ETSI Security Standardization

Dr. Carmine Rizzo, *CISA, CISM, CISSP, ITIL, PRINCE2*
ETSI (European Telecommunications Standards Institute), www.etsi.org
650, route des Lucioles, 06921 Sophia-Antipolis Cedex, France
Email carmine.rizzo@etsi.org

ABSTRACT

Information security standards are essential to ensure interoperability among systems and networks, compliance with legislations and adequate levels of security. These standards provide the means for protecting the user, creating a more secure and profitable environment for the industrial sector, from SMEs to large global companies, and providing benefits for a diverse range of interest groups that include government organisations, research bodies and universities.

The increasingly rapid evolution and growth in the complexity of new systems and networks, coupled with the sophistication of changing threats and the presence of intrinsic vulnerabilities, present demanding challenges for maintaining the security of Information and Communications Technology (ICT) systems and networks. To minimise exposure to risks, security must be built in from the beginning when designing new architectures, not added on later as an optional feature.

As a response to such challenges, ETSI, the European Telecommunications Standards Institute, is committed to the establishment and continuous improvement of effective and interoperable telecommunications systems for the benefit of the global community. As such, ETSI is a key player of the global Cybersecurity efforts, by addressing security issues in a broad number of areas including Next Generation Networks (NGN), protecting communications and the ICT infrastructure, working on mobile/wireless communications, emergency telecommunications, lawful interception and data retention.

1. INTRODUCTION

ETSI is an independent, non-profit organisation, with over 20 years of experience of successfully pursuing its mission to produce globally-applicable ICT standards. It has always maintained a strong focus on security matters.

ETSI's work is organised into Technical Committees (TCs) and ETSI Partnership Projects. Supported by Working Groups (WG), each is responsible for producing and maintaining standards in its own technical area. The scope of some TCs is closely related to security aspects; others, including the Partnership Projects (ETSI is the main co-founder of the 3rd Generation Partnership Project, 3GPP), have a much broader scope, but necessarily deal with security issues in the process of producing a complete set of standards for a technology.

2. CYBERSECURITY: ETSI'S WORK

ETSI's strategic direction to ensure that relevant standards meet the Cybersecurity goals is supported by the work within various Technical Committees and Working Groups. Of paramount importance is the related work for the Next Generation Networks. It is widely expected that the telecommunication services of the future will be delivered seamlessly over the most appropriate access network, with users roaming between domains and networks unaware of the underlying mechanisms that enable them to do so (e.g. using fixed and mobile, terrestrial and satellite systems). The new converged and access-independent network model - dubbed Next Generation Networks (NGN) - is based on the extensive use of IP, and is designed to accommodate the diversity of applications inherent in emerging broadband technologies. This opens the door to a new range of security risks. ETSI is already heavily committed to, and is well advanced in, developing the necessary standards to bridge disparate networks and domains and enable them to interoperate. Our work on NGN is being managed by Technical Committee TISPAN (Telecommunications and Internet converged

Services and Protocols for Advanced Networking) and security is one of its core concerns.

TC TISPAN collaborates closely with 3GPP, with the aim of reusing 3GPP security mechanisms on the IP Multimedia Subsystem (IMS). In particular, TC TISPAN is standardising, within its Working Group 7, the security for the fixed network part of NGN and identifying gaps and requirements to extend or modify 3GPP security specifications for its purpose. The committee is also looking into the possibility of standardising new NGN-specific security components where necessary, and is responsible for formally approving technical deliverables covering generic security aspects.

When designing new architectures, security must be built in from the beginning - not patched on later. TC TISPAN established the security requirements for the subsystems of Next Generation Networks [1] in its first version (NGN Release 1) of the general network and service specifications for the convergence between the traditional public switched telephone networks (PSTNs) and the new IP-based networks. The challenge of security in Next Generation Networks was addressed with an analysis of risks and threats [2] and by defining an extensible NGN security architecture [3] (latest revision published in 2009).

In addition, TC TISPAN has produced a set of Security Design Guides ([4], [5] and [6]) which should be followed in the design of any new component of the network. This work references the guidelines on the use of the Common Criteria for the evaluation of IT security (ISO/IEC 15408), which primarily address the protection of information from unauthorised disclosure, modification or loss.

The publications deal with the issue of the application of the Common Criteria framework in the ETSI standardisation process and the development of protocols and architecture standards [6]. They describe the way to map the Common Criteria framework drivers onto the process of defining a new standard, from the *a priori* definition of the purpose, the environment and the acceptable level of risk, to the actual definition of the subsystems, modules and protocols that constitute the standard.

TISPAN has also published an ETSI Guide on the application of security countermeasures to service capabilities [7], an analysis of security mechanisms for customer networks connected to TISPAN NGN Release 2 [8], a feasibility study on Media Security in TISPAN NGN [9], a NAT traversal feasibility study report [10], a feasibility study on the prevention of unsolicited communication in NGN [11], a report on the security of identity in NGN [12], and a report on the application of ISO 15408-2 requirements to ETSI standards (method and application with examples) [13].

A TR was published in 2009 providing guidance on the use of the ETSI eTVRA (electronic Threat Vulnerability and Risk Analysis) web application ([14]), which acts as a tool for entering analysis results obtained through the ETSI TVRA method defined in [15].

Current work on Cybersecurity matters within the ETSI TC TISPAN focuses on security issues emergency communication from citizen to authority within the NGN architecture, a feasibility study on IPTV security architecture, the development of a schematic overview of the NGN security architecture, a TS on how to counteract the occurrence of Unsolicited Communications (UC) in NGN, and a TS on the provision of countermeasures to assure that users of the NGN are protected from abuse of identity.

During 2009, ETSI has started to work on RFID security and privacy “by design” for the NGN, in response to the European Commission's RFID Mandate (Mandate M/436, published December 2008). In the envisaged context that RFID will be the “gateway” technology for the future “Internet of Things” (IoT), this mandate stresses the related crucial security and privacy aspects, and encourages the European Standards Organisations (ESOs) to perform the relevant standardisation work. The work in ETSI on this Mandate is being carried out in cooperation with the other ESOs: CEN and CENELEC.

A very important Cybersecurity area of work in ETSI is Lawful Interception (LI), together with Data Retention (DR). For the future NGN, TC TISPAN has identified appropriate interfaces, reference points and entities in the NGN architecture through the Technical Specification (TS) [16] and has published a Technical Report (TR)

[17] providing guidance on compliance to the data retention directive (explained in more detail below).

With regards to the existing global network infrastructure in use, ETSI has played a leading role in LI standardisation since 1991; today the work is concentrated in Technical Committee Lawful Interception (TC LI), which has the active participation of the major telecom manufacturers, network operators and regulatory authorities of Europe and from around the world. Lawful Interception (LI) is the legally authorised process by which a network operator or service provider gives law enforcement officials access to the communications (telephone calls, e-mail messages etc) of private individuals or organisations. Lawful Interception is becoming crucial to preserve national security, to combat terrorism and in the investigation of serious criminal activities

The standardisation of Lawful Interception is vital to provide an economically and technically feasible solution that complies with national and international conventions and legislation.

ETSI's LI work covers the whole spectrum of interception aspects, from a logical overview of the entire architecture and the generic intercepted data flow, to the service-specific details for e-mail and Internet, and the requirements of law enforcement agencies. In the recent years TC LI has intensified its efforts with regards to standardisation of retained data.

A major achievement of ETSI's work in this area has been the publication of the specifications for the handover procedure: TS 101 671 [18] and ES 201 671 [19]. These specifications illustrate the flow that the intercepted data should follow in telecommunication networks and services. In this context, they specify the network or service protocols necessary to provide lawful interception, as well as the physical or logical point at which the interception has to take place (the handover interface) both for packet data and circuit-switched communications.

Other ETSI Technical Committees have also produced other important specifications on Lawful Interception. TC LI therefore works in close collaboration with those committees, notably TC TISPAN, as well as TC TETRA (Terrestrial Trunked Radio), 3GPP and TC ATTM (Access, Terminals, Transmission and Multiplexing) ([20] to [21]).

The LI handover specifications are already widely used in a number of countries, being first adopted in 2003. Other countries are in the process of implementation or have expressed an interest in adopting them.

ETSI TC LI has standardised the general requirements of network operators, service providers and access providers [22] who are obliged to make available results of interception to the law enforcement agencies. Complementing these requirements, a Technical Specification [23] relating to handover interfaces for the interception provides guidance for law enforcement agencies on the co-operation required by network operators/service providers with the lawful interception of telecommunications.

The specifications are subject to regular review and updating within ETSI to accommodate emerging needs, and are being used as the basis for specifying the procedures for LI. The increasing trend in the use of packet-switched technologies has necessitated the production of standards for the delivery of IP-based interception. As a result, since LI has to be possible on several specific services that make use of the IP framework, a multi-part ETSI TS on the ‘Handover Interface and Service-Specific Details (SSD) for IP delivery' has been published. This currently contains seven parts:

- part 1: Handover specification for IP delivery [24]
- part 2: SSD for e-mail services [25]
- part 3: SSD for Internet access services [26]
- part 4: SSD for Layer 2 services [27]
- part 5: SSD for IP Multimedia Services [28]
- part 6: SSD for PSTN/ISDN services [29]
- part 7: SSD for Mobile Packet Services [30]

Several versions have been published of an ETSI Technical Report (TR) on Abstract Syntax Notation version 1 (ASN.1) Object Identifiers in Lawful Interception Specifications, which focuses on the ASN.1 tree structure of the security domain [31].

Two other TRs, published in 2006, cover Lawful Interception of public Wireless LAN Internet Access [32] and the Lawful Interception domain architecture for IP networks [33].

TC LI has produced a TR ([34]), which was published at the end of 2008, defining a security framework for securing Lawful Interception and Retained Data environment (see below) of the Communication Service Provider *(*CSP) and the Handover of the information.

ETSI organised two Plugtests™ events for TC LI in order to test the interoperability of equipment from different vendors against a number of TC LI specifications. During the first LI Plugtests™ event in 2006, the following TSs were tested: [24], [25], [26]. During the second LI Plugtests™ event in 2007, the following TSs were tested: [18], [24], [25], [28], [29]. The outcome of both events highlighted issues which were looked after by the TC LI through a number of updates to the relevant publications.

Data Retention is another vital subject for TC LI. The ability for Law Enforcement Agencies to request, and for operators and service providers to deliver, retained data are requirements of European Directive 2006/24/EC on the retention of data. TC LI has produced a TS [38] which deals with the requirements from Law Enforcement Agencies for the handling of Retained Data (RD). This document gives guidance for the delivery and associated issues of retained data of telecommunications and subscribers. It provides a set of requirements relating to handover interfaces for the retained traffic data and subscriber data by law enforcement and state security agencies and other authorised requesting authorities.

TC LI's work on Retained Data has been intense, and is now widely recognised worldwide. At the end of 2008 a Technical Specification was published ([39]) which standardises the Handover Interface (HI) for the request and delivery of retained subscriber and traffic data from a Network Operator, an Access Provider or a Service Provider (NWO/AP/SvP) to the Requesting Authority.

TC LI continues to maintain the suite of Lawful Interception and Data Retention publications by updating them regularly. In 2009 work started on a new TS providing a standardised mechanism for the dynamic triggering and revocation of the interception of communications content. This involves important security aspects, as the dynamic triggering functions need to be carried out with adequate levels of security to protect them from misuse or eavesdropping of the related commands. It is also essential that the triggering interface does not impact the underlying security of the network or services being intercepted. The publication of this TS is expected in 2010.

3. ETSI's OTHER AREAS OF WORK

ETSI's other main areas of work related to security cover Mobile/Wireless Communications, Emergency Telecommunications, Information Technology Infrastructure, Smart Cards, Fixed Communications and Security Algorithms. The table below provides a fully comprehensive list of **ETSI Technical Committees and Partnership Projects**

3GPP	Third Generation Partnership Project
MESA	Mobility for Emergency and Safety Applications (partnership project)
AERO	Aeronautics
ATTM	Access, Terminals, Transmission and Multiplexing
BROADCAST	Joint TC on broadcasting matters
DECT	Digital Enhanced Cordless Telecommunications
EMTEL	Special Committee on Emergency Telecommunications
ERM	Electromagnetic Compatibility and Radio Spectrum Matters
ESI	Electronic Signatures and Infrastructures
ITS	Intelligent Transport Systems
LI	Lawful Interception
M-COMM	Mobile Commerce (closed TC)
MSG	Mobile Standards Group
MTS	Methods for Testing and Specification
QKD (ISG)	Quantum Key Distribution (Industry Specification Group)
RRS	Reconfigurable Radio Systems
RT	Railways Telecommunications
SAGE	Security Algorithms Group of Experts
SCP	Smart Card Platform
SES	Satellite Earth Stations and Systems
SMG	Special Mobile Group (closed TC)
TETRA	Terrestrial Trunked Radio
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking

4. ETSI SECURITY WHITE PAPER

The ETSI Security White Paper outlines ETSI's work in each of the security-related fields. A complete list of the relevant publications for each field is included at the end of this document, freely downloadable from the ETSI website:

www.etsi.org/SECURITYWHITEPAPER

5. ETSI SECURITY WORKSHOPS

Each year, in January, ETSI organises a Security Workshop in its premises, attracting a large number of experts from all over the world. This event provides valuable co-operation opportunities, and helps set the direction for future standardisation work, in line with the requirements of ETSI Members. In recent years the discussions have focused increasingly on the broad issue of security innovation, and the role that security standards can and should play in such context. ETSI continues to intensify its focus on matters related to security innovation by participating actively in EU security research and innovation initiatives which aim to provide Europe, and the rest of the world, with the tools necessary to create a secure environment for the global citizen.

ETSI Security Workshops regularly feature many expert speakers, representing organisations that typically include ETSI, CEN, CENELEC, European Commission, ENISA, ITU-T, ISO, NIST as well as the private sector, governments, universities and research bodies, including the European Commission's Joint Research Centre.

The 5th ETSI Security Workshop (focusing on Security Innovation) took place on 20-22 January 2010 in the ETSI premises in Sophia Antipolis, France. Information about this workshop as well as previous and future planned ETSI Security Workshops, together with the summary reports and presentations for download are available from the ETSI website:

www.etsi.org/SECURITYWORKSHOP

The **6th ETSI Security Workshop** will be held again in Sophia Antipolis, France, on **19-20 January 2011**.

6. CONCLUSIONS

The confidence of the citizen in security in broad terms is crucial in a highly networked global environment. Working together is vital in our global efforts for a secure world, in order to share ideas, optimise resources and avoid duplication of work. Cooperation among Standard Developing Organisations (SDOs) and any stakeholders is strongly needed and has to be encouraged on a global scale. SDOs need to take on the Cyber threats challenge by strengthening their cooperation with governments, industry, academia, research bodies and end users' groups. This paper highlights that ETSI, the European Telecommunications Standards Institute, is a key player of the global Cybersecurity efforts, by addressing security issues in a broad number of areas within its Technical Bodies.

7. REFERENCES

[1] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[2] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat, Vulnerability and Risk Analysis".

[3] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[4] ETSI ES 202 382: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".

[5] ETSI ES 202 383: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".

[6] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[7] ETSI EG 202 549: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Design Guide; Application of security countermeasures to service capabilities".

[8] ETSI TR 185 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Analysis of security mechanisms for customer networks connected to TISPAN NGN R2".

[9] ETSI TR 187 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study on Media Security in TISPAN NGN".
[10] ETSI TR 187 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NAT traversal feasibility study report".
[11] ETSI TR 187 009: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN".
[12] ETSI TR 187 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity management and their resolution in the NGN".
[13] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".
[14] ETSI TR 187 014: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); eSecurity; User Guide to eTVRA web-database".
[15] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".
[16] ETSI TS 187 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 2 Lawful Interception; Stage 1 and Stage 2 definition".
[17] ETSI TR 187 012: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report and recommendations on compliance to the data retention directive for NGN-R2".
[18] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".
[19] ETSI ES 201 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".
[20] ETSI EG 201 781 (TC SPAN): "Intelligent Network (IN); Lawful interception".
[21] ETSI TS 101 909-20-2 (AT Digital): "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services".
[22] ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".
[23] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".
[24] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".
[25] ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for E-mail services".
[26] ETSI TS 102 232-3: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services".
[27] ETSI TS 102 232-4: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services".
[28] ETSI TS 102 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services".
[29] ETSI TS 102 232-6: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services".
[30] ETSI TS 102 232-7: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services".
[31] ETSI TR 102 503: "Lawful Interception (LI); ASN.1 Object Identifiers in Lawful Interception Specifications".
[32] ETSI TR 102 519: "Lawful Interception of public Wireless LAN Internet Access".
[33] ETSI TR 102 528: "Lawful Interception (LI) Interception domain Architecture for IP networks".
[34] ETSI TR 102 661: "Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment".
[35] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".
[36] ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for E-mail services".
[37] ETSI TS 102 232-3: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services".
[38] ETSI TS 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".
[39] ETSI TS 102 657: "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".