# *CEN Network and Information Security Report*

## *in support of the Communication form 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 – "Dialog, partnership and empowerment"*

*Issue 1.2, 23 June 2006*

# 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.<br>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.<br>All changes have been marked for easy identification. |

# Executive Summary

This report is a draft proposed for issue by CEN and ETSI in response to the European Commission's call for *"a comprehensive strategy on security of electronic networks including practical implementing action."* The report deals with issues which are relevant to the European Standards Organizations (ESOs). It recommends actions on both the ESOs and on industry standards bodies that when undertaken will improve the availability of secure electronic communication, including e-commerce and the exchange of information within a European environment and beyond.

CEN and ETSI share the aims set forward in the Communication from the Commission COM(2006) 251. It is agreed that there are comprehensive standards available for secure electronic networks. However, the report notes that there are few security frameworks to guarantee multi-vendor systems will operate securely together. Also it is noted that there is a lack of appropriate certification in some areas. The result is fragmentation and uneven implementation in real networks and insecurities remain despite some parts being very secure.

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

- **Interoperability**: There are many security standards available. This often leads to problems of interoperability – with potentially annoying consequences for the consumer and perhaps business consequences for the provider of electronic services. A number of mechanisms exist to improve this situation including the use of standards frameworks which can help to identify and incorporate interoperable standards in such a way that users become unaware of interoperability issues. Also interoperability testing can help to ensure equipment conforming to standards and frameworks does really interoperate. The report's recommendations encourage interoperability testing and the incorporation of "overlapping" standards within suitable frameworks which unify as far as possible the different technical means of doing certain tasks. Interoperability and security are both important, and as these might conflict, the respective requirements should be balanced to ensure that both are appropriately addressed.
- **Upgradeability**: Security is not a static problem: the implementation of a standard in a product may need to be updated as weaknesses are discovered; and new standards will be needed whenever existing ones become ineffective in countering threats to security. Several of the report's recommendations are aimed at ensuring this need is recognized and dealt with in a manner that is as simple as possible for the end user, through the use of frameworks that can handle updates in a transparent manner.
- **Home users and Small and Medium Enterprises**: In the near future it is very clear that many home users and many Small and Medium Enterprises will be making new, permanent connections to the Internet for the purposes of e-commerce, information and entertainment. These users will naturally have neither the expertise nor the inclination to apply obscure security measures to consistently prevent security breaches. The report makes recommendations to deal with this issue before it becomes a major problem.

Finally, it is hoped that the awareness of these issues generated within the European Standards Organizations will encourage the development of high quality security standards and frameworks in close cooperation with other Standards Development Organizations

(whether recognized or not). This will be to the benefit of end users and will help to ensure the development of a more secure environment for electronic communication.

# 1 Introduction

This report is issued by CEN and ETSI in response to:

COM(2006) 251 Communication from The Commission to The Council, The Eureopean Parliament, The Eureopean 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 2001 Communication defines NIS as “*the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems*”. Over recent years, the European Community has implemented a number of actions to improve 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.

[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.

*[**Editors Note**: further text will be added to this introduction based on COM(2006) 251 (this is attached to this documents for reference).]*

# 2 Network and Information Security

## *2.1 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:

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]

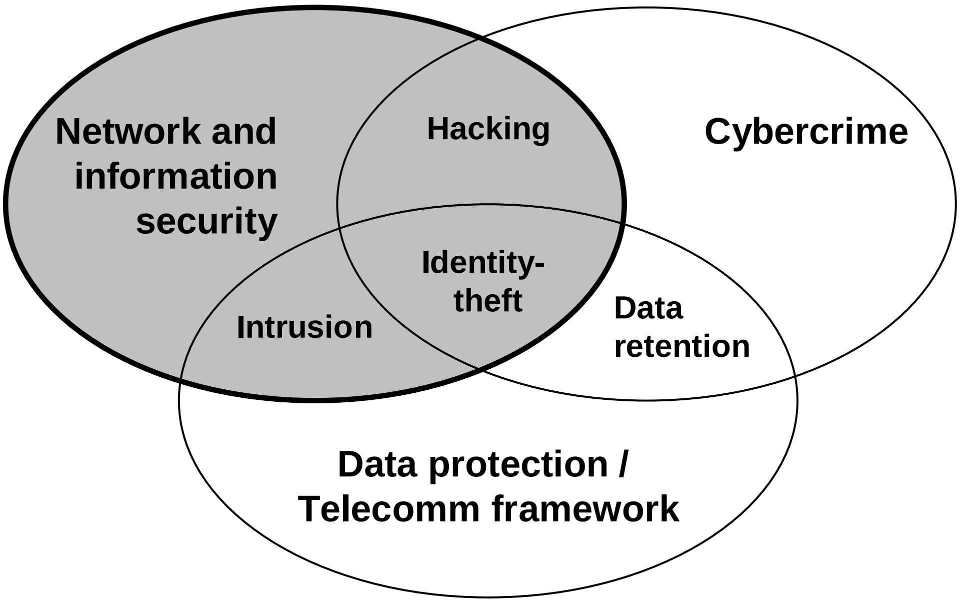
Integrity: the property of safeguarding the accuracy and completeness of assets [7]

The background and context of this report is discussed in Section 3 below.

## *2.2 Issues not covered in this report*

Network and Information Security in the context of this report therefore excludes legal issues and policy and excludes law enforcement (for more information about law enforcement. In addition, this report does also not address security problems arising from natural disasters.

The following chart extracted from COM(2001) 298 [2] illustrates this in diagrammatic form:


Network and information security
Hacking
Cybercrime
Identity-theft
Intrusion
Data retention
Data protection / Telecomm framework

### 2.2.1 Legal issues

For an overview of legal issues, the reader is referred to other sources, including ETSI Technical Report 336 [9], which provides further information on this subject. Digital Rights Management (DRM) is not covered. It is the subject of a "state of the art" overview by the CEN/ISSS DRM Focus Group, which will shortly be published; standards issues include the work of the Moving Pictures Experts Group (MPEG) in committee ISO/IEC JTC1/SC29. Data protection and privacy is the subject of the 2002 report of the CEN/ISSS IPSE initiative (http://www.cenorm.be/isss/Projects/DataProtection/dp.default.htm). Information about products and services for lawful interception and standards related to this topic can be found on http://www.gliif.org/standards.htm. More information about data protection and privacy can also be found on the CEN Website (http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/activity/wsdpp.asp), where a workshop on these issues was held.

### 2.2.2 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.

### 2.2.3 Information security professional qualifications

In view of the removal of barriers to the movement of labour within Europe there is a need for a common understanding of some of the issues which impact upon Information Security. 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 organisations 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 protecting the organisations critical assets then it make good business sense to employ people who have a track record in information security and they can deploy such competence in a professional manner.

### 2.2.4 Longevity of archiving

Concern exists over the length of time over which legally-binding signatures, certificates, certificate revocation lists and other cryptographic keys can be archived and successfully retrieved. Even if the raw data remains accessible it is necessary to satisfy the requirements for checking and verification. *[**Editor's note:** This text should make reference to retention of telecoms data.]*

# 3 Context 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 lined out in [1].

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 to then convince the end user that doing business in this way in Europe is not only efficient but also secure.

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 crime in products and services, electronic communication, and application areas, such as e-health. To help understand the scope reference should be made to the security architecture described in the ITU-T report COM 17 – D29 [8]. In essence the NIS report addresses those security issues arising in the "End User Plane" as defined in the ITU report. This means that certain significant elements of the internal security of backbone networks are not addressed. These are elements where standards from the European Standards Organizations (ESOs) 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 end user 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 based networks. However specific reference is also made to the use of Virtual Private Networks, wireless LANs and 3G networks since it is likely that any electronic transaction or communication may utilise 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 The structure of this report

In the introductory sections, this report links to the issues identified in the Communication from the Commission [1] Section 5 addresses general issues that can be addressed by standardisation, and also discusses upcoming trends and future developments.

Section 6 describes the general user requirements for network and information security, including home users, small to medium enterprises, through to large organizations. This is followed by Section 7, which identifies typical network and information security related threats.

Sections 8 – 12 then identify existing standards and suggest further solutions to these threats, based on the table in Section 7 that links the identified threats with the security services discussed in sections 8 – 12.

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

# 5 CEN and ETSI response to proposed actions

*[**Editors Note**: This section will be expanded with text based on COM(2006) 251 (see Annex 2 for reference).]*

In this section the report provides recommendations arising from those actions specifically proposed in the Communication from the Commission COM(2006) 251 [2] which are directed at or are relevant to the ESOs.

## *5.1 Awareness raising*

There are three proposed awareness-raising actions in [2] aimed at Member States.

Although these actions are aimed at the Member States, the ESOs can also continue to contribute to awareness-raising within their own membership and within their own technical organizations. An important area for awareness is the SME environment, and this issue is further discussed in Section 6.2 below.

## *5.2 Technology support*

There are two proposed actions in [2] on Technology Support aimed at Member States and the Commission, concerning security in the 6th Framework programme and pluggable strong encryption.

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

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

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

## 5.3 Support for market oriented standardization and certification

### Interoperability

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

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

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

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

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

### 5.3.1 EU initiatives

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

### 5.3.2 Certification and accreditation

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

### 5.3.3 Participation in standardization activities

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

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

### 5.3.4 Stimulation of standardization activities

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

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

## *5.4 International co-operation*

*[**Editors Note**: This section will be expanded with text based on COM(2006) 251 (see Annex 2 for reference).]*

## *5.5 Future developments*

Taking account of new technologies and future developments, and the results these developments might have on the NIS security in place is an important issue to provide dynamic security solutions. It is therefore important to be aware of these new developments and their security implications. The issues discussed in this section will not be subject of the considerations in the following sections.

### 5.5.1 RFID

Radio frequency identification (RFID) tags have gained considerable attention and interest within industry and the media. This arising 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 [http://www.rfidjournal.com/.]. 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. 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. That impact maybe very important on SMEs activities. RFID is certainly a way to improve the security of SMEs businesses in the near future.

Contactless communication for identification has been used for years in public transportation, access control mechanisms, etc… in many countries. The novelty relies in the cost of small devices that provide secure RFID functionality. Therefore the device costs will be an extremely important requirement when it comes to choose the cryptography to be used.

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. However, these standards are limited to passive RFIDs. Therefore there is an urgent need for standardisation for active tags. Protocols for the radio communication between passive tags and readers are defined in ISO 18000, 10536, 14443, 15693, 10373-6.

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, security features can not be added. The challenging problems will occur for middle range tags. The prices will highly depend on the cryptography used and therefore from the security level offered by the tags.

#### 5.5.1.1 Security Threats

The security threats in RFID tag deployment to be addressed are numerous and can not be assessed 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.

#### 5.5.1.2 Security solutions for deploying RFID Tags

When it comes to deployment of a cryptographic solution, there is the unavoidable question of what kind of cryptography to implement.

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 earlier in this report. Another difference is that symmetric algorithm usually requires less computational resources than asymmetric algorithms. However, for RFID this difference can be narrowed down.

Many of the papers published in the area can be found at [http://www.rfidjournal.com/]. An optimised implementation of the AES has been proposed, but the time for the AES computation is still a little too large to fit easily within standard communication protocols. Nevertheless, that indicates that strong standardised 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 standardised asymmetric schemes, such as elliptic curves based algorithms have the same drawbacks as RSA. On the other hand, some existing standardised asymmetric algorithms with different performance profiles may be considered as valid solutions. These public-key algorithms (for instance GPS algorithm specified in ISO/CEI 9798-5) may be suited to RFID deployment and may offer more efficient performances than standard symmetric cryptographic solutions.

### 5.5.2 Next generation networks

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

- On one side 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 this always has been a “closed system” in the sense that the general public knows little of these systems. As a consequence, little security beaches are known to the general public.
- On the other side, we have the data communications world based on the Internet Protocol, with many popular applications, like e-mail, web browsing, … that have entered our daily live. Systems build 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 already known 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 (Sevices and Protocols for Advanced Networking), which have 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 keeps an overall look on 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 on a high level the "co-operation" between access networks (like xDSL, UMTS …) and service domains, like IMS. Corresponding with this NGN reference architecture ETIS 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.

# 6 User Requirements

The general recommendations proposed in this section are based upon a consideration of the security requirements of various classes of potential users of e-business services. The User classes are home users, Small and Medium Enterprises (SMEs) and large organisations and industries. More specific recommendations are also made in sections 8 to 13 of this report.

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 may acquire the responsibility to provide security capabilities but they cannot acquire the responsibility for their correct use. However, the usability of the security features of the product need to be designed so that end user can be expected to use these features. In addition, end users 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.

## *6.1 Home Users*

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

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

### 6.1.1 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.

### 6.1.2 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.

### 6.1.3 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 are the SmartHouse project, which has the overall objective to grow and sustain convergence and interoperability of systems, services and devices home users that will provide an increased functionality, accessibility, reliability and security.

Annex G lists the standards and reports available.

### 6.1.4 General Security Requirements

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

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

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

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

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

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

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

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

## *6.2 Small and Medium Enterprises*

The SME user will typically be an organisation 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.

### 6.2.1 The SME as a user of e-business services

An example is an organisation 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 type 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

### 6.2.2 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..

### 6.2.3 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 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 6.1, final paragraph.

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.

## *6.3 Large Organisations and industries*

The large organisation 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 organisations and Trusted Third Parties (e.g. Certification and Registration authorities). The organisation will have large numbers of networked workstations and may make use of Virtual Private Networks (VPNs). In the context of this report “large organisations” include government organisations where the communication is between government and citizen but government to government is outside the scope.

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

### 6.3.1 General Security Requirements

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

a. Large organisations 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 organisations 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 organisations 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.

# 7 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, accountability and availability of the service. The assets of these electronic services are:

- The data of organisations 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.

The threats to the assets of the e-business service s 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 both through invasion of the privacy of individuals and through the exploitation of data intercepted.*

*T2. Unauthorised access into computer and computer networks is usually carried out with malicious intent to copy, modify or destroy data and 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.*

*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, contracts may be repudiated, and confidential information may be sent to the wrong persons.*

*T5. Security incidents are due to unforeseen and unintentional events such as hardware or software failures, human error, unexpected behaviour from users, or natural disasters (floods, storms, and earthquakes).*

*T6. Illegal content decryption and/or copying and/or forwarding on the Internet can cause a range of problems and have become quite common.*

***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 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. These attacks include VoIP spamming, denial of service (DoS) and distributed denial of service (DDoS) attacks.*

*T9. The more and more common use of Voip telecommunications makes telecommunication services and networks more vulnerable and definitely less reliable.*

The threats T1 to T9 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 8 to 12 inclusive. For the purposes of this report, the security services are defined as follows[1].

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 authorised. The overall security of the e-business services and their assets rely ultimately on the capability to authenticate users of the service.

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

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

d. **Network and Information Security Services**. These services are required to ensure sufficient security management, taking account a holistic set of security measures (in addition to those discussed in the previous sections) to achieve security management. The security controls in this section include policies, organisational controls, controls to achieve asset management, human resources security, physical security, controls to acieve operational and communcations controls, controls against malicious code, the secure design and configuartion of applications, incident management and business continuity.

e. **Assurance Services**. These services are intended to provide the e-business user 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. The end result of the process can be a certificate[2], following a process of independent audit or evaluation.

The following table shows the relationship between threats T1 to T9 and the set of security services defined above (note that Assurance services are not included because they do not counter threats in themselves but define what confidence can be placed in security measures):

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

[2] 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.

| **Threat** | **Security Services** | | | |
|---|---|---|---|---|
| | Registration, Authentication and Authorization | Confidentiality and Privacy | Trust | Network and Information Security |
| T1 | | **X** | | |
| T2 | **X** | **X** | | |
| T3 | | | | **X** |
| T4 | **X** | | **X** | |
| T5 | | | | **X** |
| T6 | | | | **X** |
| T7 | | | | **X** |
| T8 | | | | **X** |
| T9 | | | | **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 procedural security measures. The following sections of the report, each associated with an Annex containing a list of relevant standards and related work, now describe these security measures under the high level security services defined in the previous section and contain relevant recommendations:

Section 8 and Annex A: **Registration, Authentication and Authorization Services**;

Section 9 and Annex B: **Confidentiality and Privacy Services**;

Section 10 and Annex C: **Trust Services**;

Section 11 and Annex D: **Network and Information Security Services**;

Section 13 and Annex E: **Assurance Services**.

# 8 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 credential supplied in the registration process) is validated by the e-business system to access specific e-business services. In general the authentication process checks that the user of his virtual identity is the true owner of the credential supplied during the registration process by means of a password or biometric for instance.
- **Authorization** Authorisation is the granting of rights to access services, information and resources.

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

## *8.1 Security Measures*

Registration and authentication services comprise the following security measures:

a. Effective user registration

b. Effective user identification;

c. Effective user authentication;

d. Effective authorization/access control;

e. Effective user management.

### 8.1.1 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. A standard is needed for users to store and retrieve their web passwords in a convenient and secure way, under a master password.

### 8.1.2 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 (notably in health care) 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 8.1.3 below).

### 8.1.3 Effective User Authentication

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

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

b. The use of **access control mechanisms, like access control lists (**ACL) and **firewalls** will help prevent all unverified users (including “hackers”) from gaining unauthorised access to e-business services (these matters are dealt with in section 11 on Network and Information Security Services).

Note that the use of biometrics implies both identification and authentication, so they will only provide limited privacy protection.

### 8.1.4 Effective User Authorization/Access Control

Authorization and access control are considered two sides of the same coin. While authorization considers the rights of a user to access application, access control addresses the same rights from the viewpoint of the application(s).

Authorization may be based on 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.

### 8.1.5 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. As different users may have different needs and may use different parts of the profile, user authentication and access control (by using authorization attributes, or role based access) should be carried out. 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

## *8.2 Passwords*

Username/password combinations are relatively insecure. Passwords are vulnerable to opportunistic attacks (e.g. badly structured passwords may be guessed, passwords may be accidentally disclosed to unauthorised 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 organisations 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.

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 server to obtain a service (entry to the network, or even his own computer). The protocol is desiged so that the password of the user cannot be verified without cooperation of the server. This allows the server to control the number of attempts to protect simple passwords.

An implementation of password authenticated key agreement is suggested under the name Secure Remote Password (SRP), see also RFC 2945. It is suggested to be used for Transport Layer Security (TLS). Details can be found in the IETF internet draft “Using SRP for TLS Authentication”.

## 8.3 Biometrics

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

Nevertheless, Biometric-based authentication systems offer flexibility and convenience in use. For instance they can be used in the same way as a password to verify a claimed identity (i.e. one to one comparison).

It is not recommended to use biometrics to identify an individual, since the probability of “false positive” matches is too high. Even with the most accurate biometrics, such as iris recognition, it is not possible to distinguish more than a few hundred individuals. Even then, there is no authentication, so additional authentication measures are necessary. The use of biometrics for authentication is a relatively new technique which potentially offers advantages over traditional authentication techniques particularly in terms of convenience and some security aspects (e.g. a biometric cannot be stolen or guessed). However, current issues over performance mean that biometric systems in isolation may be suitable only for use in situations where the highest level of certainty is not demanded.

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

If biometrics are used as part of a large infrastructure, there is a large number of devices that measure the biometric property. These devices are typically not 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.

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

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

## 8.4 Digital Certificates

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

## *8.5 Smart Cards*

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

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

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

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

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

## *8.6 Recommendations*

*[**Editor's note:** All recommendations will be produced when the text of the report has been agreed.]*

# 9 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 authorised 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).

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

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

## 9.1 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 authorised 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[3], destination etc. See http://www.mobihealth.org.

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 8). 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 re-use** procedure to prevent the accidental release of sensitive information to unauthorised individuals.

## 9.2 Encryption of stored information

There are many stand-alone consumer-oriented PC-based products available for encrypting stored information. Unfortunately these are often difficult to use for the non-technical user. Documentation is generally poor and there is a lack of information on issues such as key management. Note that TLS/SSL and PGP are not useful for storage encryption.

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.

## 9.3 Electronic mail encryption

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

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

Other products such as Pretty Good Privacy (PGP) are also widely used but are not yet regarded as official standards. The main issue surrounding the use of products such as PGP is the lack of a standard infrastructure for key distribution.

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

## 9.4 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.

In general, if we want to secure all communication between two entities, providing security at the lowest layer end-to-end protocol between the entities is one possibility to solve the problem. 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.

A lot of applications use of 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.

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.

## 9.5 Cryptographic Algorithms

ETSI SAGE (Security Algorithms Expert Group) is a task force with responsibility for standardisation in the areas of cryptographic algorithms, fraud prevention, unauthorised 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 funded within the IST programme of the European Commission's FP6.

One particularly important part of the ECRYPT project is the *eSTREAM* project – www.ecrypt.eu.org/estream – 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.

## *9.6 Privacy*

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

On the other hand, there are circumstances where security measures reduce privacy. It is recommended that security measures are implemented in such a way that privacy reduction is kept to a minimum.

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 may 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 http://www.projectliberty.org/) 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 http://www.w3.org/P3P/), "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." It is strongly recommended that the EU supports these initiatives.

## *9.7 Media Re-use Policy*

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

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

## *9.8 Recommendations*

*[**Editor's note:** All recommendations will be produced when the text of the report has been agreed.]*

# 10 Trust Services

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

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

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

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

## *10.1 Security Measures*

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

a. Key Management

b. Non-Repudiation.

c. Evidence of Receipt.

d. Trusted Commitment Service.

e. Integrity.

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

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

### 10.1.1 Non-Repudiation

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

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

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 10.6 below).

### 10.1.2 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 authorised.

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.

### 10.1.3 Integrity

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

- For protection again non-malicious events, such as accidental corruption, simple **checksums** may be adequate.
- For protection against malicious attacks **digital signatures** 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.

## *10.2 Electronic signatures*

An electronic signature is data in electronic form that is attached to or logically associated with other electronic subject data and serves as a means of authentication. The definition includes scanned images, signatures produced by hand-written signature capture devices and digital signatures. 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. 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 http://www.ict.etsi.org/eessi/Documents/e-sign-directive.pdf. This Directive focuses on the legal recognition of electronic signatures. It identifies minimal requirements for certificates, certification service providers and signature creation and verification devices. Individual Member States were tasked with implementing the Directive in national legislation.

The European ICT Standards Board, with a mandate from the European Commission, has launched an industry initiative bringing together industry and public authorities, experts and other market players, in support of the European Directive on electronic signatures: the European Electronic Signature Standardisation Initiative (EESSI). Further information regarding EESSI can be found at http:// www.ict.etsi.org/eessi/EESSI-homepage.htm.

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

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

Under a Commission Decision of 14 July 2003, two CEN Workshop Agreements (CWA 14167-1 and CWA 14167-2) have been cited in a "List of generally recognised 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 recognised standards in compliance with Annex III of the Directive.

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

## *10.3 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.

## *10.4 Time-stamping*

A time stamping function creates a verifiable cryptographic binding between a data item (such as a digital signature) and the time the data item was generated. ISO/IEC has issued ISO/IEC 18014 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*.

## *10.5 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 recognised 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 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.

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.

## *10.6 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 unauthorised 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 http://portal.etsi.org/li).

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.

### 10.6.1 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 3 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.

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, revocation of stolen 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.

It is important that users can use the PKI to verify the validity of a given certificate to find out information about the owner. Fraud using fake certificates is just beginning, and is expected to grow in the near future.

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.

However, we should note that from an end-user point of view, most of these products are found to difficult to use (people don't understand what is happening, bad user interfaces, …). To some extend, smart cards that store the private key and certificate can improve this situation a little bit. Additionally, there is also a lack of attention to interoperability requirements.

## *10.7 Harmonisation of Trust Services*

ETSI and CEN via the European Electronic Signature Standardisation Initiative (EESSI) did undertake work on the harmonisation 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 to 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 have been 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 ot this full set of standards, EESSI has fulfilled its mandate and consequently ICTSB decided to close EESSI WG in October 2004.

However, note that standardization work in this area is still ongoing, be it at a somewhat lower level of activity:

- While the CEN/ISSS E-Sign workshop was closed in 2003, the results are being taken on by the CEN members. for maintenance. Some specifications are meant to progress to ENs, while others are taken on-board by other groups

- New standardization work as well as maintenance of existing standards and specifications is still being carried out in ETSI TC/ESI.

- Any remaining co-ordination tasks in the area of electronic signature are now carried out by the Network and Information Security Steering Group (NISSG) of ICTSB.

## *10.8 Recommendations*

*[**Editor's note:** All recommendations will be produced when the text of the report has been agreed.]*

# 11 Network and Information Security Services

Network and information security services refer to the overall information security management that should be applied to secure any e-business services and applications. Whilst Sections 8 – 10 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 cane be used to achieve these security services, and finally several different examples of security measures that can be considered.

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

## 11.1 Security Measures

Business Services comprises the following security measures:

a. Risk assessment

b. Information security management standards

c. Examples of security measures for business services

d. Exampoles of security measures for network defence services

## 11.2 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, identify the assets of the organization and how important they are for the organization, and to identify that threats and vulnerabilities that could cause problems if they are coming together, and the overall risk situation.

ISO/IEC CD 27005 (see 11.3 below) is a recognised 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. There are, for example, several NIST publications for information security management, which are listed in Annex F. The NIST publication SP 800-30 Risk Management Guide for Information Technology Systems describes methods of risk assessment and is particularly intended for US government. There is also the IT-Baseline Protection Manual from the German Information Security Agency in Germany, which provides a set of controls which can be applied to support the implementation of the security measures selected from ISO/IEC 17799 (or ISO/IEC 27002, see 11.3 below).

## 11.3 Information security management standards

### 11.3.1 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 summarised 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 13.3 for more detail about this).

These standards are listed in Annex D of this report, 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 organisation. In addition, it can be used for third party certification, and is discussed in Section 13.4 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. More information about risk assessment is contained in Section 13.2.1 below.

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 13.5 below.

### 11.3.2 Other standards for security maesures 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 (these standards are also listed in Annex D of this report):

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.

## *11.4 Examples of security measures for business services*

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

Business Services in the context of this report includes applications such as web services, interactive services and electronic messaging

### 11.4.1 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.

### 11.4.2 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

### 11.4.3 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 analyse client and service transactions that could compromise the service. The level of accounting and audit will depend upon the assessed impact of a failure but may include:

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

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

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

### 11.4.4 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.

### 11.4.5 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.

### 11.4.6 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 is as yet no internationally approved standards.

### 11.4.7 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.

### 11.4.8 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.

## *11.5 Examples of security measures for network defence services*

Network Defence services provide the means by which *malicious* threats emanating from electronic connection to external IT resources and networks (including the Internet) are countered. If such threats materialise 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.

### 11.5.1 Preventative Measures

Preventative measures comprise a combination of procedural and technical measures:

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

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

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

d. Using suitably configured **firewalls** to prevent hacking attacks. System responses to service refusals should be designed to prevent a potential hacker deducing useful system information such as physical IP addresses[4].

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 organisation (CERT) to obtain information about potential attacks and to report and disseminate security incidents. For further information about CERTS see http://www.ecsirt.net.

### 11.5.2 Detection Measures

The main technical measure is the deployment of **Intrusion Detection Systems** (see also 11.3.2 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.

# 13 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

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

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 recognised standard for the overall management of Information Security.

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

## 13.1 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.

## 13.2 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. 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.

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). 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 focussed 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.

## *13.3 Information Security Management System Certification*

Certification of ISMS is a procedure where an independent third party assesses the management system of an organisation against the ISMS standard ISO/IEC 27001:2005 (see 11.3). This provides written assurance that the ISMS of the organisation conforms to the standard. This includes all activities the organisation 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 organisation has carried out a risk assessment (see also 11.2 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.

Organisations 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 organisation.

The Web site www.iso27001certificates.com provides an overview of the accredited ISMS certificates that have been issued, and also information about some of the scopes, and further statistics.

## *13.5 Accreditation Bodies*

National accreditation bodies are set up to accredit certification organisations 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), EOTC the European Organisation for Conformity Assessment (EOTC) and the International Accreditation Forum (IAF). More information on these organisations can be found at the respective web sites: http://www.iso.ch/iso/en , http://www.eotc.be , http://www.iaf.nu/. They are also listed in Annex F.

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.

# 14 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 standardising security for TMN*.

Further information was obtained from web sites of various organisations 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 has been 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.

## 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.

## Web Service Security

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 Web Services 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 1.1 OASIS standard:

- WS-Security Core Specification 1.1
- Username Token Profile 1.1
- X.509 Token Profile 1.1
- SAML Token Profile 1.1
- Kerberos Token Profile 1.1
- Rights Expression Language (REL) Token Profile 1.1
- SOAP with Attachments (SWA) Profile 1.1

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, […]
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"

**{SEC(2006) aaa}**

# CONTENTS

# 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"

## 1. INTRODUCTION

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 revitalise 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 2001 Communication defines NIS as "*the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems*". Over recent years, the European Community has implemented a number of actions to improve 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.

[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.

Trust and security also play an important part in the European Community programmes devoted to research and development. The 6th Research Framework Programme addresses these issues through a wide range of projects. Security-related research is to be reinforced in the 7th Framework Programme with the establishment of a European Security Research Programme (ESRP)[6]. Furthermore, the Safer Internet Plus programme supports networking projects and the exchange of best practices to combat harmful content circulating on information networks.

As a part of its response to security threats, the European Community decided in 2004 to create the European Network and Information Security Agency (ENISA). ENISA contributes to the development of a culture of network and information security for the benefit of citizens, consumers, enterprises and public sector organisations throughout the European Union (EU).

The EU also plays an active role in the international fora addressing these topics, such as the OECD, the Council of Europe or the UN. At the World Summit on the Information Society in Tunis, the EU strongly supported the discussions on the availability, reliability and security of networks and information. The Tunis Agenda[7], which together with the Tunis Commitment sets out further steps for the policy debate on the global Information Society as endorsed by the world's leaders, highlights the need to continue the fight against cybercrime and spam while ensuring the protection of privacy and freedom of expression. It identifies the need for a common understanding of the issues of Internet security and for further cooperation to facilitate the collection and dissemination of security-related information and the exchange of good practice among all stakeholders on measures to combat security threats.

## 2. IMPROVING THE SECURITY OF THE INFORMATION SOCIETY: THE KEY CHALLENGES

Despite the efforts at international, European and national level, security continues to pose challenging problems.

Firstly, attacks on information systems are increasingly motivated by profit rather than by the desire to create disruption for its own sake. Data are illegally mined, increasingly without the user's knowledge, while the number of variants (and the rate of evolution) of malware[8] is increasing rapidly. Spam is a good example of this evolution: it is becoming a vehicle for viruses and fraudulent and criminal activities, such as spyware, phishing[9] and other forms of malware. Its widespread distribution increasingly relies on botnets[10], i.e. compromised servers and PCs used as relays without the knowledge of their owners.

The increasing deployment of mobile devices (including 3G mobile phones, portable videogames, etc.) and mobile-based network services will pose new challenges, as IP-based services develop rapidly. These could eventually prove to be a more common route for attacks than personal computers since the latter already deploy a significant level of security. Indeed,

[6] The ESPR is being prepared in the course of a Preparatory Action for Security Research during the period 2004-2006.

[7] *Towards a global partnership in the Information Society: follow-up to the Tunis Phase of the World Summit on the Information Society (WSIS)*, COM(2006) 181 final of 27.4.2006.

[8] Malware stands for "malicious software".

[9] Phishing is a form of Internet fraud aiming to steal valuable information such as credit cards, bank account numbers, user IDs and passwords.

[10] Botnets are networks of bots, which are applications that perform actions on behalf of a remote controller and are installed covertly on a victim machine.

all new forms of communication platforms and information systems inevitably provide new windows of opportunity for malicious attacks.

Another significant development is the advent of "ambient intelligence", in which intelligent devices supported by computing and networking technology will become ubiquitous (e.g. through RFID[11], IPv6 and sensor networks). A totally interconnected and networked everyday life promises significant opportunities. However, it will also create additional security and privacy-related risks. While common platforms and applications contribute positively to interoperability and the take-up of Information and Communication Technologies (ICTs), they can also increase risks. For example, the greater the use of "off-the-shelf" software, the greater the impact when vulnerabilities are exploited or failures occur. The emergence of certain "monocultures" in software platforms and applications can greatly facilitate the growth and spread of security threats such as malware and viruses. **Diversity, openness and interoperability are integral components of security and should be promoted**.

The relevance of the ICT sector for the European economy and for European society as a whole is incontestable. ICT is a critical component of innovation and is responsible for nearly 40% of productivity growth. In addition, this highly innovative sector is responsible for more than a quarter of the total European R&D effort and plays a key role in the creation of economic growth and jobs throughout the economy. More and more Europeans live in a truly information-based society where the use of ICTs has rapidly accelerated as a core function of human social and economic interaction. According to Eurostat, 89% of EU enterprises actively used the Internet in 2004 and around 50% of consumers had recently used the Internet[12].

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.

In addition, 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.

Both business and citizens in Europe still underestimate the risks. This is for various reasons, but the most important seems to be, in the case of enterprises, the poor visibility of the return on investment in security and, in the case of citizens, the fact that they are not aware of their responsibility in the global security chain.

Indeed, given the ubiquity of ICTs and information systems, network and information security is a challenge for everybody:

- **Public administrations** need to address the security of their systems, not just to protect public sector information, but also to serve as an example of best practice for other players;

- **Enterprises** need to address NIS more as an asset and an element of competitive advantage than as a "negative cost";

[11] Radio Frequency Identification.

[12] Eurostat, *Internet activities in the European Union*, 40/2005.

- **Individual users** need to understand that their home systems are critical for the overall "security chain".

In order to successfully tackle the problems described above, all stakeholders need reliable data on information security incidents and trends. However, reliable and comprehensive data on such incidents are difficult to obtain for many reasons, ranging from the rapidity with which security events can happen to the unwillingness of some organisations to disclose and publicise security breaches. Nonetheless, one of the cornerstones in developing a culture of security is **improving our knowledge of the problem**.

It is important that awareness programmes, designed to highlight security threats, do not undermine the trust and confidence of consumers and users by focusing only on negative aspects of security. Wherever possible, therefore, **NIS should be presented as a virtue and an opportunity** rather than as a liability and a cost. It needs to be viewed as an asset in building trust and consumer confidence, a competitive advantage for enterprises operating information systems, and a service quality issue for both public and private sector service providers.

The key challenge for policy makers is to achieve a holistic approach. This approach must recognise the respective roles of the various stakeholders. It must ensure proper coordination of the range of public policy and regulatory provisions that impact either directly or indirectly on NIS. The processes of liberalisation, deregulation and convergence have produced a multiplicity of players among the various stakeholder groups, which does not make this task easier. The contribution of ENISA to this goal can be important. ENISA could serve as a centre for information sharing, cooperation amongst all stakeholders, and the exchange of commendable practices, both within Europe and with the rest of the world, in order to contribute to the competitiveness of our ICT industries and a well-functioning Internal Market.

## 3. TOWARDS A DYNAMIC APPROACH TO A SECURE INFORMATION SOCIETY

A secure Information Society must be based on **enhanced NIS** and a widespread **culture of security**. To this end, the European Commission proposes a **dynamic and integrated approach** that involves all stakeholders and is based **on dialogue, partnership and empowerment**. Given the complementary roles of public and private sectors in creating a culture of security, policy initiatives in this field must be based on an **open and inclusive multi-stakeholder dialogue**.

This approach, and its associated actions, will complement and enrich the Commission's plan to continue the development of a comprehensive and dynamic policy framework through a number of initiatives in 2006:

(1) Addressing the evolution of spam and threats, like spyware and other forms of malware, in a Communication on these specific issues.

(2) Making proposals for improving cooperation between law enforcement authorities and addressing new forms of criminal activity that exploit the Internet and undermine the operation of critical infrastructures. This will be the subject of a specific Communication on cybercrime.

These policy initiatives also complement the activity being planned to achieve the goals of the Commission's Green Paper on the European Programme for Critical Infrastructure Protection (EPCIP)[13], developed in response to a request by the December 2004 Council. The Green Paper process is likely to lead to an action plan combining an overall "umbrella" approach to critical infrastructure protection with the necessary sector-specific policies, including one for the ICT sector. The sector-specific policy for the ICT sector would examine, via **a multi-stakeholder dialogue**, the relevant economic, business and societal drivers with a view to enhancing the security and the resilience of networks and information systems.

Moreover, the 2006 review of the regulatory framework for electronic communications will also consider elements to improve NIS, such as technical and organisational measures to be taken by service providers, provisions dealing with the notification of security breaches, and specific remedies and penalties regarding breaches of obligations.

It is largely up to the private sector to deliver solutions, services and security products to end users. It is therefore of strategic importance that **European industry be both a demanding user** of security products and services **as well as a competitive supplier** of NIS products and services.

National governments need to be able to identify and implement best practice in policy-making, as well as demonstrate commitment to these policy objectives by managing their own information systems in a secure manner. Public authorities, in Member States and at EU level, have a key role to play in properly informing users to enable them to contribute to their own security and safety. Raising awareness on NIS issues and providing appropriate and timely information via dedicated e-security web portals on threats, risks and alerts as well as on best practices should be priorities. To this end, examining the feasibility of **creating a European multilingual information sharing and alert system**, which would build upon and link together existing or planned national public and private initiatives, could be a major goal for ENISA.

The global dimension of network and information security challenges the Commission, both at international level and in coordination with Member States, to increase its efforts to **promote global cooperation on NIS**, notably in implementing the agenda adopted at the World Summit on the Information Society (WSIS) in November 2005.

Lastly, research and development, notably at EU level, will help develop new and innovative partnerships to boost the growth of the European ICT industry at large, and the European ICT security industry in particular. The Commission will therefore seek to ensure that appropriate financial resources are allocated to research on NIS and dependability technologies under the 7th EU Framework Programmes.

### 3.1. Dialogue

3.1.1 As a first step to enhancing dialogue between public authorities, the Commission proposes initiating an exercise to **benchmark national NIS-related policies**, including specific security policies for the public sector. This exercise will help identify the most effective practices, so that they can then be deployed wherever possible on a broader basis throughout the EU and help make public administrations a driver of best practice in security. The work on electronic identification, for

[13] COM(2005) 576 final of 17.11.2005.

example as part of the recent eGovernment Action Plan, could play an important role in that respect.

If appropriately structured, the results of such a benchmarking exercise will **identify 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. ENISA should be called upon to play an active role in this dialogue, and in consolidating and exchanging best practices.

3.1.2 A **structured multi-stakeholder debate** on how best to exploit existing tools and regulatory instruments to attain an appropriate societal balance between security and the protection of fundamental rights, including privacy, is needed. The planned Conference "i2010 – Towards a Ubiquitous European Information Society" being organised by the forthcoming Finnish Presidency, and the consultation on the security and privacy implications of RFID, which is part of the broader consultation recently launched by the Commission, will contribute to this debate. In addition, the Commission will organise:

- A business event to stimulate industry commitment to adopting effective approaches to implement a culture of security **in industry**.

- A seminar reflecting on ways to raise security awareness and strengthen the trust of **end-users** in the use of electronic networks and information systems.

### 3.2. Partnership

3.2.1 Effective policy making needs a clear understanding of the nature and extent of the challenges. This calls for not only reliable and up-to-date statistical and economic data both on information security incidents and levels of consumer and user confidence, but also up-to-date data on the size and trends of the ICT security industry in Europe. The Commission intends to ask ENISA to develop **a trusted partnership with Member States and stakeholders** to develop an **appropriate data collection framework**, including the procedures and mechanisms to collect and analyse EU-wide data on security incidents and consumer confidence.

In parallel, because of the highly fragmented market in the EU and its rather specific nature, the Commission will invite Member States, the private sector and the research community to **establish a strategic partnership** to ensure the availability of data on the ICT security industry and on the evolving market trends for products and services in the EU.

3.2.2 In order to improve the European capability to respond to network security threats, the Commission will ask ENISA to examine the **feasibility of a European information sharing and alert system** to facilitate effective responses to existing and emerging threats to electronic networks. A requirement of such a system will be **a multilingual EU portal** to provide tailored information on threats, risks and alerts.

### 3.3. Empowerment

The empowerment of each stakeholder group is a prerequisite to foster awareness of security needs and risks in order to promote NIS.

3.3.1 In this respect the Commission invites **Member States** to:

- Proactively participate in the proposed benchmarking exercise of national NIS policies;

- Promote, in close cooperation with ENISA, awareness campaigns on the virtues, benefits and rewards of adopting effective security technologies, practices and behaviour;

- Leverage the roll-out of e-government services to communicate and promote good security practices that could then be extended to other sectors;

- Stimulate the development of network and information security programmes as part of higher education curricula.

3.3.2 The Commission also invites **private sector** stakeholders to take initiatives to:

- Develop an appropriate definition of responsibilities for software producers and Internet service providers in relation to the provision of adequate and auditable levels of security. Here, support for standardised processes that would meet commonly agreed security standards and best practice rules is needed.

- Promote diversity, openness, interoperability, usability and competition as key drivers for security as well as stimulate the deployment of security-enhancing products, processes and services to prevent and fight ID theft and other privacy-intrusive attacks.

- Disseminate good security practices for network operators, service providers and SMEs as baseline levels for security and business continuity.

- Promote training programmes in the business sector, in particular for SMEs, to provide employees with the knowledge and skills necessary to effectively implement security practices.

- Work towards affordable security certification schemes for products, processes and services that will address EU-specific needs (in particular with respect to privacy).

- Involve the insurance sector in developing appropriate risk management tools and methods to tackle ICT-related risks and foster a culture of risk management in organisations and business (in particular in SMEs).

## 4. CONCLUSIONS

Identifying and meeting security challenges in relation to information systems and networks in the EU requires the full commitment of all stakeholders. The policy approach outlined in this Communication seeks to achieve this by reinforcing **a multi-stakeholder approach**. This would build on mutual interests, identify respective roles and develop a dynamic framework to promote effective public policy-making and private sector initiatives.

The Commission will report to Council and Parliament in the middle of 2007 on the activities launched, the initial findings and the state of play of individual initiatives, including those of ENISA and those taken at Member State level and in the private sector. If appropriate, the Commission will propose a Recommendation on network and information security (NIS).