



ETSI Future Security Workshop: The threats, risks and opportunities 16-17 January 2006 – Sophia Antipolis, France

WORKSHOP OVERVIEW

Overview

The workshop on the 16th and 17th of January 2006 hosted by ETSI (and supported by Vodafone and the United Kingdom DTI) brought together over 70 people together involved in Security Standards work in Sophia Antipolis for 2 days. Brief presentations were given by experts representing many organizations, such as ETSI, CEN, The European Commission, ITU-T, ENISA and the Industry.

A number of discussions were held on key points, and directions noted for further work. Feedback from the participants indicated enthusiasm for the concept and content, and that they would like a repeat for next year, and so an annual event looks to be indicated. The input slides are all freely available on the workshop web pages¹, and in addition a web cast was organized for those not able to attend.

Conclusions

The participants in the workshop discussed the final lessons and made suggestions for future standardization. The following topics were identified as being of vital importance:

1. **Next Generation Networks:** There are different access technologies with different security mechanisms, and eventually we will converge to one platform. New players to be taken into account, and there are NGN security related recommendations in USA (NSTAC). *We need a great deal of further coordination with other bodies on NGN security issues.*
2. **Definition of privacy levels** for users need further work, with guidelines in UPM, and a policy and description of constraints. Users should not have to make security related decisions, and they should have a default of good security. *We need to define security levels to give users a safe level of security without the need of any knowledge or education on their side.*
3. **Product proofing** against crime, and the European Mandate. Much useful work has been carried out within the groups, but we have not brought this together in one coherent summary. *We need to issue clear guidance to security related activities on this issue. We need to produce a summary on product proofing activities, and find a way of issuing guidance on this and future security-related directives to working groups.*

¹ See <http://portal.etsi.org/securityworkshop/home.asp> - Presentations are also available on these pages.

4. **Collaboration with standards bodies:** There are many official and unofficial security standards being defined. This has led to duplication in some areas, and conflicting standards in others. *We need to find ways of coordinating security standards to ensure that we do not duplicate or produce different standards.*
5. **Digital Rights Management:** A number of schemes exist for DRM, and no single solution. *We should explore the possibility of creating a single DRM specification.*
6. **X.805, Common Criteria and TVRA:** There are a number of different standards for realizing the assurance of the security of systems. *We should try and simplify these different standards for assurance.*
7. **Data Retention Directive:** Standardization is required to ensure that systems, networks and products conform. *We need to create standards to meet the requirement of the Data Retention Directive.*
8. **Network issues:** Network availability, Network Resilience and Physical layer security are all subjects that merit further standardization. *We need to look at methods to improve network security standards.*
9. **Mobile terminal security:** Methods are required to define the ability of a mobile to be closed down when attacked by malware. We need to look at terminal security (antivirus, firewall ...), and this is also connected to security of the network and over the air management. False emergency calls have also been an issue. *We need to define security of a mobile terminal to a) Stop malware from spreading b) Improve the MMI to reduce false calls c) Remove security decisions from the users d) Allow terminals to be remotely yet securely managed..*
10. **Security in Banking systems** (and collaboration), ECBS, contacts with other bodies with others in the banking security. *We need to consider ways of cooperating on standards that exist within banking and telecommunications.*
11. **Real-time security challenges,** Distributed Denial of Service is an increasing threat. *We need to find ways of networks stopping DDOS.*



Summary of the Workshop

Opening Speeches

Adrian Scrase - ETSI Chief Technical Officer

Described the work of ETSI and welcomed the participants to the workshop. GSM was developed (by ETSI) for Europe, and is now a worldwide success story, with more than 1.5 billion users in over 200 countries, and one million new users every day. ETSI's Lawful Interception handover standard is being deployed in Europe, and also in USA and Australia, where the laws are being developed to comply with the ETSI Standard. DVB system specifications based on DVB Project proposals have services available on every continent. TETRA has more that 600 contracts in 70 countries. There are also Radio microphones and cordless audio equipment, and global agreement on common standards amongst may other successes.

ETSI has global membership; the Institute was established as a European body and retains European responsibilities. But many of ETSI's Members are global players and so ETSI seeks to have its standards adopted worldwide. Over 100 of ETSI's Members (about 20% of the total) have no established operations in Europe and many of the other 80% are headquartered outside Europe

Some of the latest standards are:

- Next Generation Networks (NGN)
- Ultra wideband (UWB)
- Bandsharing
- Grid
- RFID
- Low Power Devices
- Emergency alerting, e-call
- GSM on aircraft
- Communications for Public Safety.

Emerging technologies and new technologies bring new security challenges: New technologies require new security mechanisms and features and technology is becoming more powerful, so attackers take advantage of new technologies and become more powerful too. Adoption of new services and take-up of new technologies are materially affected by Security, Trust, Privacy, Reliability: these are all key factors for success. Security failures are no longer just an embarrassment; they directly affect the stock value of companies, and the market success of new products and services.

ETSI does not work in isolation: it is also necessary to maintain and strengthen collaboration with other bodies that are active in security standardization.



Charles Brookson - ETSI OCG-Security Chairman, DTI

Described an overview of work within ETSI and introduced the various topics which would be covered within the workshop, the objective of the workshop was to:

- Share information
- To assess what has been done so far
- To identify the gaps and/or duplication
- To indicate and propose the areas for future work to be performed

Elisabetta Carrara - ENISA Expert Security Technologies

Described the different activities within ENISA:

Cooperation and Support Department is responsible for Computer incident and response handling, Awareness raising, Relations with EU bodies and Member States Relations with industry and international institutions.

Technical Department looks at Risk Management, NIS Security Policies and Security Technologies.

Risk management is making an Inventory of methods (composed of what is available on the “market” to provide information so that comparisons are possible), Information packages (to generate comprehensive information packages for types of stakeholders), consolidation of existing definitions, and finally producing a roadmap on emerging risks.

NIS Security Policies looks at Best practices for technical and procedural security policies for SMEs and other sectors. It is conducting an Inventory of measures and principles recommended or adopted by providers of electronic communication services to comply with legal requirements, an Assessment of the need to facilitate application of existing accreditation and certification schemes, and a Framework for identifying various levels of security, in particular for different authentication methods.

And finally **Security Technologies** is working on

- Analysis of the major technical developments in relation with standardization and other NIS initiatives.
- User interface and security.
- Presence of ENISA in various fora and establishment of a network of contacts in the technical, development, standardization, and research community.
- Dissemination using the Web Portal and the ENISA Quarterly (a magazine about ENISA’s main activities, together with articles by NIS experts).

Session 1: ETSI Security Standardization

Chaired by Charles Brookson - ETSI OCG-Security Chairman, DTI

Lawful Interception - Scott Cadzow - ETSI LI Vice-Chairman, 3CL

Described the standardization activities concerning Lawful interception.

The actors in lawful interception are:

- The target, this is the entity against which the interception is made.
- The correspondent, who the target is talking to and whose communication with the target is intercepted.
- The monitor, the entity that any interception is given to (usually a Law Enforcement Monitoring Facility (LEMF))
- The operator, the entity that serves the target and manages the interception

The reason why ETSI has taken a lead in this area for many years is that the Institute is the source of many communications protocols, it has the knowledge centre for how to intercept, it is membership driven with National and regional requirement to support LI identified to members, and standards have benefits of lower cost to members if protocol and data model is standard (one model fits wherever the communications protocols are used).

Within ETSI there is a Division by functions of Handover and Interception

- Handover: is led by TC LI, and defines means for delivering intercepted signalling and communication to LEMF.
- Interception: is performed within technology TBs and defines how technology specific data is intercepted.

There is great fluidity in the environment because communications models and modes change; there are Pay as you go models, Text and Instant messaging over voice. Operators may be virtual and real operators, small or large operators, bit carriers and service providers, or even interconnected or discrete. Support of law enforcement stays constant, but criminal behaviour may change and evolve to take on the new technologies.

The challenges are

- Encapsulation versus Mapping, and who does the processing?
- Broadband, interception and handover, and identification and capacity
- Multi-provider environment, one target many provider relationships involving the network, service and content
- NGN, with object based capabilities rather than services, open architectures with open provision, and end user service logic.

NGN Security: Evolutionary Security Standards - Judith E. Y. Rossebø - ETSI TISPAN WG7 Chairman, Telenor R&D

Covered the areas of ETSI TISPAN (WG7 security) and ETSI NGN security (security goals for the NGN and the challenges and threats).

TISPAN Working Group (WG) 7 is responsible for the management and co-ordination of the development of security specifications for TC TISPAN. For TISPAN NGN Release 1, TISPAN WG7, assisted by the specialist task force (STF) 292, has:

- Defined security requirements;
- Defined a security architecture for NGN R1;
- Conducted threat and risk analysis for specific NGN use cases;
- Proposed countermeasures.

WG7 security standardization is risk-based using the STF292 methodology for Systematic threat, vulnerability and risk analysis (TVRA).

The objective is fixed and mobile convergence, and so the TB is in close collaboration with 3GPP to ensure, for example, IMS security is aligned to carry out this goal. The security goals of TISPAN are:

- Prevention of masquerade, using checks to see who the users really are, these may be used to limit fraud and may be used to raise trust (confidence);
- Privacy of communication, in line with regulatory requirements and customer expectations;
- Availability of the NGN services also in line with regulatory requirement (sometimes) and customer expectation.

There are some constraints in the areas of the regulatory environment:

- Support of citizen, with emergency call services and lifeline services,
- Support of privacy Directive with call tracing and malicious communication identification,
- Support for law enforcement, with lawful Interception

This must be balanced with legacy networks and equipment and strong security mechanisms may not be applicable. A question to be answered is how to mitigate at lowest risk.

The security challenges to NGN come from the legacy fixed and from the fact that 2G/3G security is fundamentally different: for example Authentication, Confidentiality and Integrity are treated in different ways and xDSL security relies on some of the assumptions of legacy fixed. Also, Far-end NAT is used in fixed IP-based networks, but not in 2G/3G, and the use of WLAN in home networks.

Current areas of work include the new threats and risks landscape:

- Authentication to IMS, with solutions for legacy deployments, access to IMS granted based on access network authentication (NASS-IMS bundled);
- ISIM over UICC otherwise, the reuse of IMS mandates this, and the challenge – realizing use of ISIM over UICC for access to IMS (from any terminal – not just 3G terminals).

In conclusion, TISPAN WG7 is addressing NGN security, but we have the challenges of new risks, an IP-world, a large legacy base with a diversity of access and terminals. ETSI TISPAN WG7 is addressing the threats and challenges for securing the NGN by systematic threat, vulnerability and risk analysis (TVRA). Based on the results of the



TVRA countermeasures are being standardized. And by this means ETSI TISPAN NGN security standards are helping to enable fixed-mobile convergence

Smart Cards - Klaus Vedder - ETSI SCP Chairman, Giesecke & Devrient GmbH

Described Smart Card activities in TC SCP and earlier initiatives.

The group has 18 Years of Dedication and Real-life Experience, and was founded in March 2000 as the successor of SMG9 (the SIM-people, which specified the SIM for GSM). This is the most successful smart card application with more than 1,6 billion subscribers and 4 billion SIMs deployed.

The Mission of the group is to create a series of specifications for a smart card platform, based on real-life (outside) requirements, on which other bodies can base their system specific applications to achieve compatibility between all applications resident on the smart card. "A SIM is the physically secured module which contains the IMSI, an authentication algorithm, the authentication key and other (security related) information and functions. The basic function of the SIM is to authenticate the subscriber identity in order to prevent misuse of the MS (Mobile Station) and the network." (from the report of SIMEG#1 in January 1988.)

Today the SIM has successfully stood the test of time, as time goes by attacks become more sophisticated and so do the countermeasures. The mechanical check that a SIM is not removed was enhanced by an electrical/logical check in the very early days, and verification of the PIN was made a pre-requisite to perform the authentication in 1993.

Now we have evolved from the SIM to the UICC: From a standardized application offering secure value added services to a true multi-application security platform providing the user with a wealth of opportunities.

The UICC provides a standardized security platform on which specific applications can be realized using today's interface to the outside world. Logical channels allow to run applications in parallel, applications may share standardized security functions, and applications may have their own security functions and attributes (algorithms, (file) access conditions). As long as an application uses only the functionality specified in the platform it will run on any terminal supporting the entire platform. A new high speed Megabit interface is about to be standardized and will allow to use the smart card for DRM, stream ciphering (Pay TV) and as a mass storage device. A contactless interface will create a wealth of new opportunities.

The vision is to turn today's mobile phone into a multipurpose terminal, a lifestyle tool, and personal security device by establishing a second, contactless communication channel. This is to be achieved by turning the mobile phone into a "contactless card" using the true multi-application capabilities of the UICC combining applications on the card with the offerings of GSM and 3G networks



EMTEL - Raymond Forbes - ETSI EMTEL Chairman, Marconi

ETSI EMTEL is a Special Committee on Emergency Communications. Emergency telecommunications covers both voice and non-voice communications. The need for emergency telecommunications includes many scenarios ranging from a minor road traffic accident to a major incident like a passenger train crash, a terrorist incident, a natural disaster (e.g. an Earthquake, Tsunami). Provision for emergency telecommunications is also a major requirement in disaster situations.

EMTEL acts as a key coordinator in getting requirements on Emergency Communications, outside ETSI (i.e. from different stakeholders) and inside ETSI (i.e. ETSI Bodies). It provides requirements on issues of network security, network integrity, network behavior in emergency situations, and emergency telecommunications needs in networks. It also co-ordinates the ETSI positions on EMTEL related issues. also In addition it is the Interface for emergency communications issues between ETSI and EC/EFTA, NATO, ITU groups, the CEPT ERO and relevant CEN and CENELEC committees.

It covers the issues of

- Communication of citizens with authorities,
- Communication from authorities to citizens,
- Communication between authorities,
- Communication amongst citizens.

Although SC EMTEL was formed to specifically address public safety user requirements for Emergency Telecommunications, other Technical Bodies (TBs) within ETSI have been active for some time: ETSI TISPAN has approved the Emergency requirements for NGN Systems, there is an activity co-operating between 3GPP and ETSI TISPAN on the specification of a Mobile Location Positioning protocol for the delivery to the Emergency Authority the position of a caller to the Emergency Services

A lot of standards related to EMTEL topics (more than 700) are developed by other ETSI Bodies i.e. 3GPP, TC TISPAN, EP MESA, TC TETRA and TC ERM

A Memorandum of Understanding has just been signed between ETSI and NENA (National Emergency Number Association) involving mainly EMTEL and TISPAN. Regular liaisons are exchanged with TIA, ITU-T, and NATO

Electronic Signatures - Riccardo Genghini - ETSI ESI Chairman, Studio Notarile Genghini

Gave a description of the current status of ESI TC and the future of electronic signatures.

TC ESI is responsible for Electronic Signatures and Infrastructures standardization. There are currently 4 Special Task Forces assisting in this activity:

- STF 288 - International harmonisation of ETSI Electronic Signature Standards

- STF 289 - Joint ESI-W3C WG on XML Advanced Electronic Signatures
- STF 290 - Relying Party Access to TSP Status List
- STF298 - Profiles for ETSI TS 101 733 and TS 101 903 Electronic Signatures Formats.

Current open issues are European Interoperability, European co-ordination of Supervision, European Accreditation Schemes, European Root Authority, and Sustainable Business Models. EESSI Standards have been a first important step towards the solution of these Open Issues.

Future use will include e-Invoicing: since greater companies do 90% of invoicing with partner or controlled companies. The production (print and storage) of paper invoices is currently made only for compliance.

The overall cost of a printed invoice varies from € 2 up to € 10 per invoice, while the overall cost of an e-Invoice is less than € 0,2.

Activities concerning standardization of registered Email will allow: Origin authentication, Proof of delivery and Long term availability.

Another future activity is Digital Accounting: paper based accounting is currently made only for compliance to fiscal regulation. Even in SMEs the accounting is software-based. Paper was ineffective in all major accounting frauds and Digital accounting supported by a Trusted Third Party is more resilient and trustworthy.

Future items within ESI TC will be Policies and Procedures for Issuance and Storage of Digital Accounting Documents, and Policies and Procedures for registered electronic mail services.

In conclusion, there is no WYSIWYS, the Technology is clumsy, the social acceptance is low (used only if mandated), and there are wrong expectations on what the QES can do. So far the only success story has been data origin authentication.

Satellite Communications Networks Security - Haitham S. Cruickshank - SES BSM STF 283 Expert

The ETSI Broadband Satellite Multimedia (BSM) working group aims to develop broadband satellite services based on complete interworking with the Internet Protocol (IP). An important feature of BSM is the Satellite Independent Service Access Point interface or SI-SAP interface: This interface provides the BSM with a layer of abstraction for the lower layer functions. Part of BSM STF 283 work focuses on the security architecture for BSM networks (ETSI TS 102 465).

Secure multicast is difficult to achieve. There are many open issues: IPsec with multicast between BSM security gateways, key management architecture for large groups, security

policies creation and enforcement, centralized versus distributed architectures. BSM multicast security architecture will aim to provide a balanced solution between existing link layer (such as DVB-RCS) and network layer (such as IPsec) solutions: Interactions through the SI-SAP interface has to be carefully thought.

The work in ETSI BSM on security will not be complete without full liaison with relevant IST projects: The aim is to achieve co-ordination of work between BSM and these projects. One example is the EU NoE SATNEX project (SATellite communications Network of EXcellence). Another example is the EU STREP project called SATLIFE (Satellite Access Technologies: Leading Improvements for Europe).

In conclusion, Interworking with the Internet security (IPsec) is critical for the success of BSM specifications. Security interactions through the BSM SI-SAP interface have been defined. There are future challenges in secure multicast over satellites. The next phase in BSM security work will focus on multicast issues (ETSI TS 102 466).

Security assurance and the role of ETSI - Scott Cadzow - STF 268, 292 and 3CL

Presented ongoing activities concerning assurance in ETSI.

Poor statement of objectives (eg “I want my product/service to be secure” or “I want to authenticate my users”) and prior assumptions or declaration of solution (eg “I need to use IPsec” or “I must use PKI”) are some of the bad practices in security design.

An understanding of vulnerability and risk, leading to a proof of security, supported by a security assurance is probably what is required. This assurance may be:

- Standards authoring as a tool for clarity;
- Measuring security;
- Illustrating security (ETSI has proven expertise in methods to aid standardization, guides to the use of UML, SDL, text, and normative language (shall, should, may, can).

In particular, Common Criteria can be used to ensure that products offering security features are always carefully evaluated (particularly by government bodies). Work needs to be done in the areas of:

- Method for effective vulnerability analysis, using UML for illustration and simulation, and template and proforma to allow simpler preparation;
- Security for the NGN, with Objectives, Requirements, New methods, Assurance;
- And finally new techniques for Digital Rights Management over networks, Multi-value content over networks, Multi-level countermeasures in networks and Interoperability.



ETSI is good at standards, and is probably the world leader. ETSI is also good at security with protocols (TETRA, DECT, GSM, 3GPP, TISPAN and others), Algorithms (SAGE) and Methods (TISPAN).

Session 2: Mobile Communications Security (15.30-17.00)

Chaired by Charles Brookson - ETSI OCG-Security Chairman, DTI

GSM Association - James Moran - GSMA Fraud and Security Director

Described the work of the GSMA and in particular the security group.

The GSMA is the world's largest and leading cellular trade association, with 683 network operators in 212 countries, and 150 key manufacturers and suppliers. The objective is to arrive at a single voice on behalf of the operator community to establish building block requirements. GSM is serving 1.6 Billion customers globally. It took over a century for fixed line telephony to exceed 1 Billion – GSM did it in less than 12 years. It now offers global access – more people have access to GSM services than running water, more GSM handsets than PC and TVs combined, and is a \$500 Billion industry and GSMA is at the heart of it all.

The security group is the oldest working group - Established 1989. It helped specify security protocols for GSM - the most secure mobile standard; it partners with 3GPP TSG SA3 and ETSI SAGE, with 4 meetings per year with 1 annual joint meeting with Fraud Forum. It also has a GSM 2000 joint project team with ETSI/3GPP TSG SA3. The average attendance is 30 delegates.

The mission of GSM association is to:

- Identify and analyse security risks to which network operators are exposed;
- Advise network operators of the latest best practice being adopted in terms of technical security;
- Maintain and develop security algorithms and protocols;
- Apply and maintain technical security aspects of customer apparatus and network infrastructure;
- Submit operator requirements to international standards bodies;
- Advise on technical solutions to combat fraud.

Work items for 2006 are:

- Oversee and Monitor Network Operator Swap out of A5/2
- Commence Distribution of New UMTS Cipher Algorithm
- Wireless Emergency Response Team Service to reduce exposure to security attacks/vulnerabilities GPRS
- Development of Secure Use of Mobile Phones Public Information Portal
- Legal framework to sanction mobile virus writers
- Secure migration from IPv4 to IPv6

- GPRS Immediate Service Termination.

Security analysis of UMTS and future converged devices - Akbar Rahman - Interdigital Communications Corporation

Described some of the security threats in MBMS, including threats associated with attacks on the radio interface, unauthorized access to MBMS user services and/or data.

One of the main problems is that users have very little incentive to protect the confidentiality of the data required for the service and service keys can be distributed making the traffic keys vulnerable.

There is also the threat to data integrity which follows from illegal acquisition of MTKs whereby the alteration of the transmission is possible. Finally, Privacy violation has to be taken into account, because “Content provider is located in 3GPP Network and then linked to the content” (See 3GPP TS 33.246, B.1.5), and it is at this point that the user identity can be obtained, either by legal or illegal means, by the content provider: identity theft is a distinct result.

Concerning security threats in WLAN: 802.11 wireless systems face numerous threats of which many will be addressed by the 802.11i security standard and an eventual 802.11w standard (that protects “management” frames). The three principal threats that will remain are:

- Traffic Analysis: on a WLAN an attacker can monitor the radio spectrum and initial unprotected exchanges to determine the location of nodes as well as basic parameters of the network (e.g. SSID). This information could then be used to launch physical or other types of attacks;
- Denial of Service: due to the CSMA/CA mechanism of WLAN systems (deferring mechanism) by simply generating white noise or 802.11 MAC frames at the same frequency an attacker could create a Denial of Service attack;
- Identity Theft: an attacker gains unauthorized access to the network. For example an attacker could have stolen a laptop with digital certificates, or stolen a login password or Pre-Shared Keys, etc.

The overall Threats to a Converged Device (if we consider a converged device having just cellular and WLAN interfaces) would include:

- Traffic Analysis
- Denial of Service
- Unauthorized Access of
- Data stored
- Credentials used for authentication
- Network resources

Integration of other interfaces (e.g. Bluetooth, WiMAX, and Ethernet) would bring with them interface-specific threats that must also be addressed. Thus the overall threats to a converged device can be considered to be the sum of individual threats posed by each interface.

In summary, the opportunities for Security Enhancements are through Trusted Processing:

- Ensure hardware and software perform as designed and mitigate attacks from any unauthorized parties;
- Operating systems, platforms, application level functionality and SIM, USIM etc. must interact in a secure and trusted manner;
- Trusted authentication assures that the platform configuration and software running on it has not been tampered with, enabling trustworthiness;
- Trusted platforms are based on Trusted Platform Modules (TPM), a security component being specified by TCG and functions as the basis of trust within a device;
- We also have hardware and physical security.

In conclusion we face with the evolution of personal handheld devices towards open platforms and an always connected world (converged device); the threat of security is more real than ever. Up to now, some threats on cellular networks have been contained due to the cost of launching the sophisticated attacks. These attacks may become easier to launch with the wider availability of equipment. The Non-cellular radio access technologies can become an avenue for backdoor attacks. Operators are increasingly seeking ways to protect the user and hence their networks from attack and moving to specifying comprehensive device level security requirements. New developments in security offer a route to providing security which goes beyond just ciphering, Wireless networks become more secure and can assure the continued roll out of advanced wireless enabled services and applications.

Security and the Convergence of Wireless Standards - Philip Nobles - Dept. of Information Systems Cranfield University Defence Academy

Described fixed and mobile convergence and relevant security issues.

With mobile wireless convergence and many different access mechanisms being included on one device, this leads to issues, such as 3G-WiFi interworking with authentication and trusted roaming.

Issues were raised as to the impact this would have on the Citizen, the technology deployed and if we could protect the user successfully without them having to understand the technological risks.

Session 3: CEN Security Standardization

Chaired by John Ketchell - CEN/ISSS Director

CEN ICT security initiatives - John Ketchell - CEN/ISSS Director

Presented an overview of the ICT security initiatives in CEN.

CEN (European Standards Committee) has national standards bodies as members. CEN/ISSS is the CEN Department dealing with ICT applications. Most CEN/ISSS work is in Workshops and Focus Groups.

- **Electronic signatures:** the CEN/ISSS Workshop eSign produced CEN Workshop Agreements, referred to in Official Journal of EU as relevant to implementation of electronic signatures Directive. Many CWAs are now work items in CEN TC224 and candidates to become European Standards;
- **Protection and security of the citizen:** CEN Technical Board WG161 has a wider scope than ICT. Producing overview of requirements in this domain;
- **Electronic invoices:** CEN/ISSS Workshop eINV is having an open meeting on 29 March. Activity is in connection with implementation of the relevant EU Directive. Work is done in liaison with ETSI TC ESI.

Standardization activities in the area of Biometrics - Nicolas Delvaux - CEN/ISSS Focus Group on Biometrics, SAGEM

Presented an overview of standardization activities in the area of Biometrics.

Biometrics is anonymous data, owned and unique for each individual. A fundamental concept for this technology is the compromise between ease of identification and verification.

Some biometric types of data are signature, eye, face, hand geometry, fingerprint and DNA.

Biometrics can be used in travel documents for border control.

Relevant regulations are: ICAO recommendation on travel document 9303 and EU regulation 2254/2004.

In e-passport biometry can be used to link the ID document and the person and to detect falsification.

Facial recognition (ICAO mandatory), Fingerprint recognition (ICAO option – EU mandatory) and Iris recognition (ICAO option – EU option) are all biometric technologies that are likely to be deployed.

On an international level, ISO/IEC SC37 and SC27 are working on Biometrics security; on a European level, CEN/ISSS Focus Group on Biometrics is active.

In the past there have been successful spoofing attacks to biometrics; in regard, one of the major issues is spoofing protection for biometrics sensors.

Solutions for theft prevention of biometric data must be developed.

Another current challenge is expanding memory size for biometric carriers.

SmartCards as electronic signature devices - Helmut Scherzer - CEN TC 224, IBM Germany Chief Engineer/Consultant

Presented SmartCards as electronic signature devices and some latest news from standardization in this field.

In CEN TC224/WG16 is conducting work on an Application Interface for smart card as Secure Signature Creation Device

ISO/IEC JTC1 SC17/WG4 is also working on this field.

TC224/WG16 is maintaining CWA 14890 (created by ESIGN-K group) and producing a working draft for the new European Standard EN Application Interface for smart card used as Secure Signature Creation Device based.

CEN/TC224/WG15 is producing the European Citizen Card (ECC) standard that will provide Machine Readable Travel Document functionality and Identification, Authentication and electronic signature. The technical standard to be delivered by the end of 2006 will be building the base for national ID card specifications.

Security activities for eHealth - Bernd Blobel - CEN/ISSS eHealth Standardization Focus Group

Presented advanced security activities for eHealth.

The challenge to improve quality, safety and efficiency of their health systems is a requirement under the present conditions of:

- demographic developments with aging and multi-diseased citizens
- increased expectations to quality of life
- growing costs for advanced biomedical, pharmaceutical and technical methods and products for prevention, diagnosis and therapy
- changing social and economical environment moving towards globalization
- increased flexibility and mobility of citizens, goods and services.

This requires turning health systems into customizable, comprehensive and completely integrated care in close relation to efficient public health. Such development must be supported by appropriate ICT to support health telematics and telemedicine (eHealth). The CEN/ISSS eHealth Standardization Focus Group is producing recommendations to establish a permanent eHealth Interoperability Platform.

This requires appropriate Security and Privacy Services and Security Policy

Session 4: Global Security Standardization

Chaired by Ted Humphreys - JTC1/SC27, XiSEC Director

ISO ISMS standards - Ted Humphreys - JTC1/SC27, XiSEC Director

Presented ISO ISMS standards and related initiatives

ISO/IEC JTC 1/SC27 WG1 interests include: Information security management systems (ISMS), Information security best practice, Risk management, Metrics and measurements, Implementation guidance, Information security incident handling, IT network security, TTP services and DR services.

ISO 27000 ISMS Series include standards on Requirements, Measurements, Risk Management and Implementation.

ISO/IEC 17799 (to be renumbered 27002) is the Code of Practice for information security management on a large number of topics such as asset management, mobile code, vulnerability management, human resources, incident handling and other. A revised version of ISO/IEC 17799 was published on the 15th June 2005.

ISO/IEC JTC 1/SC27 WG1 has a liaison with ITU-T and collaboration is taking place in a number of issues.

It was noted that there is no current liaison with ETSI's Technical Committee's, except for a liaison of ISO/IEC JTC 1/SC27 WG2 with ETSI SAGE Special Committee.

Issues related to the use of RFID towards digital evidence - Bertus Pretorius - iPico, Chief System Architect

Presented issues related to the use of RFID as a means of digital evidence, related to some real experience.

Digital evidence is a recording of an occurrence, which can be held in court. The recording and storage method must thus stand scrutiny before the data can be analysed. Digital Evidence proves that a specific Real-World-Occurrence did take place and is what it claims to be.

Positive identification of items is the key to digital evidence.

Digital evidence in the supply chain can allow for the brand owner to protect brand integrity, eliminate counterfeit goods and prevent illegal trade. Also, it can allow brand users to be trust authenticity of goods (this must be guaranteed by a Trusted Third Party).

Electronic Vehicle Intelligence (EVI) is a technology based on an Electronic Registration Device (ERD) that if applied to all vehicles makes illegal vehicles stand out. This allows for prosecution of the illegals, without harassment of the legals. EVI can be used as a trust service.

Digital evidence (both bidimensional barcodes and RFID are applicable) can be used for face value documents such as vehicle licenses, certificates and legal documents, way-bills to achieve proof of source and proof of delivery.

Levels of scrutiny can be electronic suspect selection, physical inspection after suspect selection, digital data and physical verification, forensic level verification.

RFID tags must have a unique ChipID, they require at least 256 bits on tag, tag needs to be reliably read in 5ms, requires a cost efficient reader and spectrum must allow for high density free-flow tag scrutiny.

This in all requires a regulatory framework.

**NGN Network Security Forensics and the EU Data Retention Directive -
Anthony M. Rutkowski - VeriSign, Inc. Vice-President for Regulatory Affairs and
Standards**

Presented NGN Network Security Forensics and the EU Data Retention Directive.

Public networks forensic components are Identity, Stored Traffic, Real-time traffic and Analysis.

Identity: ability to authoritatively identify the service provider, obtain contact information and get to authoritative user/subscriber/object directories and network identifier bindings; key requirements established by law and regulation and may be maintained in part by government agencies.

Stored Traffic: any information generated by network processes that is relevant to a user/subscriber/object communication and has significant latency; requirements and access controlled by law and regulation and may include ad hoc requests, preservation orders, and general data retention.

Real-time Traffic: any information generated by a network process that is obtained in real-time; Requirements and access controlled by law and regulation.

Analysis: concerns network operations, administration, maintenance, fraud detection and prevention, infrastructure protection, law enforcement, public safety, and national security needs.

The EU Data Retention Directive harmonizes data retention and access across Europe. It applies to fixed and mobile network telephony, internet access, instant messaging and internet telephony.

The Directive requires to provide data necessary to trace and identify the source and destination of a communication, identify the type, date, time and duration of a communication, identify the communication device or purported and the location of mobile communication equipment. It does not include content but includes privacy enhancement features.

It was adopted by the European Parliament on 14 Dec 2005.

Challenges and ways to turn the Directive and other forensic implementation capabilities into service opportunities are: Fraud management, Presence and availability management, Extended roaming and easy "sign-on", Personal and public safety support, Authenticated calling name, DoNotCall, Priority access and enhanced QoS, Language and disability support, Push services, Intercarrier compensation.

Principal security and Directive forensic needs are: discovery and access to authoritative European provider information, discovery and access to authoritative user/subscriber/object information, Stored Data Handover Architecture with discovery

and access to authoritative information handover schema, Harmonisation of Data Retention Directive provisions.

NIS Report - Geoff Lister - NISSG, Echelon

Presented the NIS Report.

The NIS Report is the response of CEN and ETSI to the Commission Communication COM (2001) 298. It addresses standardisation issues which are relevant to: the European Standards Organisations (ESOs), industry and academic standards groups and (within an e-business environment) any commercial transaction carried out electronically that relates both to the user and provider of an e-business service.

It is structured in three parts:

- e-Business user security requirements for Home users, SMEs, Large Organisations and industries;
- e-Business service provider security requirements for Registration and Authentication services, Confidentiality and privacy services and Trust services;
- Standards references Annexes.

In July 2003 there was the Joint Issue of the final report by CEN/ISSS (web site) and ETSI (ETSI SR 002 298).

In March 2004 the ICTSB set up NISSG (Network and Information Security Standards Group) to act as a focal point for European Standardisation on network and information security standardization, to implement the recommendations of the NIS report and to provide a focal point of contact between the standardization community and ENISA.

The existing report should be updated as it is out of date and a snapshot at a point in time as technology and standards evolve continuously. Also, structure should be revised as to make it easy to extend it to other business areas.

Standards Information needs to be updated based on a flexible framework to enable the report to be expanded, also being capable of responding to advances in security technology and standards developments, being more accessible and taking into account ENISA.

A first proposal could be for a web-based, three-tier document on the ICTSB web space, where the first tier can be an introduction, the second can identify and define the business areas and the third contain modules on groups of related security services.

ITU-T security standards activities - Ted Humphreys - XiSEC Director

Provided a brief overview of ITU-T security standards activities and a highlight some of the recent key achievements, particularly those resulting from the October workshop *New Horizons for Security Standardization*.

ITU-T SG 17 is the Lead Study Group on telecommunication security - It is responsible for coordination of security across all Study Groups.

It is subdivided into three Working Parties (WPs)

- WP1 - Open systems technologies;
- WP2 - Telecommunications security; and
- WP3 - Languages and telecommunications software.

Current interests are:

- End-to-end Multicast Communications with QoS Managing Facility
- Directory services, Directory systems, and public key/attribute certificates
- Open Systems Interconnection (OSI)
- Communications Systems Security Project
- Security Architecture and Framework
- Cyber Security
- Security Management
- Telebiometrics
- Secure Communication
- Countering spam by technical means

New Horizons for Security Standardization Workshop was held in Geneva 3-4 October 2005. It was hosted by ITU-T SG17 as part of security coordination responsibility. ISO/IEC JTC1 played an important role in planning the program and in providing speakers/panelists. Speakers came from ITU-T, ISO/IEC, IETF, OASIS, 3GPP, ATIS, ETSI, RAIS.

Objectives were:

- Provide an overview of key international security standardization activities;
- Seek to find out from stakeholders (e.g., network operators, system developers, manufacturers and end-users) their primary security concerns and issues (including possible issues of adoption or implementation of standards);
- Try to determine which issues are amenable to a standards-based solution and how the SDOs can most effectively play a role in helping address these issues;
- Identify which SDOs are already working on these issues or are best equipped to do so; and
- Consider how SDOs can collaborate to improve the timeliness and effectiveness of security standards and avoid duplication of effort.

Suggestions and useful discussion took place during the event. The output was included in the workshop's report.

SG17 Roadmap is a four-part project:

- Part 1 contains information about organizations working on ICT security standards

- Part 2 is a database of existing security standards
- Part 3 will be a list of standards in development
- Part 4 will identify future needs and proposed new standards

Concerning the future, the threat scenario is likely to continue to evolve. Attacks are widespread and innovative and broad collaboration is needed to understand and respond to the threats.

Business needs to understand what is happening in the standardization work and anticipate events to defend competitive position and avoid bad things happening. Participating directly in the standards work can have a real payoff. The ITU-T welcomes this kind of opportunity.

Denial of Service Protection “Standardize Defense or Loose the War”

Emir Arslanagic- Cable and Wireless, Director of Global Security Engineering

Presented aspects relevant to DoS attacks.

DoS is an incident in which a system is deprived of the resources it would normally have. It is usually a target of choice risk, and very often related to extortion or racketeering. DoS usually targets publicly available profitable services (extortion), or other opinioned portals (political violence). Distributed DoS sometimes involves more than hundred thousands boots.

Efforts to prevent and stop DoS have been done from various standards bodies.

The history of DoS protection has shown that the only solution is to stop attacks as close as possible to source.

Some questions and consideration on DoS are:

- Does internet users have a right to expect only benign packets to be sent to them?
- Road and car analogy: At the beginning was primary goal to increase road coverage and car speed. Passenger safety has not been consider seriously until seventies;
- Moore’s law is working for us or is there another killer application that will eat all available bandwidth?
- Cleaning function in every switch - standardization will come when technology is ready.

Annex A

Results of Workshop Survey and Evaluation

The questionnaire that was conducted gave the following results:

- Average rating of the usefulness for the participants was 4,2 (on a 1 to 5 scale);
- Average rating of the presentations given was 4,0 (on a 1 to 5 scale);
- 99% of the participants thought there was need for an annual event of this kind and would join next year;
- Concerning the organization it was mainly suggested to have more time for discussion, maybe extending the workshop's duration from 1,5 days to 2 or 3 days;
- Concerning topics on which to focus more the following areas were:
 - Terminal security
 - Regulatory and law issues (eg Directive on Data Retention)
 - DRM
 - Risk Management
 - Security in IP-based technologies
 - Internet Security

35% of the participants filled in and returned the questionnaire.



Annex B

Collective Letter

To: ETSI MEMBERS, OBSERVERS AND COUNSELLORS

Subject: Call for Papers for / Invitation to “Future Security Workshop: the threats, risks and opportunities”

Dear Madam,
Dear Sir,

Security is a key aspect for the evolution and success of Information and Communication Technology (ICT) systems and infrastructures. Networks and information systems are becoming a commodity: they have to be available at all times and especially in emergency situations, preventing loss or leakage of sensitive data and allowing at the same time for law enforcement agencies to capture this data when necessary. The diversity in implementation and characteristics of every technology make the process of securing ICT systems even more complex.

It is essential to put together the different pieces of security work performed in order to ensure coherence and better efficiency in security standardization activities, avoiding duplication of work, promoting security-related initiatives and briefing the people involved in security standardization.

ETSI is hosting a “**Future Security Workshop: the threats, risks and opportunities**” on 16th & 17th January 2006, at its Headquarters in Sophia Antipolis, France.

The main objectives of the workshop are to:

- promote security standards
- identify work areas that are being covered
- identify possible gaps and duplication in the standards
- identify future work items in short, medium and long-term

ETSI will provide an overview of the work being done in the area of security across its technical bodies (Electronic Signatures, Lawful Interception, Mobile Telecommunications Security, Next Generation Networks Security, Security Algorithms, Smart Cards and others). This will be followed by a series of presentations from major organisations involved in several security areas. The topics presented are meant to stimulate open debate and dialogue that will follow the sessions, and will aim to identify security areas in which the standards community can advance and produce new work.

Participation to the workshop is free of charge and open to delegates both inside and outside the ETSI Members.

Candidate speakers are invited to send a synopsis of their presentation to dionisio.zumerle@etsi.org by Friday 28th October 2005. For further details on the workshop including registration please see <http://webapp.etsi.org/MeetingCalendar/MeetingDetails.asp?mid=25156>.

Yours faithfully,

K. H. Rosenbrock
Director General



Annex C

Workshop Programme

Monday 16th January 2006

Registration (9.00-10.00)

Opening speeches (10.00-11.00)

Adrian Scrase - ETSI Chief Technical Officer

Charles Brookson - ETSI OCG-Security
Chairman, DTI

Elisabetta Carrara - ENISA Expert Security
Technologies

Coffee Break (11.00-11.30)

**Session 1: ETSI Security Standardization,
Morning (11.30-13.00)**

Chaired by Charles Brookson - ETSI OCG-
Security Chairman, DTI

Lawful Interception
Scott Cadzow - ETSI LI Vice-Chairman, 3CL

NGN Security - Evolutionary Security Standards
Judith E. Y. Rossebø - ETSI TISPAN WG7
Chairman, Telenor R&D

Smart Cards
Klaus Vedder - ETSI SCP Chairman, Giesecke
& Devrient GmbH

EMTEL
Raymond Forbes - ETSI EMTEL Chairman,
Marconi

Lunch (13.00-14.00)

**Session 1: ETSI Security Standardization,
Afternoon (14.00-15.00)**

Chaired by Charles Brookson - ETSI OCG-
Security Chairman, DTI

Electronic Signatures
Riccardo Genghini - ETSI ESI Chairman, Studio
Notarile Genghini

Satellite Communications Networks Security
Haitham S. Cruickshank - SES BSM STF 283
Expert

Security assurance and the role of ETSI
Scott Cadzow - STF 268, 292 and 3CL

Coffee Break (15.00-15.30)

**Session 2: Mobile Communications Security
(15.30-17.00)**

Chaired by Charles Brookson - ETSI OCG-
Security Chairman, DTI

3GPP Security
Niemi Valtteri - 3GPP SA3 Chairman, Nokia

GSM Association
James Moran - GSMA Fraud and Security
Director

Security analysis of UMTS and future converged
devices
Akbar Rahman - Interdigital Communications
Corporation

Security and the Convergence of Wireless
Standards
Philip Nobles - Dept. of Information Systems
Cranfield University Defence Academy

Cocktail (17.00-18.00)



Tuesday 17th January 2006

**Session 3: CEN Security Standardization
(9.00-10.30)**

Chaired by John Ketchell - CEN/ISSS Director

An overview of standardization activities in the area of Biometrics

Nicolas Delvaux - CEN/ISSS Focus Group on Biometrics, SAGEM

SmartCards as electronic signature devices - Latest news from standardization
Helmut Scherzer - CEN TC 224, IBM Germany Chief Engineer/Consultant

Advanced security activities for eHealth
Bernd Blobel - CEN/ISSS eHealth Standardization Focus Group

Coffee Break (10.30-11.00)

**Session 4: Global Security Standardization
(11.00-13.00)**

Chaired by Ted Humphreys - JTC1/SC27, XiSEC Director

ISO/IEC 17799
Ted Humphreys - JTC1/SC27, XiSEC Director

Issues related to the use of RFID towards digital evidence; a real world experience
Bertus Pretorius - iPico, Chief System Architect

NGN Network Security Forensics and the Data Retention Directive
Anthony M. Rutkowski - VeriSign, Inc. Vice-President for Regulatory Affairs and Standards

NIS Report
Geoff Lister - NISSG, Echelon

ITU-T Network Security Initiatives
Ted Humphreys - XiSEC Director

Denial of Service Protection "Standardize Defense or Loose the War"
Emir Arslanagic- Cable and Wireless, Director of Global Security Engineering

Lunch (13.00-14.00)

Session 5: Round Table Discussion and Conclusions (14.00-15.00)
Chaired by Charles Brookson - ETSI OCG-Security Chairman, DTI

Coffee Break (15.00-15.30)

*NISSG Meeting (15.30-16.30)
(For NISSG members only)*