currently at a lower level of activity. The Commission will launch a study on eSignatures in 2007 on standardization aspects. By assessing the model proposed by the Directive 1999/93/EC on electronic signature, the study shall provide the information and assessment needed for a possible review of the needs for standardization in this context.

9 Network and Information Security Management Services

Network and information security management services refer to the overall information security management that should be applied to secure any e-business services and applications. Whilst Sections 6 – 8 refer to specific security solutions, this section provides the framework in which these security solutions can be applied. This section first discusses risk assessment, which should be the basis of any security measures being selected to achieve network and information security services. It then discusses the various standards that can be used to achieve these security services, and finally several different examples of security measures that can be considered.

The next part of this section discusses business services, which 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 in the context of this report includes applications such as web services, interactive services and electronic messaging.

This section finally considers network defence services, which provide the means by which malicious threats emanating from electronic connection to external IT resources and networks (including the Internet) are countered.

9.1 Security Measures

Network and information security management services comprise the following security measures:

a. Risk assessment

b. Information security management standards

c. Examples of security measures for business services

d. Examples of security measures for network defence services

9.2 Risk assessment

Risk assessment should be the basis of any risk management decision and selection of security measures. It is important to identify all information security requirements, to identify the assets of the organization and how important they are for the organization, to identify the threats and vulnerabilities and the likelihood of threats exploiting vulnerabilities, and the overall risk situation resulting from that.

ISO/IEC CD 27005 (see 9.3 below) is a recognized international reference on information security risk management and provides useful information on how to carry out risk assessments and what type of information to take into account in that process. Guidance material has also been issued for specific sectors (national and international) and by industrial fora (such as the International Security Forum) and academic consortia.

9.3 Information security management standards

9.3.1 27000 Family of standards

There are several standards currently in development to support information security management. They are developed in ISO/IEC JTC 1 SC 27, and these standards are summarized in the 27000 family of standards. The aim of these standards is to support the information security management system standard ISO/IEC 27001 (see also Section 10.3 for more detail about this).

These standards are listed on [Web-Site 1], but they are also briefly discussed here to give some further information about their content:

a. ISO/IEC 27000 Information security management system fundamentals and vocabulary.
This standard is currently at WD level and discusses the underlying principles of information security management, explains the concepts applied in the 27000 family of standards and includes the vocabulary used in that family.

b. ISO/IEC 27001 Information security management system – Requirements
This standard describes the requirements to establish, implement, operate, monitor,

review and improve an ISMS in an organization. In addition, it can be used for third party certification, and is discussed in Section 10.3 below.

c. ISO/IEC 27002 Code of practice for information security management
This standard is currently numbered and well known as ISO/IEC 17799:2005 and will be renumbered in Spring 2007 to make it part of the 27000 family of standards. It contains a set of best practice controls for information security management. These controls should be selected based on a risk assessment, and additional controls can be used, as required. The controls of this standard are also contained in Annex A of ISO/IEC 27001 and are therefore part of the ISMS process described in ISO/IEC 27001.

d. ISO/IEC 27003 Information security management system implementation guidance
This standard is currently at WD level, and gives implementation guidance to support the establishment, operation, implementation, review, maintenance and improvement of the ISMS.

e. ISO/IEC 27004 Information security management measurements
This standard is also at WD level, and describes metrics and measurement procedures to determining and describing the effectiveness of information security controls, information security processes, and information security management systems.

f. ISO/IEC 27005 Information security risk management
This standard is at 1st CD level and discusses techniques for risk assessment and risk management, to address the requirements contained in ISO/IEC 27001.

g. ISO/IEC 27006 Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems based on the Conformity Assessment standard ISO/IEC 17021
This is at the moment a suggested New Work Item, and will replace the currently used accreditation guideline EA7/03 – more about this document and other information about accreditation is contained in Section 10.4 below.

9.3.2 Other standards for security measures and services

In addition to the standards in the 27000 family of standards, there are standards elaborating on particular security measures and services. They are also developed in ISO/IEC JTC 1 SC 27:

a. ISO/IEC TR 18044 Information security incident management.

b. ISO/IEC TR 15947 IT intrusion detection framework.

c. ISO/IEC 18043 Selection, deployment and operations of intrusion detection systems.

d. A five part standard on IT network security, comprising:

- ISO/IEC 18028-1 IT network security — Part 1: Network security management,
- ISO/IEC 18028-2 IT network security - Part 2: Network security architecture,
- ISO/IEC 18028-3 IT network security - Part 3: Securing communications between networks using security gateways,

- ISO/IEC 18028-4 IT network security — Part 4: Securing remote access,
- IS 18028-5 IT Network security — Part 5: Securing communications across networks using virtual private networks.

9.4 Examples of security measures for business services

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, or the impacts of natural disasters affecting business services.

9.4.1 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:

- The use of commercial best practise products and adherence to good practise for system design, implementation and operations.
- Ongoing **Failure Impact analysis**, **Capacity Planning**, **Business Continuity Planning** and **Configuration Management**.
- Alternative communications facilities in case of failure, the availability of battery backup or Un-interruptible Power Supplies (UPS) need to be in place.
- Regular testing of system recovery.
- Service Level Agreements setting out availability targets with clients of the service.

The CEN BT Working Group 161 was set up in order to identify needs and possibilities for standardisation activities for security and emergency preparedness within energy supply.

9.4.2 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

9.4.3 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 analyze 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.

9.4.4 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.

9.4.5 Capacity Planning

E-business service providers should 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 and reflected in SLAs with customers.

9.4.6 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 are as yet no internationally approved standards. Protecting against critical national infrastructure (CNI) threats is an important role for any government to ensure the continuity of society in times of crisis. In the UK, the NISCC has been set up to minimize the risk to the CNI from electronic attack; other parts of government work to protect the CNI from physical attack or natural disasters (more on [Web-Site 14]).

9.4.7 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.

9.4.8 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.

9.5 Examples of security measures for network defence services

If threats to network services 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.

9.5.1 Preventive Measures

Preventive 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**. This includes screening of all imported and exported material for recognizable virus signatures or other unwanted content. ANEC, the European Association for the Co-ordination of Consumer Representation in Standardization, and a CEN Associate Member, has commissioned a report into the potential of standardization in this domain, which can be downloaded from [Web-Site 15]. In addition, all imports transaction should be recorded 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[9].

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 [Web-Site 16].

g. Using evaluated products (see Section 10.2).

9.5.2 Detection Measures

The main technical measure is the deployment of **Intrusion Detection Systems** (see also 9.3.2 above). 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.

Recommendation 14 The detection and prevention measures described here should be further developed and, if possible, standardized in order to protect against malware, adware, spyware and viruses which are always evolving.

Suggested responsibility: NISSG to consider inputs from CEN BT WG 194, ETSI TISPAN and 3GPP

Priority: High

Deadline and Timeframe: This is a permanent and never ending effort.

[9] Note that Firewalls which are effective against IPv4 may not be effective against the emerging IPv6 protocol

10 Assurance Services

Previous sections 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 all users of these 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 this section is to provide that confidence.

There are different ways of how this assurance can be achieved:

a. Product-based certifications or evaluations;

b. Establishment and/or certification of an Information Security Management System (ISMS).

Regardless which of these ways (or a combination) to achieve assurance is chosen, it should always be based on a risk assessment to identify the most appropriate solutions.

Any use of third party evaluation or certification will increase inter-organizational and customer confidence. Particular confidence in an e-business service will also be created if the organization providing the service conforms to an internationally recognized standard for the overall management of Information Security.

10.1 Security Measures

In the context of this report Assurance Services comprise the following security measures:

b. Product evaluation.

c. Information security management system certification

d. Accreditation.

10.2 Product 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. Certification can also be awarded for products that have successfully undergone evaluation.

It is important to understand that this evaluation is always a snapshot in time, and any modification of the product or system under consideration might make a re-evaluation necessary. It is therefore important to understand that product or system certification or other forms of assurance related to that should only be used if the risk assessment has determined the requirement for this, and that this form of assurance is the best way to manage the identified risks. Nevertheless, to support product changes and to extend the validity of certificates, national certification schemes provide an assurance continuity program not only including re-evaluation, but also maintenance and surveillance processes. 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 Information technology - Security techniques - Evaluation criteria for IT security; 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 and are the international scheme for product evaluation. The standard ISO/IEC 15408 has been recently updated, and the most recent version is ISO/IEC 15408:2005. Certification based on Common Criteria is performed

by several national certification schemes of member states. Mutual recognition agreements are in place to ensure European and international recognition of their certificates issued for products and protection profiles.

There is also the standard ISO/IEC 19790:2006, which specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems. This standard has been derived from NIST Federal Information Processing Standard PUB 140-2 May 25, 2001.

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 and CWA 14167-3). In ISO, there is also the standard ISO/IEC 15292 for the registration of protection profiles and ISO/IEC TR 15446:2004, which provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with ISO/IEC 15408 (the "Common Criteria").

In addition to the above, a framework for IT assurance has been developed in ISO, and this is contained in the multipart standard ISO/IEC TR 15443. Parts 1 and 2 of this standard are published:

a. ISO/IEC TR 15443-1:2005 describes the fundamentals of security assurance and its relation to other security concepts. This is to clarify why security assurance is required and dispel common misconceptions such as that increased assurance is gained by increasing the strength of a security mechanism. The framework includes a categorization of assurance types and a generic lifecycle model to identify the appropriate assurance types required for the deliverable with respect to the deliverable's lifecycle.

b. ISO/IEC TR 15443-2:2005 describes a variety of IT security assurance methods and approaches and relates them to the IT security assurance framework in ISO/IEC TR 15443-1. The emphasis is to identify qualitative properties of the assurance methods and elements that contribute to assurance, and where possible, to define assurance ratings. This material is intended for IT security professionals for the understanding of how to obtain assurance in a given life-cycle stage of a product or service.

Another standard that has been developed is the Capability Maturity Model for System Security Engineering (SSE-CMM) ISO/IEC 21827. The SSE-CMM is a process reference model that focuses on systems security engineering, especially for security service providers and product developers. The SSE-CMM Model is focused on the processes used to achieve IT security, most specifically on the maturity of those processes. The scope encompasses:

a. The SSE-CMM addresses security engineering activities that span the entire trusted product or secure system life cycle, including concept definition, requirements analysis, design, development, integration, installation, operations, maintenance, and decommissioning;

b. The SSE-CMM applies to secure product developers, secure system developers and integrators, and organizations that provide security services and security engineering.

Note: ISO/IEC 21827:2002 is freely available at [Web-Site 34] and a new version is now under review.

10.3 Information Security Management System Certification

Certification of ISMS is a procedure where an independent third party assesses the management system of an organization against the ISMS standard ISO/IEC 27001:2005 (see 9.3). This provides written assurance that the ISMS of the organization conforms to the standard. This includes all activities the organization has in place to establish, implement, operate, monitor, review and improve the ISMS. In addition to third party certifications, the standard can also be used for peer assessments or own initiatives.

The organization can determine the scope of the assessment, e.g. the whole organization, or a part of it, or a particular department, service of business process. The ISMS certification assesses whether an organization has carried out a risk assessment (see also 9.2 above) of its operations and has implemented appropriate security controls to counter the assessed risk. ISO/IEC 27001 specifies the typical elements of the risk assessment, but does not mandate a specific method to be used. Therefore, each organization should identify a risk assessment method that suits to their requirements and ways to conduct business.

Organizations that provide accredited certification services need to 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.

The site [Web-Site 17] provides an overview of the accredited ISMS certificates that have been issued, and also information about some of the scopes, and further statistics.

10.4 Accreditation Bodies

National accreditation bodies are set up to accredit certification organizations based upon strict independence. They are signatories to international agreements in order that the methods and practices of Certification Bodies conform to the relevant 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), and the International Accreditation Forum (IAF). More information on these organizations can be found at the respective web sites [Web-Site 18] and [Web-Site 19].

The standard ISO/IEC 27006, which is currently developed within ISO is a joint effort between ISO; IAF and CASCO to develop guidelines and describes guidelines for the accreditation of bodies operating certification of an ISMS, based on the general accreditation standard ISO/IEC 17021.

11 Important NIS-related Topics outside the Scope of this Report

This section highlights important NIS-relevant topics other than eBusiness, starting by a short discussion of the criminogenic nature of using and applying ICT services and products. Another topic that is briefly mentioned here is eHealth, which has a lot of additional requirements to those that are addressed here in this report. Nevertheless, eHealth security can make use of considerable parts of the information provided in this report, therefore it has been included here. Another topic discussed here is Critical National Infrastructures, to

address the increased dependence the Critical National Infrastructures have on network and information security. Finally, this section shows the issues not covered in this report.

11.1 Criminogenic ICT services and products

By their design and range of applications, ICT services and products are tools and facilities that can be used for criminogenic purposes.. Indeed, the following characteristics have made the internet and ICT services very attractive to criminals both individuals or organized associations:

- Transborder communications allowing new crimes and making the task of policing more difficult;
- Ability to remain anonymous;
- Possible opportunities to steal information, IDs and other items;
- Lucrative area for denial of service attacks or intrusion;
- Ease of automated or organized crimes;
- Large scale economic gains for criminals
- Opportunities for hackers, political activists, human and animal rights groups' large scale Internet attacks as a means of bring down companies systems, creating chaos and business interruptions, for media publicity and for furthering their cause.

To limit the number of criminal possibilities, not only is information security vital but also the security of ICT products and services needs to be improved such as having fewer software bugs which can always be exploited by those criminals. They also need security features that can easily be used by normal users and should be used with the security options turned on as default.

Moreover, it is clear that even software security patches and upgrades versions that organizations installed can be inefficient against well-organized criminals, against new and emerging intentional and malicious threats such as denial of service attacks, Internet fraud, viruses and Trojan horses. Very common security products such as firewalls and anti-virus tools are far too complicated for normal users and need proper management to gain value and benefit from these products. Guidelines and support for installation, configuration and maintenance of products should be written in easily understood, non-technical terms. Product suppliers need to develop better ways in which robust security products can be simply configured and maintained by the everyday user.

ISPs should improve their filtering solutions included in their access service. It is also possible to use automated blacklisting of the sources from which they received the problem traffic, to record sources information and if needed to deliver this information to legal authorities.

The variety and complexity of information systems and applications makes it very difficult to define a specific and all embracing set of security standard solutions against the criminal use and exploitation of ICT products and services.

Recommendation 15 Initiatives to educate users about the risks related to Internet services, intrusion attacks, legal issues and malicious software should be encouraged and supported by national government bodies, and standardization organizations, and any ICT stakeholders.

Suggested responsibility: ENISA

Priority: High

Deadline and Timeframe: This is a permanent and never ending effort needing to be actualized according to new services and products launched in the future.

11.2 eHealth

For guaranteeing security, privacy and safety in the special domain of health, there are many developments being progressed as well as already existing standards and other publicly available specifications have been developed and are available. The most important SDOs (standards developing organizations) in this field are:

- CEN/TC251 Health Informatics
- ISO/IEC 215 Health Informatics
- ETSI/ERM/TG30 Wireless Medical Devices
- ETSI/HEALTH
- DICOM Digital Imaging and Communications in Medicine

Due to the complexity of the eHealth issues and the diversity of standards available to address these issues, it is recommended that another initiative is started to address them, possibly also in relation to the standardization mandate for eHealth which was approved early 2007.

Recommendation 16 A project should be started to address the diverse issues relating to eHealth and security. This project should also identify the existing standards and requirements for new standards in the area of eHealth.

Suggested responsibility: ESOs to consider this in relation to the mandate work programme

Priority: High

Deadline and Timeframe: This project needs to start as soon as possible and should be completed before the end of 2008.

11.3 Critical Infrastructures

11.3.1 Pervasive ICT

Networked infrastructures supporting the management of energy supplies, transportation, financial services, government services, etc. are fundamentally changing in the way they are deployed, controlled and monitored. One of the main factors behind this evolution is the pervasive and intensive use of Information and Communication Technologies (ICT). The application of electronic technologies to networked infrastructures began as soon as those technologies were available, because they appeared as an effective means for implementing control and monitoring mechanisms. However, the use of ICT has two sides: while it provides new means for improving the operational and monitoring capabilities, it also opens dangerous opportunities to cyber threats and risks.

Taking as an example the evolution of the electricity generation and delivery systems in Europe, it is difficult to understand how their unbundling and interconnectedness at the Member State level would have made it possible to achieve an integrated European system without the parallel intervention and application of ICT. Within each country, the application of the regulations over the infrastructure depends on the flow of information between actors: be it the application of connectivity rules or tariffs, electricity supplies, information systems based on ICT go together. We can only expect this trend to continue. All aspects of the electric power infrastructure, from the commercial operations in electricity supply exchanges and transportation, to enhanced services to end users, to the assessment and management of risk and costs, etc., are nowadays infused with information. Energy markets function on line. In summary, the electric power infrastructure is information-based:

- within each company: such as operations and maintenance
- in relation with customers: such as energy information services
- between companies: such as management of congestions and contingencies over the power transport network

This scenario presents information security challenges that are not only more numerous or more complex than in the previous periods, but are also different in nature.

The issues outlined for the electricity systems also applies to other energy infrastructures, like oil and gas transport, and more generally to the whole sector of industrial process control – although the extension and complexity of energy delivery infrastructures enhances the impact of local malfunctions, hence the related security risks. Furthermore, similar information security issues and the growing dependence on ICT can be seen in other infrastructural aspects such as water and gas supplies, air, road and sea transportation, health services, emergency services, food supply chains, financial services, government and administrative services.

11.3.2 Consequences of pervasive use of ICT

Most of the technologies used for control systems have shifted towards the adoption of hardware and software components used in general-purpose computation and communication (e.g. operation system, TCP/IP protocols, etc.). Consequently, while taking advantage of the technical possibilities provided by the new ICT, energy systems have inherited dangerous vulnerabilities. In addition, the economic benefits deriving from the adoption of standardized technologies accelerate the implementation of control systems and related communications without any guarantee of secure operation.

Vulnerabilities due to design and technology flaws may be exploited by malicious antagonist actors, who can gain access to the systems through external and internal connections. These threats menace industry throughout the energy industrial sector, as their supervisory control and data acquisition systems (SCADA for short) are based on similar technologies and are deployed using analogous architectures. Standards might help in the protection of SCADA in different ways:

- Help in setting a common conceptual basis between all stakeholders: operators, vendors, certifiers, authorities, etc.
- Supporting all engineering processes: from specification to procurement, and from operation to maintenance.

- Fostering the development of a market for security products and services, with verifiable levels of assurance.

However, there is a time gap between the availability of standards and their application. Security standards in SCADA are as yet not sufficiently mature to guarantee their effectiveness. In the meantime critical infrastructures and the process industry will continue deploying SCADA systems. The situation is challenging, and by all accounts will continue to be so for the next decade – if not more. It is unlikely that effective security standards for SCADA will be available in the short term. In the meantime information and communication technologies are being deployed with an ad-hoc approach to security, based on the restricted knowledge of each company. Related to critical networked infrastructures such as power systems, where information and communication systems are at the core of the interconnections among the different stakeholders, the delay in the availability of effective standards is by itself another vulnerability issue: the near future will see a great window of opportunity for incidents related to intentional exploitation of this vulnerability.

11.3.3 SCADA Standardization in Europe

There are many initiatives going on in the international area regarding security aspects of SCADA systems that respond to the clear and concrete industrial needs. These initiatives are carried out by several organizations, most significantly IEC. Here, two existing technical committees appear specifically relevant:

- IEC TC 65 addressing standardization of SCADA cyber security;
- IEC TC 57 addressing implementation of cyber security features within existing communication protocols for the electricity sector.

The latter, although partly encompassing SCADA, extends beyond to embrace the requirements of innovative measurement systems like wide-area measurement. This is indicative of the need to cover control and communication systems. Based on this and on the wide application on many industrial domains, the area of SCADA (accepting a broad meaning of the term) is wide enough to discuss on its own the approach and requirements regarding standardization actions.

Recommendation 17 Because of the above, it is recommended that CEN forms a new horizontal strategic body on SCADA, possibly in form of a Forum. The purpose could be to create a network of partners for investigation and evaluating further standardization needs, for exchange of information and experience at European level, but also with the US Process Control Systems Forum and other relevant actors worldwide. The first main objective for such a group could be to develop a deeper understanding of the standardization needs in Europe, considering the international arena.

Suggested responsibility: CEN, based on input from JRC

Priority: High

Deadline and Timeframe: This initiative should start as soon as it can be implemented by CEN.

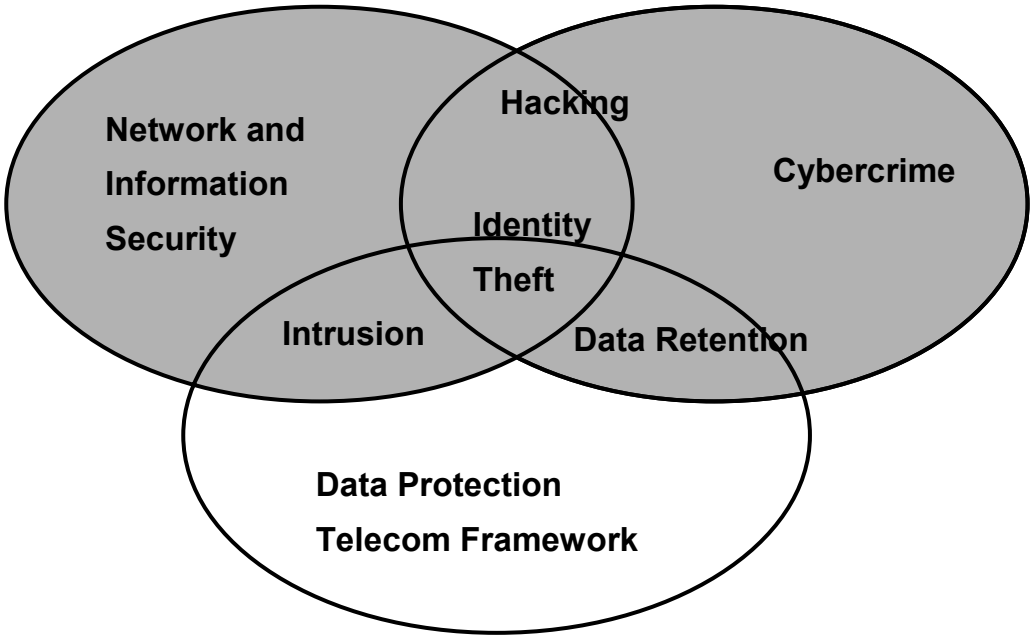
11.4 Autonomous ICT

The individualization of networked services provided to the end user implies the impossibility to adhere on the idea of designing all applications and defining all functionalities and services

bound to them including the underlying policies and conditions for communication and cooperation prior to their use or running the service. As a consequence, based on meta-models, basic principles and a set of rules including user interventions, the applications and policies must be established at runtime. This implies huge challenges not only for development processes and methodologies, but also for the legal and organizational aspects of security services for supporting the autonomous computing paradigm. In this context autonomous policy negotiation and policy bridging are essential requirements, changing the current way of security management.

11.5 Issues not covered in this report

Network and Information Security in the context of this report excludes legal issues and policy and excludes law enforcement (for more information about law enforcement, refer to the Law Enforcement Study COM(2000) 890). In addition, this report does also not address security problems arising from natural disasters and crime risks that are not directly related to network and information security (for crime risks, refer to the EU mandate 355). However, the report includes security services, which can be implemented to control systems inter-relationships, functions and behaviour. The following diagram illustrates what this report covers:



11.5.1 Legal issues

For an overview of legislation issues which may influence standardization of security in Telecommunication Management Networks, the reader is referred to ETSI Technical Report 336 [9]. Digital Rights Management (DRM) has been the subject of a "state of the art" overview by the CEN/ISSS DRM Focus Group (see also the [Web-Site 2]).

Data protection and privacy issues have been considered in the CEN/ISSS Data Protection and Privacy Workshop. More information on that activity can be found on [Web-Site 3].

Information about products and services for lawful interception and standards related to this topic can be found on [Web-Site 4].

11.5.2 Personnel screening

Incident reports suggest that as many as 80% of documented security incidents may be caused by trusted "insiders." Whilst national standards for screening of personnel 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 since it is outside the scope of this report.

11.5.3 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. Relevant national authorities should consider whether there is a need for a common Information Security qualification which will demonstrate a competence of individuals working in the area of information security. This should provide organizations that employ staff or external consultants with a degree of assurance that the individuals they use to implement, manage and advise on issues relating to information security have attained a good level of professional competence. As such individuals will need to engage in work relating to the protection of the organization's critical assets, it makes good business sense to employ people who have a track record in information security and can deploy their competences in a professional manner.

Recommendation 18 Relevant national authorities should consider the need for common information security qualifications, which will demonstrate a competence of individuals working in the area of information security.

Suggested responsibilities: National Authorities

Priority: Medium

Deadline and Timeframe: End 2009.

11.5.4 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. The EU has recently approved a new Data Retention Directive (press release with further information can be found on [Web-Site 5]). In the context of the lifelong electronic health records (EHR), the challenge for checking and verifying signatures has to be met by legal, organizational and technical solutions including the service of re-signing documents.

Also the IETF has acknowledged the problem of long term archiving and is currently conducting work in this (and related) area in its LTRANS (Long-Term Archive and Notary Services) working group. The objective of the LTRANS working group is to define requirements, data structures and protocols for the secure usage of the necessary archive and notary services. First, the requirements for long-term archiving will be collected and based on that information, a protocol to access archive services supplying long-term non-repudiation for signed documents will be defined together with common data structures and formats. Upon completion of the archive-related specifications, 'notary services' will be addressed in a similar way. The working group will determine which functions need standards, including transformation of documents from one format to another without losing the value of evidence,

electronic notarization, and further verification of legal validity of signed documents. Work done by other IETF working groups, like the PXIX, S/MIME, and SMLDSIG will be used as the basis to define the necessary data structures and protocols.

Related with the topic of longevity of archiving, is the topic of records management. This is a topic handled by ARMA [Web-Site 36]. ARMA International is a not-for-profit professional association and is involved in work on managing records and information (in paper as well as in electronic form). The association develops and publishes standards and guidelines related to records management. It was also a key contributor to the international records management standard ISO-15489.

12 New Developments

It is important to take account of new and developing technologies and the impact s these will have on NIS in order to provide effective and appropriate security solutions. It is equally important to be aware of these new developments and their information security implications. Two of the more important new technologies are outlined in the sections below but are not discussed further in the main body of the document.

12.1 RFID

Radio frequency identification (RFID) tags have gained considerable attention and interest within industry and the media. This developing technology may lead to a large deployment of tiny, cheap, uniquely-identifiable devices with variable security capabilities.

Envisaged applications for RFID tags range from stock and inventory control to some futuristic applications. For instance RFID tags may be attached to food items enabling domestic devices to read storage or cooking instructions whilst others may be attached to clothes enabling washing machines to read cleaning instructions. The existing and upcoming applications can be found at industry websites such as [Web-Site 6]. Many of these applications can be of special interest for SMEs.

RFID technology will change the way manufacturers, distributors and retailers work together. The most obvious application for RFID tags is inventory control. Instead of tracking goods, it will be much cheaper and more effective to attach RFID tags to individual items and track them automatically using the tags. Indeed, the items can be monitored the whole way from the factory to the store. Prepared food can be labelled at each step of the preparation process, giving the consumer more information about the products they buy. RFID technology will also play an important role in identification of patients, systems, devices, products, etc., and the optimization and control of workflow in the care delivery chain. In the context of patients and the products and procedures applied to them, RFID might be essential for enhancing patient's safety, e.g. by providing the right blood transfusion to the right patient. Depending on technical capabilities, RFID tags might be used against counterfeiting and to provide assurance of the genuineness of pharmaceuticals or high value machine parts. RFID technology may be included in e-passports, and RFID tags may feature in the sensor networks that will envelope the cars of the future.

It is obvious that many businesses will be impacted in the near future by RFID deployment.

Contact-free communication for identification has been used for years in many countries for public transportation, access control mechanisms and other areas of application. The novelty relies in the cost of small devices that provide secure RFID functionality.

Three categories of tags can be identified:

- The passive tag is used only when powered by a nearby reader.
- The semi-passive tag uses internal power but is dormant until triggered into activity by a reader.
- The active tag is self-powered and interacts with the reader to communicate. (One major application is sensor networks where the tag should continually monitor its environment – such as for refrigerated transport – and issue warnings if some predefined threshold is reached)

Two competing emerging standards EPC/ONS (EPC global Forum) and Ubiquitious (Ubiquitious ID)) exist for passive RFID. ETSI also published a set of regulatory standards (EN 300 330 , EN 300 220 , EN 300 440, EN 300 674) specifying technical characteristics and test methods for radio equipment of short range devices. Moreover, EN 302 208 provides an additional frequency range from 865 to 868 MHz in which RFID readers can operate (they operated between 869.4 and 869.65 MHz before).

However, these standards are limited to passive RFIDs and do not include any specification about active tags. Therefore there is an urgent need for standardization for active tags. Protocols for the radio communication between passive tags and readers are defined in ISO 18000, ISO 10536, ISO 14443, ISO 15693, and ISO 10373-6.

12.1.1 Security Threats

The security threats related to RFID tag deployment are numerous and can not be addressed in detail in this report. However, they are on a general basis the same as for any communication system. Device authentication, denial of service and availability of resources, data authentication, communication confidentiality, database and record integrity and consumer privacy should be considered when deploying RFID tags.

The range and level of security threats will vary from application to application. Different applications may have very different security requirements. Some applications for instance may require security countermeasures to counter forgery whilst others may require security countermeasures against the invasion of privacy.

12.1.2 Security solutions for deploying RFID Tags

Where it is necessary to hold sensitive information on an RFID tag it will be necessary to protect that information. Generally this will entail the use of a cryptographic solution. Clearly this will impact both the cost and the performance of the RFID tag. Obviously the more powerful a tag is, the more expensive it will be. For the more expensive tags, no restrictions on the cryptography to be used have to be made. For the cheapest tags which are only capable of providing an identifying code on demand, it may not be possible to include cryptographic measures on the tag and other means of addressing the security requirements will be required. The challenging problems will occur for middle range tags. The price of the middle range tags will depend on the level of security provided by the cryptography.

Cryptographic algorithms are divided into two classes: symmetric and asymmetric algorithms. One significant difference between them is in the type of supporting infrastructure that they require as described elsewhere in this report. Another difference is that encryption based on symmetric algorithm usually requires less computational resources than asymmetric algorithms.

Many of the papers published in the area can be found at [Web-Site 6]. An optimized implementation of the AES has been proposed, but the current computational requirements of

the AES algorithm might be too high to be accommodated within standard RFID communication protocols. However the future availability of an optimized AES algorithm indicates that strong standardized cryptography is not impossible for relatively cheap RFID tags.

The alternative to a symmetric scheme is to use an asymmetric scheme such as RSA. Other standardized asymmetric schemes, such as elliptic curves based algorithms have the same drawbacks as RSA. On the other hand, some existing standardized asymmetric algorithms with different performance profiles may be considered as valid solutions. These public-key algorithms (for instance GPS algorithm specified in ISO/IEC 9798-5) may be suited to RFID deployment and may offer more efficient performances than standard symmetric cryptographic solutions.

Recommendation 19 As standardization has been limited to passive tags so far, there is an urgent need for standardization activities on active tags.

Suggested responsibility: CEN TC 225 and ETSI TC ERM

Priority: High

Deadline and Timeframe: This standardization activity should start immediately to allow the use of secure RFID products in the near future.

Recommendation 20 Privacy issues and traceability of the RFID tag users should be one of the main research issues for a successful RFID technology development.

Suggested responsibility: CEN TC 225 and ETSI TC ERM

Priority: High

Deadline and Timeframe: These issues should be integrated and taken into account in the standardization process as early as possible.

12.2 Next generation networks

In a traditional sense, communication networks could be divided into two different worlds:

- On one hand we have voice communications networks like PSTN/ISDN (Public Switched Telephone Network/Integrated Services Digital Network), GSM and UMTS where SS7 (Signalling System 7) rules as signalling and session establishment protocol. Traditionally these have always been closed systems in the sense that the general public, security specialists and in particular potential attackers know little of these systems. Consequently there is a degree on inherent security in communications networks based upon these protocols.
- On the other hand, we have the data communications world based on the Internet Protocol, with many popular applications, like e-mail or web browsing, which have entered our daily lives. Systems built on top of the IP protocol are generally regarded as more open systems. Consequently, these systems are more vulnerable to security attacks. Indeed, over the past, numerous security breaches have already been reported.

The increasing use of voice over IP (VoIP) applications, as an application running on top of IP, has introduced the same security concerns as those in the IP world. More important, the rise of VoIP applications triggers the convergence between the voice communication

networks and the data communication networks. The ETSI standardization body did recognize this convergence between voice and data communication and between fixed and mobile networks, and started initial standardization research in two working groups, TIPHON (Telecommunications and Internet Protocol Harmonization over Networks) and SPAN (Services and Protocols for Advanced Networking), which merged in September 2003 to become ETSI TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking).

While standardization activities in ETSI TISPAN are relatively new, ETSI TISPAN re-uses work done by other standardization bodies, like the work done by 3GPP (3rd Generation Partnership Project) on IMS (IP Multimedia Subsystem) for example. ETSI TISPAN co-ordinates the work between itself and the other standardization bodies and additionally monitors the convergence between fixed and mobile network infrastructure.

ETSI TISPAN is in the process of defining a Next Generation Networks (NGN) reference architecture, which describes a high level "co-operation" between access networks (such as xDSL, UMTS …) and service domains, such as IMS. Corresponding with this NGN reference architecture ETSI TISPAN also defines an NGN security architecture. The security services offered by the NGN security architecture are:

- Authentication;
- Authorization;
- Policy enforcement;
- Key management;
- Confidentiality; and
- Integrity protection.

In addition, TC TISPAN is producing a Security Design Guide, which should be followed in the design of any new component of the network. This work references the guidelines on the use of the Common Criteria for the evaluation of IT security (ISO/IEC 15408, see also Section 10.2). Further information is available from [Web-Site 33].

Recommendation 21 In order to improve the security in upcoming Next Generation Networks (NGN), standardization bodies like ETSI, 3GPP and others should continue their work in providing adequate standards that tackle the vulnerabilities in NGN and solving key problems like end-user authentication, authorization, policy enforcement, key management, confidentiality and integrity protection.

Suggested responsibility: ETSI and 3GPP

Priority: High

Deadline and Timeframe: Security solutions should already be installed in existing VoIP networks. As communication networks evolve, new security standards and practices should be applied as they become available from standardization bodies. This should be a continuing activity.

Recommendation 22 Network operators are very well placed to protect the traffic that flows through their networks. They are also very well placed to filter out all malicious communications, this to protect the end-users from this malicious communication. Therefore, it is recommended that network operators implement existing security standards and best practices in order to secure their NGN communication networks.

Suggested responsibility: ETSI and 3GPP

Priority: High

Deadline and Timeframe: Continuous activity.

13 References

The following references were consulted during the preparation of this report:

[1] COM(2006) 251 final, May 2006: Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*

[2] 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*.

[3] Council Resolution of 28 January 2002: *On a common approach and specific actions in the area of network and information security*.

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

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

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

[7] *Glossary of IT Security Terminology*, SD 6, SC27 N4996, issued by the International Organisation for Standardisation and Electrotechnical Commission (ISO/IEC).

[8] COM – D79, Study Group 17, *Security Architecture for Systems Providing End-to-End Communications*.

[9] ETSI Technical Report 336, *Telecommunications Management Network (TMN); Introduction to standardizing security for TMN*.

Further information was obtained from web sites of various organizations notably the European Telecommunications and Standards Institute (ETSI) and the European Standards Committee (CEN).

Annex 1 - Network Encryption

Securing the communication between two entities can be done at different layers in the protocols stack (either ISO protocol stack, or TCP/IP protocol stack), depending on the type of communication between the entities and on the type of application.

In general, if we want to secure all communication between two entities, providing security at the lowest layer end-to-end protocol would solve the problem. The industry standard network layer protocol for the Internet is the Internet Protocol (IP) standard. IP protocol is a connectionless end-to-end packet switching protocol providing for the fragmentation, routing and re-assembly of packets. Protection at the IP-layer is provided by the IPsec protocol. IPsec is further discussed in section 0.

For some applications, it is more convenient to provide security by a higher protocol layer. Most applications make use of TCP or UDP. TCP adds reliable communication, flow control, multiplexing and connection-oriented communication on top of IP. TCP is used to communicate between client and server in a client/sever environment and supports applications such as HTTP, electronic mail, file transport (FTP), and Web Services. The Transport Layer Security (TLS) protocol developed by IETF provides security on top of TCP. This is further discussed in section 0.

The introduction of Web Services, as a form of distributed computing, adds even more complexity to the security situation. The communication between Web Services happens via the Simple Object Access Protocol (SOAP). SOAP messages are (mainly) transported over HTTP. Using TLS to secure this SOAP message transport only results in a point-to-point (or hop-by-hop) security model. Today's Web Services applications rely on the ability for message processing intermediaries to forward messages. The inclusion of these intermediaries could endanger the end-to-end security (integrity, authentication …) of the messages. What is additionally needed in a comprehensive Web Service security architecture is a mechanism that provides end-to-end security. Web Service Security solutions will be able to leverage both transport and application layer security mechanisms to provide a comprehensive suite of security capabilities. Web Service Security is further discussed in section 0.

IPsec

IPsec is a security architecture developed by the IETF IPsec working group, which was disbanded in April 2005. The goal of IPsec is to secure the transmission of data across IP based networks. During the period 1998-2005 the core specifications have undergone serious rewriting this to provide a better description of the complete protocol suite. The previous version of the protocol set contained several cross-references and lack of clarity, which made the IPsec protocol suite difficult to understand, and even more difficult to implement; this also led to interoperability problems in IPsec implementations from different vendors.

IPsec may be used in Transport mode to encrypt the data part of the transmitted package (i.e. routing information is sent in clear (IP headers are visible), and only higher layer protocols like TCP, UDP, … are protected in this case) or in Tunnel mode where the inner IP packet is protected (encrypted and/or integrity protected) and encapsulated in an outer IP packet. In the former case, it is widely used as the mechanism for creating IPsec secured link between and end-user system and a security gateway (e.g. VPN connection from home to corporate domain). Tunnel mode is normally being used between two security gateways connection

providing a secure connection between different IP domains (e.g. to secure the communication between a head quarter office and branch offices).

"Orthogonal" to tunnel and transport mode, IPsec provides two security protocols, Authentication Header (AH) and Encapsulated Payload (ESP). AH is used to provide connectionless integrity and data origin authentication for IP packets and to provide protection against replays. AH provides authentication for as much of the IP header as possible, as well as for next level of protocol data. Parts of the IP header that can change in transit from sender to receiver cannot be protected by AH. ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service, and (limited) traffic flow confidentiality The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology. It is also allowed to use both ESP and AH to secure the IP communication between two systems.

The basic specifications of IPsec are:

- RFC4301, which provides an overview and describes the security architecture for the Internet Protocol.
- RFC4302, which described the Authentication Header security protocol.
- RFC4303, which described the Encapsulating Security Payload protocol.
- RFC4306, which described the Internet Key Exchange (IKEv2) protocol. This protocol performs mutual authentication between two parties and establishes an IKE security association (SA) that includes shared secret information that can be used to efficiently establish SAs for ESP and/or AH.

Apart form these base specifications, lots of other specifications are available, for example specification that describe how IPsec should be used in case NAT (Network Address Translation) boxes are also used.

Note that the current protocol standard for IP networks is IPv4. The successor to IPv4 is IPv6 which should "by definition" be compatible with IPsec.

The anticipation is that IPv6 will not require NATs, as the main objective of providing more address space is provided by IPv6. Any security provision of NATs can be supplied by other means.

TLS

Transport Layer Security Protocol (TLS) was developed by the Internet Engineering Task Force (IETF) to provide encrypted communications on the Internet on top of TCP. 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 TCP 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 (HTTP communication). TLS/SSL also allows sessions that are not encrypted but are authenticated and proof against tampering.

Within TLS, different modes of operation are possible. Server authentication is always performed, based on the server certificate. If afterwards, the server wants to authenticate the client, other authentication mechanisms can be used. This client authentication will be

secured by the encrypted TLS connection. Also, during TLS negotiation, mutual authentication between client and server is also possible, but this requires client certificates.

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 IETF RFC 4346.

Security in the Web Service World

Electronic commerce (e-business) is mostly based on Web Services. Web Services use (among others) the concept of distributed computing. The communication between the different Web Services happens via the Simple Object Access Protocol (SOAP). SOAP is a lightweight, XML-based protocol that allows the exchange of information among entities in a distributed web-service environment.

Providing security for the basic Web Service communication comes down to securing the SOAP messages. The purpose of the "Web Services Security: SOAP Message security" specification is to add security features to SOAP messaging. In particular, these features are:

- Sending a security token as part of a SOAP-message
- Providing authentication and message integrity
- Providing message confidentiality

According to the Web Services architecture and terminology, a security token is a collection of claims. Claims are statements about subjects, which could be the subject's identity, keys, privileges, capabilities or other things. The provider of a Web Service requires from the service requester to prove a set of claims, otherwise the service will not be granted. Therefore, sets of claims, i.e. security tokens, have to be conveyed within SOAP messages as an essential part of Web Services related communication. Examples of security tokens are simple usernames, X.509 certificates, Kerberos tickets.

In order to provide the security features mentioned above, authentication, integrity protection and confidentiality, the "Web Services Security: SOAP Message Security" specification reuses XML signature and XML encryption mechanisms. While the XML signature and encryption specifications are targeted at XML in general, the "Web Services Security: SOAP Message Security specification" indicates, how XML signatures and encrypted data is to be included in a SOAP envelope and how it should be processed by the entities involved.

The following specifications make up the WS-Security OASIS standard:

- WS-Security Core Specification
- Username Token Profile
- X.509 Token Profile
- SAML Token Profile
- Kerberos Token Profile
- Rights Expression Language (REL) Token Profile
- SOAP with Attachments (SWA) Profile

Apart from this basic security specification, there are many other Web Services specifications either from OASIS or W3C in the security area in general. Below, we will just mention a few others.

- XML Signature (Specification by W3C): The XML Signature specification specifies XML Syntax and processing rules for creating and representing digital signatures in XML documents. XML Signatures can be applied to any digital content, including XML. More specifically, the specification defines an XML signature element type and an XML signature application. XML Signature is a method of associating a key with referenced data; it does not specify how keys are associated with persons or institutions, nor the meaning of the data being referenced and signed. This must be done by a particular application that uses this specification.
- XML Encryption (Specification by W3C): The XML Encryption specification specifies a process for encrypting data and representing the result in XML. The data may be arbitrary data (including an XML document), an XML element, or XML element content. The result of encrypting data is an XML Encryption EncryptedData element which contains (via one of its children's content) or identifies (via an URI reference) the cipher data.
- Web Services Policy (Specifications by W3C): The Web Services Policy Framework and the Web Services Policy Attachment specifications are being specified by the Web Services Policy Working Group of W3C.

  Web Services Policy is a machine-readable language for representing the capabilities and requirements of a Web Service. In other words, a Web Service Policy of a particular Web Service Provider describes how a service requester must securely interact with this Web Service Provider. The Policy describes whether and how a message must be secured, whether and how a message must be delivered reliably, whether a message must flow a transaction, etc.

  The Web Services Policy Framework provides a general purpose model and corresponding syntax to describe the policies of entities in a Web Services-based system. The Framework defines a base set of constructs that can be used and extended by other Web services specifications to describe a broad range of service requirements and capabilities. In this, a policy is a collection of policy alternatives, where a policy alternative is a collection of policy assertions; and a policy assertion represents an individual requirement, capability or other property of a behaviour.

  The Web Services Policy Attachment specification defines two general-purpose mechanisms for associating policies, as defined in Web Services Policy Framework, with the subjects to which they apply. The policies may be defined as part of existing metadata about the subject or the policies may be defined independently and associated through an external binding to the subject. This specification describes the use of these general-purpose mechanisms with WSDL (Web Service Description Language) definitions and UDDI (Universal Description Discovery and Integration).
- SAML (Specification by OASIS): The OASIS Security Assertion Markup Language (SAML) standard defines an XML-based framework for describing and exchanging security information between on-line business partners. This security information is expressed in the form of portable SAML assertions that applications working across security domain boundaries can trust. The SAML standard defines the precise syntax and processing semantics of assertions made about a subject by a system entity. The specification defines both the structure of SAML assertions, and an associated set of protocols, in addition to the processing rules involved in managing a SAML system.

It is important to note that the Web Services area is still a much researched area and therefore it can be expected that in the future many other security related Web Services specification might emerge.

Annex 2A - Overview of Information for Small and Medium Enterprises regarding Network and Information Security

Small and Medium Enterprises (SMEs, here considered to be organizations with typically less than 250 employees) have specific requirements for network and information security. 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.

The following is a summary of publicly available information and guidance for SMEs on the issue of Network and Information Security:

The SME trade bodies UEAPME [Web-Site 21] and NORMAPME [Web-Site 22] focus on typical SMEs issues and can provide further information about network and information security. The UEAPME Web site gives some information on its working group related to the security of the food chain, and the NORMAPME Web site provides information related to security standards on security management, network security and application security.

ENISA [Web-Site 23] has published a diversity of documents providing advice on different topics related to network and information security, such as information security basics, help to select security products, several issues related to network security, awareness and business continuity. This Web site gives some information and links on PC security, network security, security for operating systems, application security, security management, and safety.

The ISA-EUNET presents an integrated approach comprising security technology awareness, support, education, training, and dissemination aiming towards the diffusion of security and safety know-how to SMEs. More about this can be found by going to [Web-Site 24], as well as information regarding PC security, security for operating system, security management, and safety.

Another example is the publicly available CD from the DTI, which discusses the important topic of information security management especially for SMEs. More information is available under [Web-Site 25]. This gives a lot of useful information on PC security, network security, security for field and teleworkers, security for operating systems, application security, security management, and safety.

In addition, there are plenty more guidelines and information available from the DTI site that help to protect SME organizations, e.g. on [Web-Site 26] or on a simple search for key words such as “information security”. This Web site gives best practice measures addressing a lot of different issues, including PC security, network security, security of operating systems, application security, and information security management.

The Hong Kong government runs a regularly updated Website on Information Security & Prevention of Computer-Related Crime, which contains a SME Corner with useful information [Web-Site 27] addressing issues related to PC security, network security, security of operating systems, application security, and information security management.

There is also information available from the US, e.g. a report from the Fraud Advisory Panel providing information for SMEs about Cybercrime [Web-Site 28]; this Web site concentrates on providing information on fraud and does not address other NIS- security related issues.

A lot of information is available on the SANS Website [Web-Site 29]. This Web site maintains a large collection of research documents about various aspects of information

security, including PC security, network security, security for field and teleworkers, security for operating systems, application security, security management and safety. Within the SANS Web site, there is also SME specific information, such as a paper on how to build a secure email system, [Web-Site 30].

There are also a lot of helpful network and information security related downloads that can be found on [Web-Site 31], addressing different issues relating to PC security, network security, security of operating systems, application security, and information security management.

There are also plenty of products that help SMEs to manage network and information security, including programmes protecting against malicious software and spam, unauthorized intrusion and other typical Internet threats. Suitable products should be selected taking account of the specific security requirements of the SME.

Similar information is provided for SME users who seek information in other languages than English (see Annex 2B (German), Annex 2C (French), Annex 2D (Spanish) and Annex 2E (Italian).

Annex 2B - Überblick über Informationen über Netz- und Informationssicherheit für kleine und mittlere Unternehmen

Kleine und mittlere Unternehmen (KMUs, hier bezeichnet dies Unternehmen mit typischerweise weniger als 250 Mitarbeitern) stellen besondere Anforderungen an Netz- und Informationssicherheit. In vielen Fällen kann ein KMU nicht ausreichend mit Fragen der Computersicherheit vertraut sein, und daher von der Bereitstellung von Material zur Bewusstseinsbildung, Schulung und Anleitung profitieren.

Das Folgende ist eine Zusammenfassung von öffentlich zugänglichen Informationen und Anleitungen für KMUs für Fragen der Netz- und Informationssicherheit.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet auf seiner Web-Seite [Web-Seite German 1] einen Überblick über mehrere Themen, die Netz- und Informationssicherheit unterstützen. Dazu gehört der IT-Grundschutz, der für bestimmte vorgegeben IT-Konfigurationen nach dem Baukastenprinzip Maßnahmen zur Verfügung stellt. Eine komplette Umsetzung des IT-Grundschutzes kann für kleine und mittlere Unternehmen sehr aufwendig werden, eine für KMUs geeignete Zusammenfassung bietet der Leitfaden IT-Sicherheit [Web-Seite German 1a]. Der IT-Grundschutz behandelt Themen aus der PC Sicherheit, Netzsicherheit, Sicherheit für Betriebssysteme, Sicherheit von Anwendungen und Sicherheitsmanagement.

Die Initiative secure-it.nrw des Landes Nordrhein-Westfalen wurde im Jahr 2001 gestartet, um Fragen der Sicherheit in der Informationstechnologie zu adressieren. Auf [Web-Seite German 2] finden Sie Informationen zu aktuellen Stichwörtern, Informationen über Best Practices, Tipps und Trends. Diese Informationen behandeln Themen aus der PC Sicherheit, Netzsicherheit, Sicherheit für Betriebssysteme, Sicherheit von Anwendungen und Sicherheitsmanagement.

Die Nationale Initiative für Internet-Sicherheit (NIFIS e.V.) ist eine Selbsthilfeorganisation der Wirtschaft, um Unternehmen im Kampf gegen die wachsenden Gefahren aus dem Internet technisch, organisatorisch und rechtlich zu stärken. Eine Initiative von NIFIS ist das NIFIS-Siegel [Web-Seite German 3], dass auf der Basis der Standards ISO/IEC 27001 und ISO/IEC 27002 Gelegenheit zum Selbstaudit gibt. Das NIFIS-Siegel adressiert PC Sicherheit,

Netzsicherheit, Sicherheit für Betriebssysteme, Sicherheit von Anwendungen und Sicherheitsmanagement.

Das Netzwerk für den elektronischen Zahlungsverkehr bietet unter dem Schwerpunkt Netz- und Informationssicherheit auf der [Web-Seite German 4] verschiedenste Richtlinien, Leitlinien und Informationen, die viele verschiene Sicherheitsfragen ansprechen, einschließlich PC Sicherheit, Netzsicherheit, Sicherheit für Betriebssysteme, Sicherheit von Anwendungen und Sicherheitsmanagement.

Aus der Schweiz gibt es eine KMU-Schriftenreihe, in der es auf der [Web-Seite German 5] ein 10-Punkte-Programm zum Erreichen von mehr Sicherheit bei kleinen und mittleren Unternehmen gibt. Dieses Programm beschreibt einfache Punkte, die kleine und mittlere Unternehmen umsetzen können, um mehr Sicherheit zu erreichen. Die Punkte helfen, die PC Sicherheit, Netzsicherheit, Sicherheit für Betriebssysteme, Sicherheit von Anwendungen und das Sicherheitsmanagement zu verbessern.

Auf [Web-Seite German 6] bietet Microsoft einen Sicherheitsleitfaden für kleine und mittlere Unternehmen vor. Außerdem bietet die Seite die Möglichkeit eines Sicherheitschecks und eine Checkliste für PC-Sicherheit an. Außerdem berührt die Seite Themen wie Netzsicherheit, Sicherheit für Betriebssysteme und Sicherheit von Anwendungen.

Außerdem gibt es viele Produkte und Beratungsdienstleitungen, die KMUs helfen, Netz- und Informationssicherheit zu handhaben, einschließlich Programmen, die gegen Schadenssoftware und Spam, unberechtigtes Eindringen oder andere typische Internetbedrohungen schützen. Geeignete Produkte sollten auf Basis der spezifischen Sicherheitsanforderungen des KMU ausgewählt werden.

Web-Seiten:

[Web-Seite German 1] = http://www.bsi.de/

[Web-Seite German 1a] = http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf

[Web-Seite German 2] = http://www.secure-it.nrw.de/infodienst/inhalt.php

[Web-Seite German 3] = http://www.nifis.de/joomla/index.php?option=com_content&task=view&id=132&Itemid=160

[Web-Seite German 4] = http://www.ec-net.de/EC-Net/Navigation/netz-informationssicherheit.html

[Web-Seite German 5] = http://www.infosurance.ch/de/pdf/InfoSurance_Broschuere_10_Punkte_Design.pdf

[Web-Seite German 6] = http://www.microsoft.com/austria/kmu/businessthemen/it-sicherheit/sicherheit/default.mspx

Annex 2C –Informations relatives à la sécurité des réseaux et de l'information pour les Petites et Moyennes Entreprises (PME)

Les liens ci dessous conduisent à des sites de langue Française qui fournissent des informations pertinentes sur la sécurité de l'information pour les PME :

http://www.clusif.asso.fr/ donne des informations concernant la sécurité de l'ordinateur, des réseaux, des systèmes d'exploitation, des applications mais aussi concernant le management de la sécurité des systèmes d'information pour toutes les entreprises Françaises et plus particulièrement pour les PME.

http://doc-standarmedia.afnor.fr/etudes/FicheIso27000_3_814037502.pdf traite de la normalisation des activités pour les PME.

http://www.cases.public.lu/publications/recherche/r2sic/ fournit des informations pour toutes les sociétés Luxembourgeoises, et plus particulièrement les PME, sur la sécurité de l'ordinateur, des réseaux, des systèmes d'exploitation, des applications, du management de la sécurité des systèmes d'information.

http://clusis.ch/activities/PME.htm fournit des informations pour toutes les entreprises Suisses, et plus particulièrement les PME, sur la sécurité de l'ordinateur, des réseaux, des systèmes d'exploitation, des applications et sur le management de la sécurité des systèmes d'information.

http://www.oecd.org/dataoecd/26/12/38045683.pdf donne des informations et des recommandations quant à la sécurité des réseaux, la sécurité des applications mais aussi quant au management de la sécurité des systèmes d'information.

http://www.upaq.com/pdf/P39211_InfoSurance_f_mc.pdf fournit aux PME des directives sur la sécurité de l'ordinateur, des réseaux, des systèmes d'exploitation, des applications et du management de la sécurité des systèmes d'information.

http://www.citi.tudor.lu/cms/citi/publishingfr.nsf/id/WEBR-6XR22R donne des informations concernant la sécurité de l'ordinateur, des réseaux, des systèmes d'exploitation et du management de la sécurité des systèmes d'information.

https://www.isiq.ca/fr/Guides/PME fournit aux PME Canadiennes des directives sur la sécurité de l'ordinateur, des réseaux, des systèmes d'exploitation et du management de la sécurité des systèmes d'information.

Annex 2D – Informaciones para las pequeñas y medianas empresas (PYME) sobre la seguridad de las redes y de la información

Los siguientes enlaces a páginas Web en español proporcionan una serie de informaciones útiles para las PYME en relación a la seguridad de la información.

http://www.seguridadpymes.es/ proporciona información a todas las empresas españolas, pero especialmente a las PYME, sobre la seguridad y protección de ordenadores, redes, sistemas operativos y aplicaciones así como la gestión de la seguridad.

http://www.segu-info.com.ar/boletin/boletin_060226.htm proporciona información a las empresas y en particular a las PYME sobre la seguridad y protección de ordenadores, redes, sistemas operativos y aplicaciones así como la gestión de la seguridad.

http://timur.es/timur/noticia.jsp?id=1332&idcategoria=708 da a las PYME españolas pautas y directrices sobre la seguridad de ordenadores, redes, sistemas operativos y la gestión de la protección y seguridad.

http://www.inteco.es/frontinteco/es/frontIntecoAction.do?action=viewCategory&categoryNAME=C.+Respuesta+Pyme&id=6773 proporciona directrices para las PYME españolas en relación a la seguridad de ordenadores, redes, sistemas operativos y la gestión de la seguridad.

http://pcpymes.es/Actualidad/An%A1lisis/Infraestructuras/Soluciones/20050616029 proporciona información y noticias sobre la seguridad de ordenadores, redes, sistemas operativos, aplicaciones y la gestión de la protección y seguridad.

http://www.datapyme.com/ proporciona información sobre la seguridad de ordenadores, redes, sistemas operativos y aplicaciones.

Annex 2E - Informazioni disponibili per le PMI (piccole e medie imprese) sulla sicurezza informatica e di rete

In questa pagina potete trovare una lista di links a siti Internet in lingua italiana che contengono utili informazioni per le PMI sulla sicurezza informatica e di rete.

Il sito http://www.clusit.it/ contiene diverso materiale di riferimento relativo alla sicurezza informatica. Clusit, l'associazione italiana per la sicurezza informatica, ha come missione principale la promozione della cultura per la sicurezza informatica nelle aziende, amministrazioni pubbliche e presso i privati. Da questo sito sono scaribili delle pubblicazioni interessanti, ma che non si rivolgono esclusivamente a PMI.

Un altro sito Internet di interesse da dove iniziare la ricerca è http:///www.sicurinfo.i/

In questo sito, nella sezione « Soluzioni per PMI », potrete trovare i percorsi informativi lageti a problematiche specifiche, come controllo accessi, antivirus, network security, etc…..

Sul sito di Securinfo sono disponibili delle linee guida sulla gestione della sicurezza (informatica) (indirizzo: http://www.sicurinfo.it/materiale/guida_firenzetecnologia.pdf)

Molte informazioni su questo argomento sono disponibili anche sul sito dell'OECD, dove si puo' scaricare il documento « Linee guida dell'OECD sulla sicuerezza dei sistemi e delle reti d'informazione – verso una cultura della sicurezza » (versione in pdf a http://www.oecd.org/document/42/0,2340,en_21571361_36139259_15582250_1_1_1_1,00.html)

Per terminare, moltissime informazioni sulla sicurezza informatica sono fornite dalla Microsoft sul suo sito http://www.microsoft.com/italy/pa/approfondimenti/sicurezza.mspx.

Informazioni specifiche per le PMI sono disponibili all'indirizzo : http://www.microsoft.com/italy/pmi/sicurezza/default.mspx

Annex 3 – Security-Related Projects within the EU

Within the European Union, there is the FP6-IST Programme R&D Projects in the Strategic Objective "Towards a global dependability and security framework". In FP6 and the previous framework programs, numerous security projects have been supported by the European Commission since ICT security is one of the key objective of the European Union.

Under FP6, 4 types of research projects have been considered:

- Integrated Projects with ambitious objective driven research and a critical mass of players
- Networks of Excellence : to integrate long term European expertise & research resources
- Specific Targeted Research Projects : Research or demonstration projects to support research activities of more limited scope & ambition than Integrated Projects
- Support Actions

The list of research projects related to security and their summaries can be found at [Web-Site 43].

Moreover, The European Community eTEN programme (formerly TEN-Telecom) supports consortia consisting of public and private organizations, enabling them to make e-services available across the European Union. It focuses particularly on the critical validation and launch phases of a service, when assumptions about the operating costs and the potential revenues, savings and public benefits are put to test.

Currently the main focuses of eTEN are applications and generic services in the areas of eGovernment, eInclusion, eLearning, and Trust and Confidence. The topic of healthcare has not been considered in this annex. The list of security related projects in this programme is given below:

CERTIVER

Certification Revocation and Validation Service
eTen - 2000-2.
Theme: Trust and Security services.
Start: Nov 2002 - End: Apr 2004.

The project implements the market validation for the deployment of a certification revocation service, with its corresponding On-Line Certificate Status Protocol (OCSP) publication, as outsource to any interested Certificate authority, mainly in Europe. Some benefits are expected: reduction in the delay in delivering the revocation information, greater security and reduction of costs (economy scales).

COSEAG

Consumer Protection Seal : Assurance and Money-back-guarantee
eTen - 2000-1.
Theme: Trust and Security services.
Start: Jan 2001 - End: Dec 2001.

The COSEAG Project aims to improve confidence and security in e-commerce in Europe for both online consumers and online merchants. The Trusted Shops scheme provides consumers and online merchants with a bundle of services including certification, dispute resolution and a money back guarantee backed by insurance.

E-Poll

Electronic Polling System for Remote operation
eTen - 2003-1.
Theme: n/a.

E-POLL introduces in the e-democracy area high level services based on a seamless VPN network (wired and mobile architecture), providing high security and privacy guarantees, or on the Internet for lower security services. An extensive piloting in two countries consolidates developed technologies (FP5 - IST) and addresses interoperability and multilanguage issues.

E-TEN

European Tendering Exchange Network
eTen - 2000-1.
Theme: Trust and Security services.
Start: Jan 2001 - End: Jul 2002.

E-TEN aims to provide a Europe-wide electronic tendering system for Public Works and Public Services contracts. The system incorporates end-to-end transmission of specifications and drawings from Client to Main Contractors, sub-contractors and suppliers and operates similarly for tender submissions.

EBR-TIC SERVICE

European Business Register Trrust and Internet Confidence Service
eTen - 2000-2.
Theme: Trust and Security services.
Start: Nov 2001 - End: Oct 2003.

EBR-TIC aims to make official company information easily accessible directly from the company's website, allowed to display an "EBR trustmark". By clicking on the trustmark the user will get the basic set of data indicated on the EC Directive on electronic commerce. Sources of information are the Public Business Registers established in each EU Member State.

EMERITUS

An E-Business Model for the Effective Realisation of a TrUst Services Infrastructure
eTen - 1998-2.
Theme: Trust and Security services.
Start: Jan 1999 - End: Sep 2000.

Feasibility stage to accelerate the establishment of an European integrated trusted services infrastructure, to respond to the needs of commercial competitive services for public and business entities and citizens. This will be achieved through a consortium of non-profit industry associations creating a Global Trust Services Union prototype. Business development strategy, long-term financing, policy framework, operational procedures, legal instruments and agreements will be developed.

ESW

European Social Web
eTen - 1999-1.
Theme: Trust and Security services.
Start: Jan 2000 - End: Jul 2001.

ESW encourages the safe use of Internet for Business to Business applications by providing: generic **security** services that enable recursive authentication of individuals within their organisation;notary services that enable creation and management of communities of interest and secure transactions, such as the signing of contracts between community members ; social services, which are all kinds of applications that require authentication of their users.

EURO-LOGO

Euro - Logo
eTen - 2000-1.
Theme: Trust and Security services.
Start: Mar 2001 - End: Aug 2002.
An Internet label to create trust and stimulate growth in the European e-commerce market, launched by EuroCommerce (the retail, wholesale and international trade representation to the EU). Through an Internet-based generic services network, Euro-Logo will develop, support and monitor a Trustmark system based on the EuroCommerce Code of Conduct.

EUROWEX **University Administration Services by using DIGITAL SIGNATURE**
eTen - 2005-1.
Theme: n/a.
Start: Jun 2006 - End: Nov 2007.
EUROWEX provides an Internet based service to university professors which helps them to keep track of the performance of their students throughout the academic year. All data is entered with the use of a digital signature and therefore its correctness is entirely the responsibility of the professor. The advantages of this service over the current paper based system are improved **security** of the information, ease of management and access, and saving of office space.

ONLINE CONFIDENCE

An On-Line Dispute Resolution Service that will give Buyers and Sellers Access to an out of Court Process which will be Effective, Transparent, Independent and Fair
eTen - 2000-1.
Theme: Trust and Security services.
Start: Jan 2001 - End: Oct 2002.
The project partners will establish an innovative on-line dispute resolution service that will give buyers (both businesses and consumers) access to an out-of-court process which will be effective, transparent, independent, fair, low cost and which respects the legal rights of all concerned.

paysafecard

paysafecard - Europe's first prepaid card for micropayments over the internet for provider independent use
eTen - 2005-1.
Theme: n/a.
Start: Jan 2006 - End: Dec 2009.
Paysafecard, a highly successful online payment system in Austria and Germany, stands out for its ease of use and fraud-free **security** features. Paysafecard enables online purchasing without the need to divulge any personal data, whilst using a prepaid PIN code to validate transactions. Now this payment service shall be implemented throughout Europe.

RISER

Registry Information Service on European Residents
eTen - 2003-1.
Theme: eGovernment.
Start: Mar 2004 - End: Aug 2005.
RISER is a Trans-European eGovernment service offering the verification of address information trough access on official registries to companies and citizens. Hence, one of the most frequented services of public administration becomes a seamless value-added cross-border service. RISER conforms to highest data **security** requirements and uses open standards.

SELIS

Secure Electronic Invoicing Service
eTen - 2004-1.
Theme: n/a.

SELIS, is a cross-border service for the secure exchange of eInvoices based on an innovative architecture that adopts the most advanced standards for the secure provision of interoperable services. SELIS enables integration with accounting software currently in place or can be used as a stand-alone solution that suits smaller users. The trial users will be six or more SMEs, members of the participating Chambers, and will be the ones that provide measurable evidence of the benefits gained by the adoption of the service.

SEMOPS II.
http://ec.europa.eu/information_society/activities/eten/cf/opdb/cf/project/index.cfm?mode=detail&project_ref=ETEN-029376

Secure Mobile Payment Service International Introduction
eTen - 2005-1.
Theme: n/a.

The Secure Mobile Payment Service International Introduction (SEMOPS II.) Market Validation project has the objective to introduce the SEMOPS real time electronic payment service with 6 payment processors in four countries and to evaluate the service both as local operations and as an international payment network. Various payment transaction types will be introduced, mobile and internet ones, both on local and international level. The project workplan includes market research, financial and business modeling and the preparation of the necessary legal framework for the operation.

SPES

Setting Processes for Electronic Signature in European Cities
eTen - 2001-2.
Theme: Trust and Security services.
Start: Nov 2002 - End: Oct 2004.
SPES will promote the adoption and full exploitation of the digital signature by Public Administrations, whilst implementing real applications and best practices. These are aimed at a large number of end users of the services which are provided by the Municipalities and are at a trans-European level.

List of Abbreviations

The following abbreviations are used in this report:

3G	Third Generation (of mobile devices)
3GPP	3rd Generation Partnership Project
ACL	Access Control List
AES	Advanced Encryption Standard
ARMA	Association for Information Management
CASCO	ISO Committee on Conformity Assessment
CC	Common Criteria
CD	Committee Draft
CEN	European Committee for Standardization
CEN/ISSS	CEN Information Society Standardization System
CERT	Computer Emergency Response Team
CNI	Critical National Infrastructure
COM	Communication from the EU Commission
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
CWA	CEN Workshop Agreement
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DICOM	Digital Imaging and Communications in Medicine
DoS	Denial of Service
DRM	Digital Rights Management
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DTI	Department of Trade and Industries, UK
EC	European Commission
ECRYPT	European Network of Excellence for Cryptology
EEHIC	European Electronic Health Insurance Card
EESSI	European Electronic Signature Standardization Initiative
EHR	Electronic Health Record
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications and Standards Institute
ETSI LI	ETSI group for Lawful Interception
ETSI SAGE	ETSI Security Algorithms Expert Group
FAR	False Acceptance Rate
FRR	False Rejection Rate
FTP	File Transfer Protocol
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
IAF	International Accreditation Forum
ICT	Information and Communications Technology
ICTSB	Information and. Communications Technologies Standards Board
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IP	Internet Protocol

IPSEC	Internet Protocol Security
ISCI	International Security Certification Initiative
ISDN	Integrated Services Digital Network
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO CASCO	ISO Committee on Conformity Assessment
ISA-EUNET	Intensive Software Systems for Safety Applications; a high-tech software European lean network
ISP	Internet Service Provider
IT	Information Technology
ITU	International telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JRC	Joint Research Centre
JTC	Joint Technical Committee
LAN	Local Area Network
LTRANS	Long-Term Archive and Notary Services
MIME	Multipurpose Internet Mail Extensions
NAT	Network Address Translation
NGN	Next Generation Networks
NIS	Network and Information Security
NISCC	National Infrastructure Security Co-ordination Centre
NISSG	Network and Information Security Steering Group
NIST	National Institute of Standards and Technology
NORMAPME	European Office of Crafts, Trades and Small and Medium- Sized Enterprises for Standardization
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
PP	Protection Profile
PSTN	Public Switched Telephone Network
RBAC	Role Based Access Control
RC2	cryptographic algorithm by Ronald Rivest
RFC	Request For Comments
RFID	Radio Frequency Identification
RSA	cryptographic algorithm by Rivest, Shamir und Adleman
S/MIME	Secure MIME
SAML	Security Assertion Markup Language
SC	Sub-Committee
SCADA	Supervisory Control and Data Acquisition Systems
SDO	Standards Developing Organisation
SLA	Service Level Agreement
SME	Small and Medium Enterprise
SMLDSIG	*Still needs to be added*
SOAP	Simple Object Access Protocol
SPAN	Sevices and Protocols for Advanced Networking
SRP	Secure Remote Password
SS7	Signalling System 7
SSE-CMM	Capability Maturity Model for System Security Engineering

SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TETRA	TErrestrial Trunked RAdio
TIPHON	Telecommunications and Internet Protocol Harmonization over Networks
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
TOE	Target of Evaluation
TR	Technical Report
TS	Telecom Standard
TSP	Trusted Service Provider
UDP	User Datagram Protocol
UEAPME	European Association of Craft, Small and Medium-sized Enterprises
UMTS	Universal Mobile Telecommunications System
UPS	Un-interruptible Power Supplies
VoIP	Voice over IP
VPN	Virtual Private Network
WD	Working Draft
WG	Working Group
XACML	eXtensible Access Control Markup Language
xDSL	all Digital Subscriber Line techniques
XML	Extensible Markup Language

List of Web Sites

The following Web sites are quoted in this report:

[Web-Site 1] This Web site still needs to be established, the URL will be added once it is in place.
[Web-Site 2] http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/activity/drm_fg.asp
[Web-Site 3] http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/activity/wsdpp.asp
[Web-Site 4] http://www.gliif.org/standards.htm
[Web-Site 5] http://www.eu2006.at/en/News/Council_Conclusions/JAISchlussfolgerungen.pdf
[Web-Site 6] http://www.rfidjournal.com/
http://www.rfidjournal.com/
[Web-Site 7] http://www.mobihealth.org
[Web-Site 8] http://www.projectliberty.org/
[Web-Site 9] http://www.w3.org/P3P/
[Web-Site 10] http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf
[Web-Site 11] http:// www.ict.etsi.org/eessi/EESSI-homepage.htm
[Web-Site 12] http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/electronic_signatures.asp
[Web-Site 13] http://portal.etsi.org/li
[Web-Site 14] http://www.niscc.gov.uk/niscc/index-en.html
[Web-Site 15] http://www.anec.org/anec.asp?rd=30194&ref=01-01.03-01&lang=en
[Web-Site 16] http://www.ecsirt.net
[Web-Site 17] http://www.iso27001certificates.com
[Web-Site 18] http://www.iso.ch/iso/en
[Web-Site 19] http://www.iaf.nu/
[Web-Site 20] http://www.ecrypt.eu.org/estream
[Web-Site 21] http://www.ueapme.com
[Web-Site 22] http://www.normapme.com/
[Web-Site 23] http://www.enisa.europa.eu/
[Web-Site 24] http://www.dmst.aueb.gr/dds/pubs/conf/1999-WISE-TEKNO/html/wise.html
[Web-Site 25] http://www.ecdti.co.uk/CGIBIN/PRIAMLNK.CGI?CNO=1&MP=PNO%5EGINT64&SEARCH=02/CD18
[Web-Site 26] http://www.dti.gov.uk/files/file9972.pdf#search=%22information%20security%20SME%22
[Web-Site 27] http://www.infosec.gov.hk/engtext/sme/sme_corner.htm
[Web-Site 28] http://www.fraudadvisorypanel.org/cheker/cheker.php?idmk=5
[Web-Site 29] http://www.sans.org
[Web-Site 30] http://www.sans.org/reading_room/whitepapers/email/1218.php
[Web-Site 31] http://www.dti.gov.uk/sectors/infosec/infosecdownloads/downloads2nd/page29142.html
[Web-Site 32] http://portal.etsi.org/fixed/Security/ElectronicSignature.asp
[Web-Site 33] http://www.tispan.org
[Web-Site 34] http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm
[Web-Site 35] http://www.anec.org/anec.asp?rd=30194&ref=01-01.03-01&lang=en
[Web-Site 36] http://www.arma.org
[Web-Site 37] http://csrc.nist.gov/rbac/

[Web-Site 38] http://www.itl.nist.gov/fipspubs/fip186.htm
[Web-Site 39] http://www.mozilla.org/projects/security/pki/nss/fips1861.pdf
[Web-Site 40] http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
[Web-Site 41] http://www.etsi.org
[Web-Site 42] http://www.3gpp.org
[Web-Site 43] ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/projects-leaflet-call4-sept-2006_en.pdf