ETSI White Paper No. 1

ISBN No. 979-10-92620-05-4

Security for ICT - the work of ETSI

7th edition – June 2015

Authors:

Carmine Rizzo (ETSI)

Charles Brookson (Zeata Security and Azenby)

ETSI (European Telecommunications Standards Institute)
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

About the authors

Dr. Carmine Rizzo, CISA CISM CMP ITIL PRINCE2

ETSI Security Standardization Projects, ETSI Secretariat

Carmine Rizzo has worked in the ETSI Secretariat in France since November 2007. He is the point of reference for security standardization activities and responsible for the supervision, coordination and promotion of ETSI security standardization work within and across various Technical Committees and Working Groups.

He obtained a Masters Degree in Electronic/Telecommunication Engineering in Italy, followed by a Ph.D. in Radio Communications in the United Kingdom.

His professional background in the United Kingdom includes experience in the private sector for Nortel Networks as Data Communications Network Engineer, and over five years' experience in the international organization ECMWF (European Centre for Medium-range Weather Forecasts), working in an operational environment for the management of IT projects, services and security.

He has gained, and actively maintains, several professional certifications covering broad aspects of technical security and security management, as well as project management, change management, IT audit, control, and service management.

Charles Brookson, OBE CEng FIET FRSA M.Inst.ISP

Director Zeata Security Ltd and Azenby Ltd.

Charles Brookson worked in the UK Department for Business Innovation & Skills (BIS) for 12 years and is a Professional Electronic Engineer. He previously was Head of Security for one2one (now T-Mobile UK) for four years, and worked within British Telecom for twenty years before moving to one2one.

He is chairman of ETSI OCG Security, which is responsible for security standardization within ETSI, chaired the GSM Algorithm Group in 1986, and has been Chairman on the GSM Association Security Group (representing nearly 800 operators in 220 countries) for over 25 years, and has been involved in GSM and 3GPP security standards during this time. He was also on the Permanent Stakeholders group of ENISA, the European Network and Information Security Agency.

He is now a Director of Zeata Security Ltd and Azenby Ltd which offers consultancy in the mobile sector.

In 2015 Charles Brookson was awarded an OBE (Officer of the Order of the British Empire) for his services to telecommunication security.

Security for ICT - the Work of ETSI

June 2015

This White Paper offers an overview of ETSI's work on security in Information and Communications Technologies (ICT).

Each section introduces a specific technology and outlines ETSI's involvement in the standardization of security in that area. Some of our major achievements are then highlighted and ongoing activities are described. At the end of the paper, all ETSI's specifications and standards for security are listed. Listed documents referenced in the text are indicated by a number in [ ].

Each ETSI document number in the list of publications at the end of this paper links to the ETSI deliverable available online, from where the latest published version at the time of your search can be downloaded, as well as any previous versions.

This seventh edition of the ETSI Security White Paper updates all areas as necessary. New publications have been added, while a large number of previously referenced publications have undergone revision and now have updated versions.

Contents

Foreword

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 minimize exposure to risks, security must be built in from the beginning when designing new architectures, not added on later as an optional feature.

In the past few years threats to ICT in general have expanded and security has moved on apace, with areas such as cybersecurity, cloud, mobile, the Internet of Things producing more requirements. We have seen demands placed by the growing threat of criminal activities and risks to critical infrastructure. Sensitivity towards the privacy of the citizen and of his data is increasing with media exposure of insecure Governments businesses, but is lagging behind the rollout of new services and applications which depend on a culture of openness and sharing.

As a response to such challenges, security standards are essential to ensure interoperability among systems and networks, compliance with legislation 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 organizations, research bodies and universities.

ETSI is an independent, non-profit organization, with 25 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 is committed to the establishment and continuous improvement of effective and interoperable telecommunications systems for the benefit of the global community. Addressing security issues in all ICT areas, protecting citizens in emergency scenarios, and combating global climate change by lowering power consumption are examples which highlight some of ETSI's commitments. 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.

Standardization activities carried out within various ETSI Technical Committees, Working Groups, Industry Specification Groups and Partnership Projects cover a broad spectrum of security issues, of which this White Paper provides an overview.

Carmine Rizzo, ETSI Security Standardization Projects, ETSI Secretariat

Charles Brookson, Chairman, ETSI TC CYBER Chairman

Acknowledgements

I would like to thank the following persons whose contributions have been essential to this work:

- Charles Brookson, for the benefit of his incredibly deep knowledge and experience in the vast security arena and related ETSI work: thanks for verifying the completeness and accuracy of this document;
- Ultan Mulligan for his help with the editorial content;
- For their precious and indispensable inputs and contributions, colleagues within and outside the ETSI Secretariat: Steve Babbage, Chantal Bonardi, Scott Cadzow, Sonia Compans, Francois Ennesser, Andrea Lorelli, Sebastian Müller, Marcello Pagnozzi, Xavier Piednoir, Mirko Cano Soveri, Antoinette van Tricht, Laurent Velez and Milan Zoric.

Carmine Rizzo

Introduction – the organization of work in ETSI

ETSI's work is organized 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, have a much broader scope, but necessarily deal with security issues in the process of producing a complete set of standards for a technology.

The main areas of work at ETSI related to security cover mobile/wireless communications, emergency telecommunications, information technology infrastructure, smart cards, fixed communications and security algorithms and underpinning this is important work on security design and analysis methods. Some TCs work specifically within one of these areas, whereas the work of other TCs can overlap several areas.

This complex and dynamic scenario creates a need for a reference group to both create security standards and coordinate security matters across the ETSI work areas. For this reason ETSI has created TC CYBER, with responsibilities for cyber security standardization, while at the same time inheriting the former role of the Operational Coordination Group on Security (OCG SEC), which was then closed.

ETSI is intensively working in the Network Functions Virtualisation domain, for which security aspects are of crucial importance.

This 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, followed by the reference numbers of the documents added since the sixth edition of the ETSI Security White Paper published in January 2014.

Key to ETSI Technical Committees (TCs) / Partnership Projects (PPs) / Industry Specification Groups (ISGs)

3GPP (PP)	Third Generation Partnership Project
MESA (closed PP)	Mobility for Emergency and Safety Applications
AERO	Aeronautics
ATTM	Access, Terminals, Transmission and Multiplexing
BROADCAST	Joint TC on broadcasting matters
CABLE	Integrated broadband cable telecommunication networks
CYBER	Cyber Security
DECT	Digital Enhanced Cordless Telecommunications
E2NA (closed EP)	End to End Network Architecture
EMTEL	Special Committee on Emergency Telecommunications
ERM	Electromagnetic Compatibility and Radio Spectrum Matters
ESI	Electronic Signatures and Infrastructures
INS (closed ISG)	Identity and Access Management for Networks and Services
ISI (ISG)	Information Security Indicators
ITS	Intelligent Transport Systems
LI	Lawful Interception
MSG	Mobile Standards Group
MTS	Methods for Testing and Specification

NFV (ISG)	Network Functions Virtualisation
NTECH	Network Technologies
oneM2M	Machine to Machine
QKD (ISG)	Quantum Key Distribution (Industry Specification Group)
QSC (ISG)	Quantum-Safe Cryptography (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
Smart M2M	Machine to Machine
SMG (closed TC)	Special Mobile Group
TCCE	TETRA and Critical Communications Evolution
TISPAN (closed TC)	Telecommunications and Internet converged Services and Protocols for Advanced Networking

ETSI Security Week

Following the highly successful series of annual Security Workshops, ETSI expanded the event to extend the Security Workshop with more focused thematic streams, to provide more time for networking and offer opportunities for ETSI security-related committees to hold meetings which all delegates may attend.

This week is an ideal opportunity to learn about the full extent of ETSI's security related standardization, as well as to foster debates and discussions with security experts from many other organizations, which help shape the future direction of ETSI's security related standardization.

www.etsi.org/SECURITYWEEK

Mobile and Wireless Telecommunications

Mobile and wireless technologies are enormously flexible. Beyond the well-known and widespread commercial use (e.g. cellular telephones, wireless networks and cordless home telephones), applications include public safety and military communications.

The wireless infrastructure that terminals use to access the network makes these technologies vulnerable to attack. Over the years, ETSI has developed a unique expertise in securing these forms of communication, providing encryption techniques and fraud prevention mechanisms.

ETSI's standardization work includes various mobile and wireless technologies.

GSM™ - background and achievements

Shortly after its creation in 1988, ETSI took over the task of specifying GSM from the European Conference of Posts and Telecommunications Administrations (CEPT). In 2001, GSM standardization was transferred to the Third Generation Partnership Project (3GPP™), which ETSI helped to found to develop globally applicable specifications in the mobile telecommunications area. A new Technical Specification Group (TSG GERAN) was created within 3GPP to handle the GSM-specific radio aspects. Responsibility for standards specifically for regulatory use remains with ETSI's Mobile Standards Group (TC MSG).

Standardization of GSM has continued relentlessly, bringing enhancements to the basic GSM technology, as well as its evolution to more advanced technologies such as the General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution (EDGE). Although GSM can offer a basic data service, these newer technologies have introduced users to practical mobile data and multimedia services, dramatically extending the reach of the Information Society to all peoples of the world and helping to resolve the "Digital Divide".

Security has been a major driver for the success of GSM. Specifications have been developed to prevent terminal equipment theft, allow encryption and authentication, control payment for copyright material downloading and respond to many other security threats. The general description of the security functions can be found in [57].

Standardization work related to specific security aspects of GSM is currently being carried out within ETSI's Railways Telecommunication committee (TC RT) and within the joint ETSI ERM/MSG group.

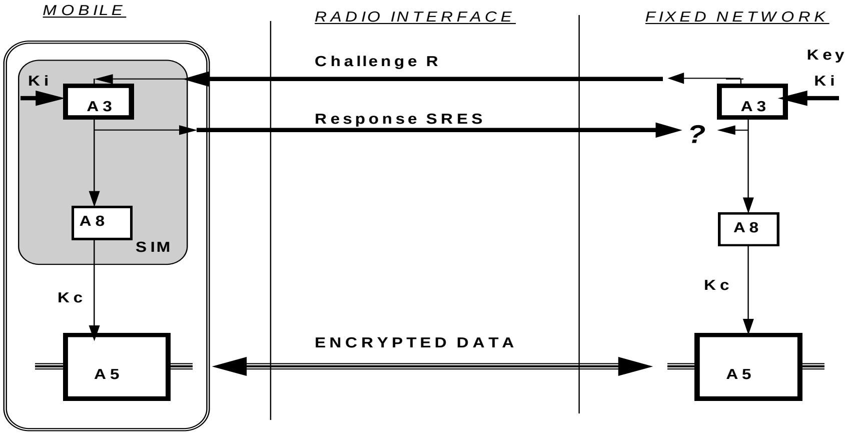
The major characteristics of security in GSM are described below.

Anonymity - Anonymity entails preventing the tracking of the location of the user and preventing the identification of calls made to or from the user by eavesdropping on the radio path. Anonymity in GSM and UMTS is provided by using temporary identifiers when the feature is activated by the operator. When a user first switches on his mobile device, the real identity is used and a temporary identifier is then issued. From then on, the temporary identifier is used, until such time as the network requests the real identity again. Only by tracking the user is it possible to determine the temporary identity being used (see [25], [66], [74] and [75]).

Authentication and Signalling Protection - Authentication is used to identify the user (i.e. the holder of a Subscriber Identity Module (SIM) card) to the network operator and is based on encryption.

ETSI has developed three security algorithms for GSM: A3, A5 and A8. The A3 and A8 algorithms are specific to the operator and are saved on the SIM card and in the authentication centre. A5 is saved in the mobile equipment and allows for data encryption and decryption over the radio air interface.

Authentication is performed by a challenge and response mechanism. A random challenge is issued to the mobile, the mobile encrypts the challenge using the authentication algorithm A3 and the key assigned to the mobile, and sends a response back. The operator can check that, given the key of the mobile, the response to the challenge is correct. Eavesdropping on the radio channel reveals no useful information, as the next time a new random challenge will be used. More specifically, the procedure is as follows: a random number (R) is generated by the network and sent to the mobile. The mobile uses the random number as the input to the encryption and, using a secret key (Ki) unique to the mobile, transforms this into a response (SRES) which is sent back to the network. The network can check that the mobile really has the secret key by performing the same process and comparing the responses with what it receives from the mobile. The response is then passed through an algorithm, A8, by both the mobile and the network to derive the key (Kc) used for encrypting the signalling and messages to provide privacy (A5 series algorithms). The process can be represented graphically as follows (see also [60] to [63]):



IMEI - Mobile terminals are by their nature attractive objects, at great risk of theft, often described by the acronym CRAVED (Concealable, Removable, Available, Valuable, Enjoyable and Disposable). ETSI has created a set of standards (see [65] and [66]) which define a system to prevent handset theft, based on a handset identity number called the International Mobile Equipment Identity (IMEI). This is a unique number attributed during handset manufacturing, registered by the Mobile Network Operator (MNO) and implemented into the mobile terminal. Using the IMEI, mobile equipment declared as stolen can be blacklisted by the MNOs.

IMEI blacklisting is currently in operation, though not yet on a world-wide basis; stolen phones often leave their original country for less developed countries where people cannot afford the price of a new handset. To use the handset in the same country it has been stolen in, the IMEI value can also be changed to an authorized one. To reduce handset theft, some countries have passed laws that make IMEI alteration illegal. In parallel, handset manufacturers are working on increasing the IMEI's security.

The IMEI offers other benefits too: for example, certain handsets can be tracked by the network for evaluation or other purposes. The IMEI is also useful for identifying makers of hoax emergency calls.

FIGS - Fraud Information Gathering System (FIGS) is a method of monitoring a subscriber's activities to limit the accumulation of large unpaid bills whilst roaming (see [1], [5], [14], [16] and [54]). FIGS allows the network that roaming subscribers are entering to collect information about their activities. The network then sends this information back to the home network of the subscriber, which can then clear certain types of calls and prevent fraudulent use of the system (see [6] and [10]).

Priority - GSM specifications include a public safety service called Priority (see [68], [69]). This allows users of the appropriate category (typically the emergency services, government agents and the military) to obtain high priority access to network services in crisis conditions, when there is a danger of overloading a potentially impaired network.

GSM™ - current work

The current standardization work carried out within ETSI related to the GSM technology includes several specific application areas, notably GSM onboard aircraft, GSM for automatic emergency calls from vehicles and GSM for railway telecommunications.

GSM onboard aircraft (GSMOBA) - GSM onboard aircraft has been developed and standardized by the joint ETSI group ERM/MSG GSMOBA, established in 2006. The European Harmonized Standard for GSMOBA (EN 302 480) was published in April 2008 [78]. GSMOBA addresses major security concerns, the main ones being related to causing interference to ground networks. To make effective use of the spectrum in terrestrial networks, these need to be protected from interference originating from installations and GSM terminals on aircraft flying above.

The GSMOBA group has devised means to prevent such communications between terrestrial networks and handheld terminals on aircraft, thus making communication from aircraft-located terminals possible only via aircraft-located base stations. This is achieved raising the RF noise floor within the cabin to such a level that neither interference nor communication with ground networks is possible. In future, the GSMOBA concept may be expanded to UMTS/LTE (Long Term Evolution) technologies. ETSI White Paper No. 4 provides more information.

GSM eCall - The term "eCall" refers to automatic emergency calls from vehicles and other eCall-equipped devices in case of a crash or other catastrophic event. This work has been ongoing in ETSI TC MSG since 2004, and relies on analysis and definition of requirements from 3GPP. eCall is expected to be GSM-based in its first deployment, although successive extensions to UMTS and LTE are foreseen.

GSM Direct Mode Operations (DMO) - DMO (Direct Mode Operation) features of GSM are being developed in ETSI TC RT for use in a variant of GSM for railway operators, known as GSM-R. The DMO features constitute an extension of GSM, allowing terminals with DMO functionality to communicate directly with each other without having to rely on a background telecom network infrastructure. In areas without GSM (or GSM-R) coverage, e.g. unpopulated areas, tunnels or during major breakdown of the underlying GSM infrastructure, track maintenance personnel and the like would still be able to communicate in simple terminal-to-terminal direct mode.

The addition of such functionality to GSM terminals is not trivial, due especially to spectrum regulation and spectrum management issues, as the GSM spectrum is licensed, and its utilization needs to be controlled by GSM (and GSM-R) operators. Properly controlled and authorized DMO demands a series of security considerations essential to the safe operation of railways in case of network breakdown. The DMO working group within TC RT is addressing these requirements.

UMTS™

Development of specifications for the 3rd Generation Universal Mobile Telecommunication Systems (UMTS) is the task of a partnership project known as 3GPP, of which ETSI is a founding partner. 3GPP brings ETSI together with five other regional standardization organizations in Asia and the USA, plus organizations representing market interests and several hundred individual companies. 3GPP is also responsible for the maintenance and evolution of the specifications for GSM, and for transitional technologies such as GPRS and EDGE.

The UMTS security specifications developed in 3GPP build on the mechanisms used in the GSM specifications. In addition, they offer numerous enhancements that include the following:

Authentication - To further enhance the security already present in GSM, 3GPP has adopted an innovative authentication and key agreement protocol for UMTS. The protocol retains the framework of the GSM authentication mechanism and provides additional features such as mutual authentication, agreement on an integrity key between the user and the serving network, and freshness assurance of agreed cipher key and integrity key. As in the GSM authentication mechanism, the serving network authenticates the user by using authentication data (called authentication vectors) transferred from the user's home network. In each authentication vector, a protected sequence number is included, verified by the terminal's smart card (USIM) to achieve authentication of the network by the user. There are also mechanisms for freshness assurance of agreed cipher and integrity keys (see [28], [29], [30], [31], [34], [38], and [41]).

Public Safety - 3GPP has invested significant effort in ensuring that emergency calls in UMTS are always connected and has introduced various public safety functionalities.

Location services are also an important feature (see [70] to [73]). Several techniques have been specified to improve the accuracy of the positioning, from the simple retrieval of the radio cell where the mobile is located to the more advanced, assisted GPS positioning. In the specification work, several ancillary aspects related to location services have been addressed such as privacy protection for the users and when there is a need for public authorities to trace mobile phones.

3GPP has also been working to enhance the capabilities of cell broadcast services to introduce the MBMS (Multicast Broadcast Multimedia Service) (see [33]). This enables MNOs to transmit multimedia content to a selected area of the mobile network, a feature of particular value when the need arises to issue public warnings.

In 2012, SAGE announced its intention to develop a new 3G authentication and key agreement algorithm set, as an alternative to MILENAGE. This new algorithm set, named TUAK (see the Algorithms section), can be used by any operator for any USIM (Universal Subscriber Identity Module) or ISIM (IMS (IP Multimedia Subsystem) Subscriber Identity Module). This provides options to operators as well as resilience against future cryptanalysis of either algorithm set.

At the end of 2013 3GPP SA3 agreed to adopt this second algorithm set for the 3GPP authentication and key generation functions, which include the algorithm specification itself, the implementers' test data and the design conformance test data.

Three new specifications were approved to gather this information:

- Algorithm specification [86]
- Implementer's test data [87]
- Design conformance test data [88].

LTE™

LTE™ is a major advance in the evolution of 3GPP radio interfaces to deliver global mobile broadband, derived from a plan first conceived in 2004. It has significantly increased data throughput with a downlink target 3-4 times greater than HSDPA (High Speed Downlink Packet Access) Release 6, and an uplink target 2-3 times greater than HSUPA (High Speed Uplink Packet Access) Release 6. The complementary core network upgrade, Evolved Packet Core (EPC), focuses on an enhancement of Packet Switched technology to cope with rapid growth in IP traffic, (i.e. higher data rates, lower latency and packet optimized systems), through fully IP networks with simplified architecture and distributed control.

LTE forms the basis of 3GPP Release 8, functionally frozen in December 2008. The security architecture was defined by the 3GPP Services and System Aspects Working Group on Security, SA3.

Authentication and key agreement are based on UMTS AKA (Authentication and Key Agreement) which is re-used for Evolved Packet Systems (EPS). Subscriber Identity Module (SIM, as used in GSM) access to LTE is explicitly excluded and only Release 99 or later Universal Subscriber Identity Modules (USIMs) are allowed.

As far as signalling protection is concerned, core network signalling (Non-Access Stratum (NAS)), integrity and confidentiality protection terminates in the Mobility Management Entity (MME). Integrity and confidentiality protection for the radio network signalling (Radio Resource Control, RRC) and for the MME is maintained over the radio path, i.e. between the UE (User Equipment) such as a mobile terminal and the eNode B (the base station in the LTE technology), as is the encryption for the User plane protection. Network domain security is used to protect the internal interfaces.

Two sets of security algorithms were developed for LTE: one set is based on AES (Advanced Encryption Standard) and the other on SNOW 3G. The principle being adopted is that the two should be as different from each other as possible, to prevent similar attacks being able to compromise them both. The ETSI Security Algorithms Group of Experts (SAGE) is responsible for specifying the algorithms. The key length is of 128 bits, with the possibility to introduce 256-bit keys in the future if necessary. In 2011 a third algorithm, ZUC, was approved for use in LTE (see section Algorithms). The encryption algorithm 128-EEA3, and the integrity algorithm 128-EIA3, based on ZUC, were finalized in 2012.

LTE enables efficient interworking with legacy and non-3GPP networks. In this scenario, trust models become more complex and a deeper key hierarchy than that used in UMTS is needed for LTE. A (one-way) Key Derivation Function (KDF) is used for LTE. The extended key hierarchy also enables faster intra-LTE handovers.

Interworking with non-3GPP networks is based on EAP-AKA and its revised version EAP-AKA', where the EAP (Extensible Authentication Protocol) server is the 3GPP AAA server residing in the EPC. The EPC provides a core network suitable for higher-data-rate, lower-latency, packet-optimized system that supports multiple Radio Access Technologies (RATs). EAP-AKA' is a small revision of the EAP-AKA method which comprises a new key derivation function that binds the keys derived within the method to the name of the access network, and employs SHA-256 instead of SHA-1 (SHA stands for Secure Hash Algorithm) In circumstances where the non-3GPP network is un-trusted, an IPSec tunnel is used.

Below is a comprehensive list of the documents completed recently:

- Machine Type Communications (MTC): feasibility aspects of the security for MTC (3GPP TR 33.868) and security aspects of enhancements for MTC [89]
- Security aspects of Public Warning System (3GPP TR 33.969), security features and mechanisms for protection against false base stations broadcasting false warning notifications
- Security aspects of various functions for Proximity Services (ProSe) [90]
- GCSE (Group Communication Enablers for LTE) security (3GPP TR 33.888) which positions LTE as technology for critical communications such as public safety, for which security for Group Communication (GC) is necessary
- Study on Security on Spoofed Call Detection and Prevention (3GPP TR 33.831), to provide guidance on the means to identify spoofed calls terminating in the Circuit Switched (CS) domain, whereby the call could have originated from either inside or outside of it.

Ongoing activities

Several studies were ongoing at the time of publication of this white paper:

- Normative work on the Security Assurance Methodology for 3GPP Network Elements with the objective to develop a Security Assurance Specification (SAS) for the MME network product class.
- Study on subscriber privacy to identify privacy requirements and risks, privacy risk mitigation approaches, and to provide privacy guidelines and/or best practices for classes of 3GPP functions and privacy protection. The overall goal of this study is to develop privacy guidelines that help in addressing privacy issue in future 3GPP specifications.
- Study on aspects of integration of Single Sign On frameworks with 3GPP networks, which aims to investigate the security aspects of interworking between the operator-centric identity management with the user-centric Web services provided outside of an operator's domain.
- Define security requirements and related solutions Mission Critical Push To Talk over LTE (MCPTT), an essential functionality of public safety communication systems
- Study on security issues to support Proximity Services (ProSe) and an evaluation of possible technical solutions needed to support such services.

HNB/H(e)NB

Access to 3G and evolved 3G Evolved Packet System (EPS) services may be provided via UMTS Terrestrial Radio Access Network (UTRAN) or Evolved UTRAN (E-UTRAN) cellular base stations used for domestic or commercial purposes. The EPS comprises the Evolved Packet Core together with the evolved radio access network. E-UTRAN is an evolution of the 3G UMTS radio access network towards a high-data-rate, low-latency and packet-optimized radio access network.

This type of access may be provided by the Public Land Mobile Network (PLMN) by means of elements referred to as Home Node B (HNB) and Home (e) Node B (H(e)NB). The H(e)NB provides services to a Closed Subscriber Group (CSG). CSG membership, including temporary membership, is managed by both the CSG manager and the network operator.

3GPP standardized Home Node B and Home eNode B technologies. From the security point of view, an important difference compared to a traditional UMTS or LTE architecture, is that while the Node B is an element traditionally owned and controlled by the operator, the Home (e) Node B resides in the customer's premises.

3GPP standardized the security architecture which specifies how networks using H(e)NBs can ensure an adequate level of security, and comply with regulatory requirements (see [80] to [82]). The threats that can occur from this change are collected in the 3GPP document TR 33.820, where the countermeasures are proposed.

A new feasibility study related to Public Safety has been completed recently: Feasibility Study on Security Aspects of Isolated E-UTRAN Operation for Public Safety (IOPS). Ensuring the continued ability of Public Safety users to communicate within mission critical situations is of the utmost importance, including when the fixed infrastructure is compromised. 3GPP will provide with the necessary security mechanisms for this isolated E-UTRAN scenario.

IP Multimedia Subsystem (IMS)

First defined by 3GPP as a core network feature dedicated to the handling of the signalling and user traffic flows related to multimedia applications, the IP Multimedia Subsystem (IMS) has since been recognized as having enormous potential for use in many different networks (mobile, fixed, cable TV etc.), particularly given the trend towards the convergence of such networks. An agreement for 3GPP to be the sole owner of the IMS specifications led to the concept of "Common IMS", i.e. a single IMS suite for all access networks maintained by 3GPP but contributed to by many ETSI TCs. This has resulted in a set of specifications defining the Core IMS and additional features, including Security, to satisfy the requirements coming from a variety of standardization bodies.

In this perspective the security requirements coming from ETSI TC TISPAN, CableLabs and 3GPP2 were inserted into the IMS specifications. More specifically, several new normative annexes have been added (see [27]):

- NASS (Network Access Subsystem) - IMS Bundled Authentication (NBA), which was a contribution by ETSI TC TISPAN;
- SIP Digest - based authentication, also a contribution by ETSI TC TISPAN;
- Access security with TLS (Transport Layer Security), which was a contribution by CableLabs;
- 3GPP2 Access, a contribution by 3GPP2.

A further annex illustrates the co-existence of authentication schemes. This annex explains how the disparate authentication mechanisms should be handled in IMS: Full IMS AKA, GIBA (GPRS-IMS Bundled Authentication), NBA, and SIP Digest.

In addition, IMS media plane security has been specified for real-time media [85]. The media plane can be protected end-to-access-edge using SDES (Session Description Protocol Security Descriptions for Media Streams). End-to-end media plane protection is also specified, either using SDES or using a Key Management Server (KMS). Rel-12 will extend the media plane security to cover IMS Messaging, IMS Conferencing and Communications Diversion.

In 2014 a report was published [91] on Security for Web Real Time Communication (WebRTC) access to IMS. A WebRTC IMS client is a WebRTC-capable browser running a JavaScript application that allows a user to access IMS services. The study focuses on the security mechanisms for authentication control and media plane.

Ongoing activities

Several studies were ongoing at the time of publication of this white paper:

- A new study on enhancements to WebRTC interoperability; the aim is to provide end-to-end support for specific WebRTC capabilities to reduce the need for protocol conversions between WebRTC and IMS protocols on the data channel
- New work on IMS call spoofing detection and prevention

Relay Nodes

E-UTRAN supports relaying by having a Relay Node (RN) wirelessly connected to an eNode B (eNB) serving the RN, called Donor eNB (DeNB), via a modified version of the E-UTRA radio interface.

Relay Node Security is addressed for Release 10 in Annex D of a specification [81], where a solution for Relay Node Security architecture and authentication is provided.

The basic idea behind the solution for RN security presented is achieving a one-to-one binding of an RN and a USIM called USIM-RN.

TETRA

ETSI Technical Committee TETRA and Critical Communications Evolution (TCCE) is responsible for maintaining and developing specifications for TErrestrial Trunked RAdio (TETRA), a mobile radio communications technology targeted primarily at public safety groups (such as the police and fire departments). Nevertheless TETRA has been - and continues to be - deployed in other traditional private/professional mobile radio (PMR) markets, such as transportation, utilities, industrial and public access mobile radio (PAMR), as well as in the military sector for peacekeeping and other activities, where fast and accurate field communications to and from a central office or dispatcher, as well as between the unit's members, are often critical.

The TETRA standards evolved to counter the interoperability problems of emergency response teams communicating with each other, due to the lack of standardization in their mobile radio equipment, and thus have created a common framework for digital radio in the private and emergency services domains. The mission-critical effectiveness and operational efficiency of TETRA as a wireless communications technology was demonstrated in the incident management resulting from a number of terrorist incidents across Europe (notably the Madrid railway bombings in 2004 and the London transport bombings in 2007), in the logistic support to the Games of the XXVIII Olympiad in Athens in 2004 and were key to the management of the Games of the XXX Olympiad in London in the summer of 2012.

Based on digital, trunked radio technology, TETRA was designed as the next-generation standard for the PMR and PAMR markets taking lessons learned from mobile radio, digital cellular telephony, paging and wireless data to offer a multi-user secure radio system for group-centric communication.

Fraud prevention and confidentiality are critical to the success of radio mobile systems such as TETRA because the air interface is open to being overheard or attacked if not protected. The security-related functions of the standard comprise the following features (see also [92], [93] and [94]):

Mutual authentication - With mutual authentication over the air interface, a mobile station can check if a network can be trusted before entering, and the TETRA system can control the access of a mobile station. This mechanism offers guarantees against an attacker penetrating the network, thus assisting in the prevention of fraud, Denial of Service (DoS) situations, spoofing and other forms of attack, while at the same time ensuring correct billing and access as well as a secure data distribution channel. In addition TETRA offers a Direct Mode Operation (DMO) where although an explicit authentication mechanism is not available, the use of strictly managed shared Static Cipher Keys can provide implicit mutual authentication.

Encryption - As the air interface is vulnerable to eavesdropping, encryption is crucial to maintain confidentiality of communications. Air interface security is intended to secure the connection between mobile stations and the network. In addition, end-to-end security can be provided to offer a higher level of security and is enabled in the TETRA standards. The use of several encryption algorithms, both standard and proprietary, is supported, with work started in 2012 to develop a migration to a new set of standard algorithms.

TETRA end-to-end security service is achieved by protecting information transmitted from one mobile station to another, not only over the air interface but also within the network. The technical solution can be customized to address particular requirements. As TETRA is implemented by diverse user groups for many purposes, this feature is essential.

Anonymity - Anonymity is achieved using temporary identities to identify the network nodes and encrypting these identities over the air interface. In addition, to counter traffic analysis attacks, each time an identity is transmitted, it is encrypted in a different way using a mechanism called TETRA Encrypted Short Identity, making it difficult to eavesdrop and identify active terminals.

Ongoing activities

The security requirements for the second release, high data rate TETRA, have been published and are in the process of review and maintenance as TETRA-2 systems are being deployed. In addition, as part of the ongoing maintenance required to ensure TETRA remains at the leading edge of security provisions with the move to a data-centric, rather than voice-centric, network, close liaison with 3GPP for the use of LTE as a complementary technology for public safety has been established and in which members of TETRA and 3GPP-LTE are working together to address adding group call capabilities and group security extension for LTE, as well as adding a public safety user capable direct mode to 3GPP-LTE.

DECT™

DECT (Digital Enhanced Cordless Telecommunications) is a flexible digital radio access standard for cordless communications in residential, corporate and public environments. The DECT standard makes use of several advanced digital radio techniques to achieve efficient use of the radio spectrum; it delivers high speech quality and security with low risk of radio interference and low power technology.

DECT standardization started in CEPT, and was transferred into ETSI at its creation in 1988. Work today is the responsibility of ETSI's DECT Technical Committee.

The major threats to cordless technologies are:

- impersonation of a subscriber identity
- illegal use of a handset
- illegal use of a base station
- impersonation of a base station
- illegal acquisition of user-related signalling information.

To combat these threats, the specifications include features which provide for:

- authentication of terminals
- data confidentiality
- user authentication.

As a contribution to DECT security, ETSI developed the DECT Standard Authentication Algorithm (DSAA) and the DECT Standard Cipher (DSC). Subsequently, DECT security has been increased with the introduction of two new security algorithms: DSAA2 and DSC2.

The combination of Time Division Multiple Access/Time Division Duplex (TDMA/TDD) digital radio technology and dynamic channel selection with additional encryption techniques, authentication and identification procedures makes DECT radio transmissions extremely secure against unauthorized radio eavesdropping by third parties.

For an overview of the security features in DECT see [99].

Ongoing activities

TC DECT is currently working on Ultra Low Energy (ULE). DECT Ultra Low Energy (ULE) is a very promising technology for the wireless machine-to-machine market segment. ULE keeps all the traditional strengths of the DECT technology: interference free, license free, high security (due to the recent introduction of stronger algorithms), secure authentication and long range.

Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is an almost ubiquitous method of storing and remotely retrieving small volumes of data for applications as diverse as stock control, ticketing and access control. The system is built from RFID tags (electronic devices that hold data) and RFID transceivers that read this data by querying the RFID tag over a radio link. Typically the tags are attached to an item and contain a serial number or other data associated with that item.

Security in RFID technology must prevent illicit tracking and cloning of tags. In addition, as RFID tags carry a relatively low amount of computational resources within the tag itself the use of standard cryptographic techniques is rendered unfeasible. Lighter encryption algorithms need to be created for the RFID tags.

In 2002, ETSI's Electromagnetic Compatibility and Radio Spectrum Matters Technical Committee (TC ERM) established a Task Group (ERM TG34) to produce deliverables for future RFID technologies and products. Two European Standards were published ([105] and [106]) and are updated regularly as necessary. A Technical Report providing guidelines for the installation and commissioning of RFID equipment at UHF was also published [107].

A number of recommendations for future work related to RFID security and promotion of "privacy by design" have been developed by the 3 ESOs (ETSI, CEN and CENELEC) in 2011 as a TR [108] published by TISPAN WG7. The future of this work is being actively pursued in a number of ETSI committees (TCs ERM TG34, Human Factors (HF) and the privacy by design guidance is being further developed in NTECH) in collaboration with partners in CEN.

ERM published a report [109] in 2011 on RFID Evaluation Tests. The report covers RFID Evaluation Tests that were carried out to evaluate the characteristics and performance of RFID equipment operating at their three principal frequencies of use. The information derived from these tests is directly relevant to the work on RFID security and privacy by design mentioned above [108].

Ongoing activities

Efforts are being made to obtain an extension of the UHF frequency band used by RFID technology. The enhanced band will serve a broader range of applications than just RFID, posing additional security issues which will need to be addressed within any future related standards.

Reconfigurable Radio Systems (RRS)

The creation of ETSI's Reconfigurable Radio Systems Technical Committee (TC RRS) was approved by the ETSI Board in September 2009. The TC is responsible for standardization activities in Software Defined Radio (SDR) and Cognitive Radio (CR). TC RRS has a Working Group (WG4) which focuses on the application of SDR and CR concepts to public safety.

TC RRS has produced a Technical Report which identifies and defines user requirements for RRS in the Public Safety and Defence domains [110].

Ongoing activities

TC RRS is working on the following documents.

- A Technical Report to identify security related use cases and threats in the deployment and operation of RRS. The following will be addressed:
- use cases and related security threats which may impact the services provision and availability of RRS networks and equipment;
- use cases and related security threats which may cause wireless interference to incumbent services;
- use cases and related security threats to the functionality of download and activation of software modules on RRS
- A Technical Specification to address security requirements for RRS, by identifying available countermeasures to security threats, as well as possible lack of such countermeasures.

Satellite

ETSI's Technical Committee on Satellite Earth Stations and Systems (TC SES) produces standards for satellite communication services and applications (including mobile and broadcasting), for earth stations and earth station equipment, especially the radio frequency interfaces and network- and user interfaces, and for protocols implemented in earth stations and satellite systems.

It is important that satellite networks are able to offer IP network services that remain comparable to and competitive with terrestrial services. These objectives require the development of satellite standards to keep pace with the rapid evolution of the terrestrial IP network standards.

TC SES has published two Technical Specifications and a Technical Report on network security ([111], [112] and [113]) in the area of broadband satellite multimedia services.

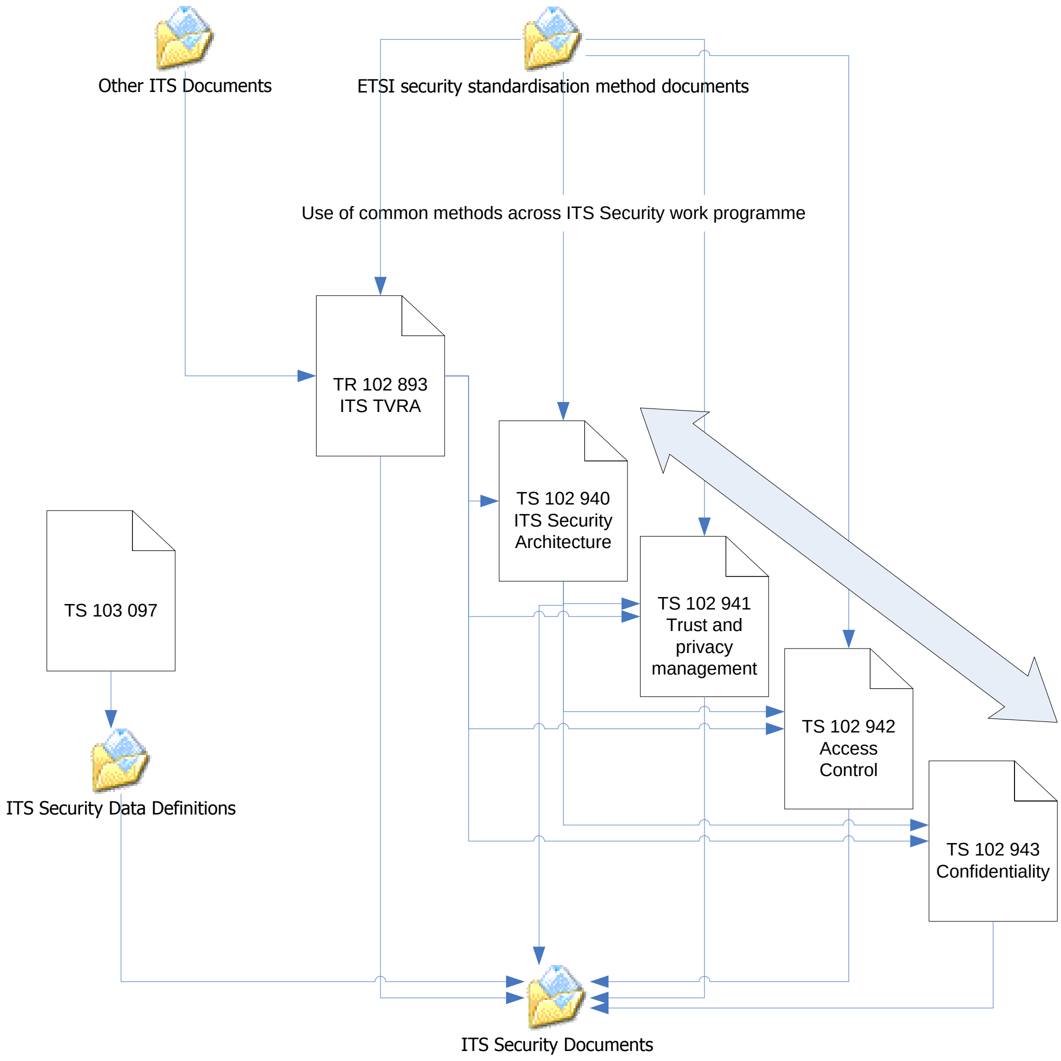
In addition, the committee's working group on geo-mobile radio interfaces, which is responsible for standards on radio interfaces for geostationary earth orbit satellite access to the core network of GSM, has undertaken work on the security of the interface and the services delivered through it ([114] to [116]). Similarly, another working group within TC SES has produced a Technical Specification for security aspects of the satellite component of UMTS [117]. The work of these two working groups was merged recently, and progress continues currently in TC SES.

Intelligent Transport Systems

Intelligent Transport Systems (ITS) concern the provision of services to improve the safety, reliability, efficiency, quality - and enjoyment - of transport. ETSI's Technical Committee on Intelligent Transport Systems (TC ITS) is responsible for the production and maintenance of standards to support the development and implementation of ITS communications and services across the network, for transport networks, vehicles and transport users.

TC ITS Working Group 5 addresses the security aspects in ITS. This group is developing and maintaining a suite of standards that are intended to enable secure inter-vehicle communication. The security features in ITS have been developed from a risk analysis following the method established in [335] and extended to address aspects of Privacy Impact Assessment (PIA) under the guidance published in [108].

The communications architectures and the services of ITS cover the range from ad-hoc all informed vehicle-to-vehicle scenarios, through lightweight vehicle-to infrastructure communication, to fully managed IP and Cellular networks. The security architecture overlaid on these communications architectures provides support to credential and identity management, privacy enhancing technologies and applications, integrity protection, authentication and authorization.



The primary aim of the current work in ITS at ETSI is to provide improved road safety through collaborative networking of vehicles. In this mode vehicles act as sensor nodes and broadcast their current position. A receiving vehicle can then calculate the speed and trajectory of all vehicles in the local vicinity and use the data alongside other data sources (e.g. road maps, weather data, current vehicle behaviour) as part of collision avoidance warning applications. The radio connection in this early ITS mode uses IEEE 802.11 technology operating at 5.9 GHz, offering low range but reasonably high data rates.

The nature of ad-hoc all-informed networks poses a number of difficulties in key distribution to enforce and validate assertions of identity or authority. The solution designed for ITS, in the absence of an always available public key infrastructure, has been to adopt and extend the IEEE 1609.2 public key certificates, and to take advantage of the capabilities of elliptical curve cryptography to allow both implicit and explicitly signed certificates and to then generate long sequences of "trusted" pseudonymous signing keys to protect transmitted data sequences from revealing long term private data. Thus PII (Personally Identifiable Information) is protected over long time durations restricting the risk of unauthorized tracking of vehicles whilst maintaining the viability of the core safety applications that require short term tracking of vehicles.

ETSI has agreed, along with other SDOs working in cooperative ITS (C-ITS), to adopt the IEEE 1609.2 data set and to profile it to the specific protocols developed at ETSI. This has been developed to date in a number of published documents including [118] representing a harmonized package of four TSs comprising ITS Security Architecture and Security Management, Trust and Privacy Management, Access Control and Confidentiality services in ITS communications [119], [120], [121], [122] (see the picture above showing how the ITS documents are structured and related to each other).

Throughout the development of this work close collaboration between IEEE and ETSI has been maintained.

One of the challenges in ETSI’s work in this area is to ensure global interoperability of the C-ITS capabilities with other ITS domains hosted in the same device (be it a vehicle, a smartphone, or embedded in roadside furniture). One of the areas being explored is ensuring a global data dictionary for the security capabilities, thus ETSI is working closely with IEEE, and with regulators in Europe and the US through the US-EU ITS Standards Harmonization Taskforce to have a single ASN.1 data syntax specification for ITS Security with further harmonization of the semantics and behaviour of protocols and services for security and privacy protection in the core ITS security deliverables.

Acceptance of ITS in the real world requires significant levels of pre-launch, pre-finalization, testing and verification of capabilities, therefore the development of Conformance Test Specifications was begun under the leadership of the ETSI CTI (Centre for Interoperability and Testing), and has been progressively developed to prepare deliverables that assure interoperability of devices produced in compliance with [126]. These Conformance Test Specifications have been integrated with the existing ITS Validation Framework [127] and have been published as a multipart TS, [123], [124] and [125].

Further work is being and will be continuously undertaken to demonstrate the viability of the standards through a series of ITS Plugtests^{TM} events, one of which was successfully carried out in November 2013, and by ongoing industry wide validation and verification events.

Machine to Machine (oneM2M - Smart M2M)

ETSI TC Machine-to-Machine (Smart M2M) specified a telecommunication technology-independent Service Layer offering a wide set of generic functionalities to facilitate the deployment of vertical M2M applications, such as Smart Metering, fleet management or remote healthcare monitoring applications. This work has now been consolidated internationally by ETSI and regional partner SDOs in the oneM2M Partnership Project. TC SmartM2M currently focuses on European Union initiatives, e.g. the security of energy infrastructures and the interoperability of smart appliances.

Achievements

TC M2M published its Release 1 deliverables in 2011. This specification was later contributed to provide a basic brick in the oneM2M Partnership Project established jointly by ARIB (Association of Radio Industries and Businesses, Japan), ATIS (Alliance for Telecommunications Industry Solutions, US), CCSA (China Communications Standards Association), ETSI, TIA (Telecommunications Industry Association, US), TTA (Telecommunications Technology Association, Korea) and TTC (Telecommunication Technology Committee, Japan), subsequently joined by TSDSI (Telecommunications Standards Development Society, India). The Release 2 of the ETSI specification is being maintained by ETSI TC SmartM2M, while the responsibility for the development of new features to support M2M and IoT was transferred to oneM2M. The specifications provide a range of standard mechanisms for mutual authentication, key agreement and optional secure connection establishment between the Service layers of the Devices/Gateways and the supporting M2M network infrastructure [128], [129] and [130]. Mechanisms are provided to distribute security credentials to M2M devices in a variety of manners (independent provisioning, derivation from pre-existing Access Network credentials, or independent infrastructure assisted bootstrapping), in order to adapt to the needs of very diverse M2M applications and underlying telecommunication technologies. The security of the M2M Service Layer may rely on the underlying Access Network provided mechanisms when trusted, on secure channel establishment at the M2M Service Layer (e.g. using TLS), or on data security provided at the object level. Release 2 brings enhancements of main security measures in underlying networks to enhance the protection of security information and facilitate its remote administration.

oneM2M published its Release 1 in January 2015. This includes a Security Solutions specification [131], supported by a Threat Analysis Technical Report, [132].

Ongoing activities

The further development of horizontal M2M specifications is now being pursued by ETSI within the oneM2M Partnership Project. While the scope of the security aspects of oneM2M Release 1 aims to address client-server based "one to many" industrial M2M deployments (with solutions similar to those addressed by ETSI SmartM2M), work is under way in the oneM2M Security Working Group to address, in future Releases, the complex challenges arising from distributed "many to many" dynamic IoT security scenarios.

TC Smart M2M also investigates the security aspects of European mandates related to Smart Energy, especially M/441 on Smart Metering and M/490 on Smart Grids, aiming at a harmonized security approach across European energy infrastructures.

Lawful Interception

Lawful Interception (LI) is the legally authorized 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 organizations. Lawful Interception is becoming crucial to preserve national security, to combat terrorism and in the investigation of serious criminal activities.

The standardization of Lawful Interception is vital to provide an economically and technically feasible solution that complies with national and international conventions and legislation. ETSI has played a leading role in LI standardization 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.

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 standardization of handover of retained data.

NOTE: Handover in the context of LI and RD (Retained Data) means the passing of data from the (Communication Service Provider) *CSP to the Authorized Organization (typically a Law Enforcement Agency (LEA)) and should not be confused with the term handover as used in cellular telephony.*

Achievements

A major achievement of ETSI's work in this area has been the publication of the specifications for the handover procedure: TS 101 671 [138] and ES 201 671 [133]. 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 handover of lawfully intercepted data and traffic, 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 play a major part in Lawful Interception as they have to ensure that LI is enabled in the core specifications and able to deliver material for handover. TC LI therefore works in close collaboration with those committees, notably TC NTECH, the committee in charge of maintaining the specifications for Next Generation Networks (NGN) developed in TISPAN, as well as TC TETRA (who have passed the maintenance of the TETRA LI specification to TC LI), 3GPP and TC ATTM ([153] to [159]).

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 standardized the general requirement placed on European network operators, service providers and access providers [134] who are obliged under provisions of the Framework Directive to make available results of interception to the law enforcement agencies. Complementing these requirements, a Technical Specification [139] relating to handover interfaces for the interception provides guidance for law enforcement agencies on the cooperation 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 [142]
- part 2: SSD for messaging services [143]; this specification, formerly for e-mail services only, has been extended to messaging services in 2012
- part 3: SSD for Internet access services [144]
- part 4: SSD for Layer 2 services [145]; this specification is particularly important because, in many situations, information on higher layers is either not accessible or not stored
- part 5: SSD for IP Multimedia Services [146]
- part 6: SSD for PSTN/ISDN services [147]
- part 7: SSD for Mobile Packet Services [148]

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 [141].

Two other TRs cover Lawful Interception of public Wireless LAN Internet Access [136] and the Lawful Interception domain architecture for IP networks [137].

TC LI has produced a TR ([149]), defining a security framework for securing Lawful Interception and Retained Data environment (see below) of the CSP and the Handover of the information.

A further TR [152] was published to provide generic recommendations for requests for handover and delivery of real-time or stored information referred to as an eWarrant Implementation Interface.

ETSI organized two PlugtestsTM 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: [142], [143] and [144]. During the second LI Plugtests event in 2007, the following TSs were tested: [138], [142], [143], [146] and [147]. The outcome of both events highlighted issues which were looked after by the TC LI through a number of updates to the relevant publications.

Retained Data

Retained Data (RD) 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 crucial. TC LI has produced a TS [135] which deals with the requirements from Law Enforcement Agencies for the handling of Retained Data. 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 authorized requesting authorities.

TC LI's work on Retained Data has been intense, and is now widely recognized worldwide. At the end of 2008 a Technical Specification was published ([150]) which standardizes 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.

A report [151] on System Architecture and Internal Interfaces for Retained Data elaborates on RD system architecture and assigns and describes internal interfaces to specific services and functional entities on the CSP side. It provides guidance on implementation issues that CSPs have to deal with. This work was coordinated with TISPAN.

Ongoing activities

TC LI continues to maintain the suite of Lawful Interception and Retained Data publications by updating them regularly.

Work is ongoing on a TS, expected to be published in 2015, providing a standardized mechanism for the dynamic triggering and revocation of the interception of communications content to take account of the increasingly dynamic configuration of CSPs and networks. 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.

TC LI continues its work on RD/LI for Cloud Computing with two TRs to provide recommendations on requests for handover and delivery of stored information associated with cloud/virtual services. The reports, expected to be published in 2015, are intended to identify any RD/LI work necessary to ensure that there are no technical obstacles in the converged cloud/virtual service environment to this aspect of regulation, thus ensuring that RD/LI obligations can be maintained while allowing businesses to utilise the advantages and innovations of Cloud Services.

TC LI started a new specification in 2012 to define an electronic interface between two systems for the exchange of information relating to the establishment and management of Lawful Interception. Typically this interface would be used between: on one side, a Communications Service Provider; and, on the other side, a Government or Law Enforcement Agency who is entitled to request Lawful Interception. While the published report [152] defines a generic interface for electronic Warrants; this document is a specific and detailed example of one particular Warrant interface.

TC LI started a new specification in 2013 on the internal network interface X1 for LI (to be extended to X2 and X3 at a later stage), which covers wide area connections between LI systems and (depending on the network) several network elements from different vendors. Nearly every network element has its own interface with different transport protocols, authentication (if any), encryption (if any), commands etc. This makes every new connection highly complicated and costly, as the interfaces between Administration and Mediation Functions are usually proprietary within an LI product. This work intends to help solve such issues.

TC LI started a new specification in 2013 on security for LI and DR systems. The need for Security, (Physical, Hardware, Software, Personnel, Cyber) is a fundamental requirement for all LI and DR systems. As networks become increasingly IP service centric, globally distributed and frequently software based, the need for good basic security becomes ever more important. The new TS will build on work already undertaken in other TC LI specifications and reports, and will use a threat based model and requirements approach to develop minimum levels of LI and DR system assurance/risk management for real operator deployment scenarios.

In 2014 TC LI began work on a new specification to create a dictionary of common parameters. This specification aims to provide an easy way to introduce commonly used parameters in other specifications, in order to reduce the amount of work involved in defining such parameters.

In 2014 TC LI began to revise the specification for a Lawful Interception interface originally developed for ETSI’s TETRA (Terrestrial Trunked Radio) standard. This will be updated to address new capabilities of TETRA related to LI and to bring the document in line with LI activity as a whole.

The committee began work on two new ETSI Special Reports in 2014. One will provide a guide to Lawful Interception and Retained Data standards and concepts (including an evolutionary overview) and the other will offer guidance on LI for LTE™ in the form of Frequently Asked Questions.

Liaisons and Cooperation - As noted earlier, effective cooperation between organizations and committees working on Lawful Interception is imperative. TC LI works closely with other committees outside and within ETSI, including:

- ETSI’s Industry Specification Group on Network Functions Virtualisation (ISG NFV) to ensure the LI requirements on NFV are met in an appropriate way
- ETSI TC CYBER for cyber security matters related to the security of LI/RD interfaces and information flow
- The International Organization for Standardization (ISO) TC 204 on building an open dialogue on LI matters
- ETSI's Operational Coordination Group on Electronic Communications Networks and Services Directives (OCG ECN&S) on an assessment of the consequences of the European Union ECN&S regulatory viewpoint on the standardization of Next Generation Networks (NGN).

TC LI also collaborates closely with the LI group in the Third Generation Partnership Project (3GPP™) (SA3-LI) on LI for the Universal Mobile Telecommunications System (UMTS) and the Global System for Mobile Communication (GSM). By monitoring each other's activities, the groups ensure that their respective LI specifications are aligned.

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.

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 data, to protect against forgery of the data by the recipient and to support signer non-repudiation.

Standards to support the use of digital signatures and public key certificates are a key driver in enabling the successful evolution of electronic transactions. ETSI's Electronic Signatures and Infrastructures Technical Committee (TC ESI) is responsible for standardization in the areas of digital signatures and Public Key Infrastructure (PKI) to support electronic transactions in open environments.

ETSI's involvement in this area began in September 1996, with the provision of specifications related to electronic signatures with the contribution of CEN. Activities in this area intensified with the release of the European Directive 1999/93/EC on a Community framework for electronic signatures. In December 2009 the European Commission issued a standardization mandate (M/460) aiming at achieving the interoperability of electronic signatures throughout Europe, by providing a rationalized European electronic signature standardization framework which will allow mutual recognition and cross-border interoperability. In July 2014, Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market was adopted, repealing the Directive 1999/93/EC. TC ESI mainly works on standards, globally applicable, in support of this new Regulation.

Achievements

In 2012, CEN and ETSI worked on the definition of a rationalized framework for electronic signatures standardization which was published a Special Report (SR) [213]. Based on this SR and its successor that TC ESI is working on (will be published as TR 119 000), the standards published in the past are and will be reviewed, and step by step migrated to the new framework. This framework comprises the use of a common numbering for standards related to digital signatures in both CEN and ETSI. The number range is x19 yyy with x being 0, 1, 2, or 3 for ETSI documents, and x being 4 for CEN documents. This rationalized framework is structured in six domains:

1. Signature creation and validation

ETSI's publication of deliverables in support of the European Directive began in 2000 with a standard on Electronic Signature formats, specifically on CMS (Cryptographic Message Syntax) Advanced Electronic Signatures (CAdES) formats [169] a major revision of which was made in 2013 to include the definition of a new archive time-stamp. An analogous twin specification was published defining XML Advanced Electronic Signature (XAdES) formats [177].

ETSI has organized several XAdES and CAdES Plugtests^{TM} events since 2003. The first ones were face-to-face meetings. They became remote events since 2008. All the outcomes of the events were used as inputs to update the related deliverables as necessary.

In 2009 TC ESI published a set of profiles for PDF Advanced Electronic Signatures (PAdES) as a multipart TS. A TR [206] was also published, providing guidelines for the use and implementation of PAdES. The possible techniques that may be used for printable representations of advanced electronic signatures

(AdES) in PDFs have been collected in a special report [207]. The first PAdES remote Plugtests^{TM} interoperability event was held at the end of 2011 with more than 35 participating organizations.

In 2011 TC ESI published a TS [212] on Associated Signature containers, a package format for associating advanced electronic signatures with one or more files to which the signature applies. A first ASiC Remote Plugtests^{TM} was held in 2014.

Four AdES baseline profiles for XAdES [215], PAdES [216], CAdES [217] and ASiC (Associated Signature Containers) [218] were published in 2012. They are be used for interoperability of AdES signatures used in electronic documents issued by competent authorities to be interchanged across borders in the context of the EU Services Directive 2006/123/EC.

Signature validation procedures and policies [219] were published in 2012.

Conformance testing was carried out for XAdES baseline profile [220], and test suites for PAdES and ASiC interoperability [221] and [222]. In such areas, Plugtests^{TM} events were organized by the ETSI Centre for Testing and Interoperability (CTI).

2. Signature creation and other related devices

This domain is addressed by CEN.

3. Cryptographic suites

ETSI TC ESI regularly updates a set of hash functions and asymmetric algorithms for Advanced Electronic Signatures [230].

4. Trust Service Providers supporting signature

Several standards address policy and security requirements for Trust Service Providers (TSPs):

- general requirements in a European Standard [223];
- requirements for TSPs/Certificate Service Providers (CSPs) issuing qualified [173] and non-qualified [175] certificates (these documents are now in widespread use both within and beyond the bounds of the European Community); [173] was superseded in 2013 by a European Standard [224]; [175] includes the policy requirements for issuing baseline and Extended Validation Certificates SSL/TLS (EVCs) and for ensuring alignment of the Certification Authorities (CA) with the EVC guidelines issued by the CAB Forum (EVCs include standardized procedures for verifying and expressing the identity of the certificate holder); in 2010 the CAB Forum recognized [175]. This allows CAs to issue baseline and EV certificates in compliance with ETSI’s policy requirements; [175] was superseded in 2013 by a European Standard [225] for public key certificates excluding web site certificates based on CAB Forum requirements, for which [175] remains valid; see also [174], a TR which provides guidance on [173], a TR [208] which provides guidance on [175] for Issuing Extended Validation Certificates for Auditors and CSPs, and a TR [214] which provides guidance on [175] to CAs issuing Baseline SSL/TLS certificates; at last a Special Report [226], published in 2013, provides recommendations on Governance and Audit Regime for CAB Forum Extended Validation and Baseline Certificates;
- organizational and security requirements for Certificate Service Providers issuing attribute certificates [166] and for Time Stamping Authorities issuing Time Stamp Tokens [183];
- policies of Trust Service Providers (TSPs) signing and/or storing data objects [191].

Certificate profiles are addressed through:

- certificate profile for Trust Service Providers issuing qualified certificates, European Standard [227] replacing [179];
- certificate profile for certificates issued to natural persons, specification [228], replacing [171];
- profile for Time Stamp Tokens [184];
- A number of Technical Reports (TRs) were also created to explain 'Signature Policy' to users ([161], [174], [182] and [185]).

As part of its ongoing work to provide new and updated standards in support of Regulation (EU) No 910/2014, in 2014 ESI published an updated specification [231] on requirements for Conformity Assessment Bodies (CAB) assessing Trust Service Providers.

5. Trust Application Service Providers

TC ESI created a Registered E-Mail (REM) framework for registered email services with a six multi-part specification: [192 to 194] providing a framework for origin authentication, proof of delivery and long term availability, [195 and 196] defining conformance and interoperability profiles, and part 6 consisting of three sub-parts [197] to [199] which specify interoperability between REM solutions based on different transport protocols. This part 6 covers the interoperability of the ESI's REM solution using Simple Mail Transfer Protocol (SMTP) with the Universal Postal Union (UPU) [197], Business Document Exchange Network (BUSDOX) [199], and Simple Object Access Protocol (SOAP) [199] solutions. In addition, ESI developed test suites for future REM interoperability tests [209].

In 2014, TC ESI published a study on standardization requirements for electronic delivery applying electronic signatures [232].

TC ESI published standards on information preservation systems security. The goal is to provide a common, objective and reliable basis both for preservation service providers to implement and manage secure Information Preservation Systems [210], and, for assessors to measure whether these systems meet the quality requirements of the EU's Directive on services in the internal market (2006/123/EC) [211].

6. Trust Service Status Lists Providers

Trust-service Status Lists (TSLs) [165] provide a harmonized way for trust services (services which enhance trust and confidence in electronic transactions) and their providers to publish information about the services and providers which they oversee. A subsequent European Union Member State (EU MS) trusted lists [229] was published as a means to express trust service status information with regards to their compliance with the relevant provisions laid down in Directive 1999/93/EC and in related national laws.

Interoperability activities

Recent Plugtests^{TM} events and other interoperability related work carried out by the ETSI Centre for Testing and Interoperability (CTI) regarding TC ESI work include:

ASiC PlugtestsTM

This event was carried out in April 2014 aiming at conducting interoperability test cases on AsiC containers. It provided full test coverage of the specifications including testing signatures evolution, simulating real life situations. 59 participants came from a total of 35 organizations.

TSL Conformance Checker

In 2011, ETSI CTI has run a project with the European Commission to develop a portal to allow members states to check the conformance of their TSL (Trust-Service Status List) signatures with the related EC Directive. It also allows to create a PDF/A human readable format of their Trusted List. The project lasted 2 years, after which ETSI TC ESI, CTI and the European Commission decided to continue their collaboration for another 2 years with a new project, until end of 2014, to upgrade the portal and to provide the tools related to the specification [229] (EU MS trusted lists).

e-Signature Validation Remote Plugtests

This remote Plugtests^{TM} interoperability event, held in November 2014, addressed validation of ETSI advanced electronic signatures. It was organized in cooperation with the European Commission. The aim of this Plugtests^{TM} was twofold: on one hand, to take stock of what the European Member States currently have as e-signatures used for their e-government purposes and to test whether these can be validated in other Member States relying on EU Member States' Trusted Lists; on the other hand, to detect possible issues in different validation processes and to identify possible divergences in the validation applications for the same signature used. 65 organizations took part.

Conformance Checker

ETSI CTI provides free online tools that perform numerous checks in order to verify the conformity of XAdES baseline, CAdES and PAdES signatures, and ASiC containers.

Ongoing activities

ETSI ESI current work focuses on the execution of the European Commission (EC) Mandate on Electronic Signature Standardization (M/460) for which CEN and ETSI are cooperating to ensure the alignment of standards and avoid overlapping work. ETSI ESI is executing phase 2 of the mandate, i.e. implementing the work programme as defined in [213]. The work covers:

- Business Guidance documents on the use of electronic signature standards in each of the Rationalized Structure areas
- General Requirements on Policy and Conformity Assessment for Signature Creation and Validation
- Signature creation & validation area: to align specifications with the rationalized framework, addressing any gaps identified in the rationalized framework work plan, and progressing all the relevant specifications to EN status. Work includes signature formats, signature creation and validation procedures and signature policies
- Requirements for Conformity Assessment Bodies (CAB) assessing Trust Service Providers, and revise the related specification [231] into an EN
- Requirements for Trust Service Providers issuing certificates
- Testing compliance and interoperability: to develop a set of technical specifications and tools that act as catalysers for implementing essential standards of the framework, particularly for signature creation and verification. In addition, new Plugtests^{TM} events are planned for CAdES, XAdES, PAdES and ASiC.

Draft standards can be found here: http://docbox.etsi.org/ESI/Open/Latest_Drafts/. New draft versions on TSPs and signature creation and validation were issued early 2014 taking into account the requirements of the Regulation (EU) No 910/2014. However, these documents are aimed to be internationally applicable within and outside the EU. These drafts were submitted to public review. The TS versions of these standards are planned for publication mid 2015 with a parallel submission for EN approval procedure.

A stakeholders' mailing list has been set up to provide regular news and updates on the progress of the execution of the mandate: Subscribe to the E-SIGNATURES_NEWS mailing list.

TC ESI also plans to initiate new work in order to complete the framework of standards. New activities will address in particular e-delivery, a preliminary study addressing the future standardization of the preservation of digital signatures, and work to be done in the context of issuance of certificates as trust services and on related TSP activities.

Algorithms

ETSI's Security Algorithms Group of Experts (SAGE) provides our standards makers with cryptographic algorithms and protocols specific to fraud prevention, unauthorized access to public and private telecommunications networks and user data privacy.

Achievements

Accomplishments include algorithms for 3GPP [264], DECT, GSM and TETRA ([245] to [249], [259] and [260]), audiovisual services ([236], [237]), GPRS and Universal Personal Telecommunications (UPT) [242]. SAGE also collaborates with other ETSI committees to produce encryption algorithms.

All of the standardized security algorithms for UMTS were developed by SAGE (for an overview of the overall algorithm mechanisms in UMTS, see [40]:

- The initial set of algorithms for the UMTS radio interface (UTRA) - UEA1 and UIA1 - was developed by SAGE in collaboration with the 3GPP Organizational Partners. UEA1 is the standard encryption algorithm, and UIA1 is the standard integrity algorithm; both are based on the Kasumi block cipher, also designed by SAGE (as a variation of Mitsubishi's MISTY1 algorithm). The specifications for the algorithms (which are only for the development and operation of 3G mobile communications and services) can be found in TS 135 201 ([45], see also [46] to [48]).

- SAGE also developed a second set of algorithms, UEA2 for encryption and UIA2 for integrity, again in collaboration with 3GPP. These algorithms are based on the SNOW 3G stream cipher, which was in turn developed by SAGE as a variant of the public domain cipher SNOW 2.0 ([265] to [269]). A strong motivation for the design is that the algorithms should be fundamentally different in nature from UEA1 and UIA1, so that any new advances in the science of cryptanalysis are unlikely to impact both sets of algorithms.

- SAGE was also responsible for the specification of the Milenage algorithm set, an example algorithm set for the UMTS authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5* ([49] to [53]).

- SAGE has completed the design and specification of a second example algorithm set for the UMTS authentication and key generation functions, with a view particularly to the nascent embedded UICC market where it may be desirable to have two algorithms built in as options. This second algorithm is called TUAK, and is based on the public KECCAK hash function family (which will also serve as the SHA-3 hash function standard). TUAK is currently being put forward for publication as a 3GPP Technical Specification.

SAGE has also specified standardized cryptographic algorithms for the Long Term Evolution (LTE™) mobile radio access architecture. Two sets of algorithms have been defined for the radio interface:

- The encryption algorithm 128-EEA1 (EPS Encryption Algorithm 1) and the integrity algorithm 128-EIA1 (EPS Integrity Algorithm 1) are identical to the UMTS algorithms UEA2 and UIA2, with a defined mapping of LTE parameters onto UMTS parameters.

- The encryption algorithm 128-EEA2 and the integrity algorithm 128-EIA2 are both modes of operation of the Advanced Encryption Standard (AES), with SAGE specifying the precise details and generating test vectors.

- The encryption algorithm 128-EEA3 and the integrity algorithm 128-EIA3 are based on a stream cipher called ZUC [270] to [273]. These algorithms were designed by a 3GPP member company, with SAGE coordinating all of the academic and public review.

SAGE has designed a new set of cryptographic algorithms for DECT: an authentication and key derivation algorithm DSAA2, and an encryption algorithm DSC2. These support longer encryption keys than the original DECT algorithms. Both algorithms are defined as modes of operation of the Advanced Encryption Standard. They are included in the current DECT standard.

Other achievements include the design of encryption algorithms for GSM, EDGE and GPRS (A5/3 and A5/4 for GSM and EDGE. GEA3 and GEA4 for GPRS) which provide users of GSM mobile phones with a higher level of protection against eavesdropping than previously available. A5/4 and GEA4 [64] use 128-bit cipher keys, longer than is available in traditional GSM, so these rely on recently standardized changes to other network nodes to deliver a 128-bit key. Again, all of these algorithms were developed in collaboration with the 3GPP organizational partners ([59] to [63], [254], [255] and [262]), and are closely based on the UMTS algorithm UEA1. A5/3 is now being adopted by some operators within their networks.

Some of the earlier work of SAGE is not publicly available, although most algorithms produced in recent years have been made public. Their implementation is generally subject to a license which restricts their utilization to the equipment or service for which they have been designed. ETSI acts as a Custodian for the algorithms and is responsible for the distribution and licensing of the confidential information and documents.

Cyber Security

In 2014 ETSI created TC CYBER with the responsibility for the standardization of cyber security and for providing a centre of relevant expertise for other ETSI committees.

The Internet has become a critical infrastructure for both businesses and individual users. Growing dependence on networked digital systems has brought with it an increase in both the variety and quantity of cyber-threats. The different methods governing secure communication in the various Member States of the European Union, as well as beyond Europe, sometimes make it difficult to assess the respective risks and to ensure adequate security. Building on its world-leading expertise in the security of Information and Communications Technologies (ICT), ETSI set up a new cyber security committee (TC CYBER) to meet the growing demand for standards to protect the Internet and the communications and business it carries.

TC CYBER is working closely with relevant stakeholders to develop appropriate standards to increase privacy and security for organizations and citizens across Europe. The committee is looking in particular at the security of infrastructure, devices, services and protocols, as well as security tools and techniques to ensure security. It offers security advice and guidance to users, manufacturers and network and infrastructure operators.

Among related duties, TC CYBER is in charge of the coordination of work with other groups in ETSI and outside, such as SDOs and other groups/platforms, and is also responsible to provide and coordinate answers to policy requests on cyber security and ICT security in broad sense.

There was enormous support for the establishment of the new committee, with more than 50 members from industry and academia attending the first meeting in May 2014 to draw up a plan of work.

TC CYBER began work on eight ETSI Technical Reports (TRs) and an ETSI Guide (EG).

Achievements

TC CYBER published a report in May 2015 to provide guidance related to the provision of Security Assurance by Default by means of Critical Security Controls for Effective Cyber Defence [233].

Ongoing activities

Listed below are the documents TC CYBER is working on at the time of publication of this paper. Several are expected to be published by summer/autumn 2015, and new ones to be created.

- To be published as TR 103 303: "Protection measures for ICT in the context of Critical Infrastructure" to provide guidance for the deployment of security technologies and security management to deliver and maintain effective Critical Infrastructures that are reliant on ICT technology
- To be published as TR 103 304: "PII Protection and Retention" as guidance for the protection and retention of PII (Personally Identifiable Information)
- To be published as TR 103 306: "Global Cyber Security Ecosystem" to provide an overview of cyber security work being undertaken in multiple forums worldwide
- To be published as TR 103 307: "Security Aspects for LI and RD interfaces" to provide guidance to protect information flows and interfaces from a security perspective (confidentiality, integrity and

authenticity) in a context of provision of Lawful Interception (LI) and Retained Data (RD) functionalities

- To be published as TR 103 308: "A security baseline regarding LI for NFV and related platforms" to provide guidance related to the legal and physical challenges to ensure LI functionalities in an NFV context, with a focus on the infrastructure of NFV rather than the functions themselves
- To be published as TR 103 309: "Secure by Default adoption – platform security technology" to provide guidance to business decision makers for the development and adoption of secure by default platform security technologies, highlighting the market need
- To be published as TR 103 331: "Structured threat information sharing" to provide Guidance for exchanging cyber threat information in a standardized and structured manner
- To be published as EG 203 310: "Post Quantum Computing Impact on ICT Systems" to review nature and vulnerabilities of security algorithms when subjected to quantum computing attacks, and evaluate characteristics required of algorithms in order to be invulnerable under such attacks.

Network Functions Virtualisation

The intent of Network Functions Virtualisation (NFV) is to allow for the transfer from a conventional hardware centric network platform to a software centric platform with the view that network functions are resident in virtual machines that can be instantiated on demand on general purpose hardware.

ETSI'S ISG NFV-SEC WG addresses the security aspects of the overall mission of ISG NFV. The security challenges of moving to a virtualised, software network cannot be understated and it is the role of NFV-SEC to quantify and qualify the risks of NFV and to identify strategies and models for giving assured security to the future networks that will be built from NFV and SDN (Software Defined Network) capabilities.

Addressing the security issues of NFV in the context of the ISG has been undertaken through an analysis of the problems that NFV introduces when compared to conventional networking architectures. The output of this has been captured in the specification [234]. The continuing work programme of NFV security has taken many of the key problems identified in [234] and expanded them to identify key system requirements. This has initially led to a review of trust in the NFV environment published as specification [235]. In turn this has led to the current work programme of the ISG that is expanding discussion on multi-level authorization and authentication that ensures separation of functions from a conventional super-user/user type of operating system model to allow for functions to be enabled on hardware that may be run by another body.

The working practices in the ISG encourage close co-operation with other bodies, with the ISG providing a framework and guiding other bodies to develop solutions. In this way the ISG enables new work for the platform without developing potentially competing standards. Thus the ISG has expanded the problem statement with collaboration of members of ETSI TC LI to address the issue of dealing with LI in an NFV environment. Similar expansion of problems and their resolution is being addressed alongside 3GPP SA3 and ETSI TC CYBER addressing such issues as root of trust, privacy protection, key management for transient platforms, accountability (including non-repudiation services) and system integrity assurance for a highly dynamic network configuration. The latter is one issue introduced by the ability to virtualise functions that have required specialised hardware in previous technologies, but that through virtualisation are able to run on general purpose hardware. Hence the concept of a fixed system architecture is challenged by the possibility to have multiple concurrent system architectures running on a common hardware platform. Such models present a new challenge to security as the conventional thinking of function mapped to specific and specialised hardware has been broken and the assurances of secure partitioning need to be reinvented.

One broad area of standards innovation addressed in the ISG is collaboration with the open-source community. The intent of this is to drive both standards and open source closer together without losing the strengths of either approach. Within the ISG this has led to close involvement with communities across the IETF and W3C and the development of a programme of standards concept verification through the Proof of Concept (PoC) programme that is managed through ETSI's CTI (Centre for Testing and Interoperability) group of experts. In due course many of the core concepts of protection of NFV will be evaluated in such PoC programmes and the results fed back to further develop ETSI's ISG NFV specifications.

Quantum Key Distribution

The creation of ETSI's Industry Specification Group (ISG) Quantum Key Distribution (QKD) was approved by the ETSI Board in September 2008 in order to bring together the important stakeholders from science, industry, and commence to address standardization issues in quantum cryptography, and quantum technology in general.

Quantum cryptography has great potential to become the key technology for securing confidentiality and privacy of communication in the future ICT world and thus to become the driver for the success of a series of services in the field of e-government, e-commerce, e-health, transmission of biometric data, intelligent transport systems and many others. Its power stems from the fact that quantum communication allows for a new primitive, which permits two parties to establish a secret key from a short pre-shared secret and a public exchange, i.e. something which was never possible with classical, non-quantum means.

ETSI's QKD Industry Specification Group develops ETSI Group Specifications (GSs) that describe quantum cryptography for ICT networks. Quantum Key Distribution is the essential credential in order to use quantum cryptography on a broad basis. It is the main task of the ISG QKD to specify a system for Quantum Key Distribution and its environment.

Achievements

Below is the list of the publications of the ETSI ISG QKD.

- A catalogue of security and other functional requirements for different user groups and different fields of application [274];
- A definition of properties of components and internal interfaces of QKD Systems [275];
- An evaluation of application interfaces over which a QKD system is attached to a cryptographic information and communication technology (ICT) system [276];
- A study and systematization of existing security proofs to serve as a reference textbook for assessing the capabilities of different QKD systems and constructing respective requirements and evaluation criteria for practical security evaluation [277];
- A generic security specification for QKD systems, based on a thorough security analysis for which the steps foreseen in the Common Criteria ISO/EN 15408 have been carried out. This document enables QKD system developers to assess their systems in terms of security evaluation and accreditation for qualified use [278].

Ongoing activities

The current work of the ISG QKD is on the following four specifications which focus on:

- A common ontology, vocabulary and terms of reference for the quantum cryptography domain
- Aspects of the design, construction, characterization and operation of QKD systems that are intended to protect against Trojan horse attacks
- Characterization of optical components for use in QKD systems
- Characteristics of QKD devices and of the required communication channels in the context of QKD deployment on a point-to-point link.

Quantum-Safe Cryptography

The creation of ETSI's Industry Specification Group (ISG) on Quantum-Safe Cryptography (QSC) was approved by the ETSI Board in February 2015 in order to make an assessment and provide recommendations on the various proposals from industry and academia for quantum safe cryptography for real-world deployment and to standardize their relevant parts when needed.

The ISG QSC aims to make recommendations on core cryptographic primitives and develop ETSI Group Specifications (GSs) for quantum-safe ICT applications highlighted by industry. It also aims to offer practical advice and guidance to industry on real-world deployment issues, such as transition timescales, generic requirements from operators or vendors, assessment of threats and risks.

The work of the QSC ISG will include:

- Identification of proposals from industry and academia for quantum safe cryptographic primitives, and the development of a framework for quantum safe algorithms
- High-level characterization of these primitives in term of computational complexity, security assumptions against classical and quantum threats, efficiency and agility
- Assessment of the suitability of the cryptographic primitives with respect to the quantum safe requirements and applications
- Threat and risk assessment for real-world use cases
- Providing evidence of the need for new standards and technological guidance, along with a development roadmap, including performance standards and verification techniques for quantum safe algorithms
- Dissemination of guidance and standards documents, and later maintenance of the standardized algorithms under the custodianship of the ETSI SC Security Algorithms Group of Experts (SAGE)
- Defining criteria for, and assessment of, the suitability of cryptographic primitives.

Ongoing activities

Below are listed the first five Group Specification ISG QSC started to work on following its first meeting in March 2015.

- Quantum safe algorithmic framework (to be published as GS QSC 001 in 2016)
- Cryptographic primitive characterization (to be published as GS QSC 002 in 2017)
- Cryptographic primitive suitability assessment (to be published as GS QSC 003 in 2016)
- Quantum safe threat assessment (to be published as GS QSC 004 in 2016)
- Quantum safe standards assessment (to be published as GS QSC 005 in 2016).

Identity and Access Management for Networks and Services (INS)

ETSI's Industry Specification Group (ISG) Identity and Access Management for Networks and Services (INS) was created in 2009 to develop ETSI Group Specifications (GSs) to achieve consensus on Identity Management protocols and architectures, in particular related to networks and services taking the Future Internet perspective into consideration.

Having achieved its mission ISG INS has been closed in 2014.

Achievements

ISG INS published the following set of GSs to support interoperability and incorporate privacy into the telecoms services and networks domain. The objectives of the specifications are:

- On IdM Interoperability between Operators, or ISPs with Enterprise, to provide mechanisms, interfaces and protocols allowing third party providers to retrieve attributes through the operator [279]
- To provide requirements on the use and application of distributed policy management, decision and enforcement in a hybrid environment (operator and services domains) [280]
- To analyze the telecommunication operator's role acting as Identity Broker to facilitate the anchor functionalities for the management of distributed user profile information. To also define the protocol and data model required to access the user profile information via the Identity Broker [281]
- To analyse mechanisms, protocols and procedures to allow federation establishment based on dynamic SLA negotiations. To identify gaps regarding the definition of formal SLA exchange, attributes and privacy issues associated, and dynamic negotiation protocols [282]
- To provide the requirements on the enforcement of policies in a distributed environment supporting interoperability between different players [283]
- To identify the need for a Global, Distributed Discovery Mechanism and to provide a gap analysis for global distributed discovery of identifiers, providers and capabilities [284]
- To create a generic architecture for distributed access control and enforcement. It includes the identification of the necessary identities as well as a general description of their interface and related interactions [285].
- To provide security and privacy requirements for distributed network monitoring in order to identify gaps regarding distributed processing and computation, protocols, and anonymized data exchange [286].
- To identify the requirements to develop a globally distributed discovery of identifiers, providers and capabilities [287].

Information Security Indicators (ISI)

ETSI's Industry Specification Group (ISG) Information Security Indicators has the following scope:

- Develop and build up a full set of Information Security Indicators (to become an ETSI Group Specification), that will be the basis for further state-of-the-art figures;

- Select the relevant Priority One Indicators (with a detailed description in compliance with ISO 27004)

- Develop an underlying Security Event Classification Model (to become an ETSI Group Specification), linked and consistent with the set of IS Indicators;

- Define a possible implementation of a subset of Indicators, with definition of the relevant monitoring tools and/or methods (with the goal to become an ETSI Group Specification);

- Encourage the innovation and pragmatism in inviting for contributions from the circles of both users companies and providers, towards developing common reference draft.

ETSI ISG ISI, created in 2011, has been working on a first set of five GSs, four of which have been published:

- GS ISI 001, published, in two parts [288] and [289], to provide ISI indicators as a way to assess security measures level of effectiveness, and an accompanying guide
- GS ISI 002, published [290], linked strictly to ISI 001 is a comprehensive security event classification model covering incidents, vulnerabilities and nonconformities (with detailed taxonomy and representation)
- GS ISI 003, published [291], to assess the maturity level regarding overall event detection through dedicated KPIs (technology/people/process) and to weigh event detection results
- GS ISI 004, published [292], to demonstrate through examples how to produce indicators and how to detect the related events with various means and methods (with categories of use cases/symptoms)
- GS ISI 005 to propose a way to produce security events and to test the effectiveness of existing detection means, expected to be published in 2015.

Smart Cards

A smart card generally takes the form of a credit card-sized device containing a micro-processor enabling it to process and store information, to support single or multiple applications operated both off-line and on-line. A smart card may be a contact card, where physical contact between the card and the card reader is necessary for operation, or a contactless card, where the card and the card reader establish a short-range wireless communication (in which case the contactless card reader acts as a power source for the contactless card thanks to inductive coupling). A smart card may offer both a contact and contactless interface.

Smart cards are an important enabler in applications where a user's credentials (e.g. a private key in a PKI scheme or a biometric template) are used for authentication and secure communication. A card may perform security-related processing and it may be certified both from the platform and the application standpoints. The card may require a user's Personal Identification Number (PIN) or biometric sample in order to perform any tasks, thus minimising the risk of security breaches associated with sending authentication data over computer networks. Smart cards are used in a wide range of applications in the banking, ID and telecom worlds, among others. Access control, payments, network authentication, electronic purses, storage of confidential information, loyalty and ticketing are further examples of common smart card applications.

As any other device, a smart card may be vulnerable to physical attacks. However such attacks are very unlikely to be successful without the use of very advanced and complex technology, as a range of strong security features and countermeasures are usually implemented to prevent unauthorized access to smart cards and tampering with the data they contain.

Standards for smart cards can roughly be split in three families:

- Definition of the physical aspects, such as form factor, physical constraints (e.g. temperature, humidity, bending) and electrical interfaces
- Definition of the logical aspects, from a platform or an application-specific standpoint; these standards address logical protocols and applications
- Definition of a runtime environment and Application Programming Interfaces (APIs) for the smart card to be able to host interoperable applications.

The main task of ETSI Technical Committee Smart Card Platform (TC SCP) is to maintain and expand the specifications of a smart card platform, the Universal Integrated Circuit Card (UICC) for mobile communication systems upon which other committees and organizations can base their system-specific applications. The current set of specifications delivered and maintained by TC SCP allows user access to global roaming by means of their smart card, irrespective of the radio access technology used. TC SCP also has an important part to play in the growth of mobile commerce, by developing the standards for Integrated Circuit (IC) cards to secure financial transactions over mobile communications systems. Additionally, the current integration of contactless card technology in mobile communication terminals requires card issuers and third parties to use a secure platform for their business critical applications. The UICC has evolved to meet this need, addressing the needs for hosting confidential applications, higher storage capacity and use of IT standard protocols. The specifications of TC SCP are generic; they provide a true and state-of-the-art multi-application platform not just for mobile communication systems but for all applications using smart cards.

In addition, TC SCP is in charge of any maintenance work for M-COMM (closed TC) deliverables, should it be required.

Achievements

ETSI standardized the Subscriber Identity Module (SIM) card for GSM, which is one of the most widely deployed smart cards ever. The concepts developed in the GSM specifications have also been imported into the 3GPP specifications to create the USIM (Universal SIM) card used in UMTS. The UICC platform can also be used in TETRA and 3GPP2 systems.

An important milestone in the evolution of the Smart Card Platform was the completion in 2008 of Release 7 of all specifications with the addition of two new interfaces to the card with respect to the legacy ISO/IEC 7816-based interface, as well as new logical interfaces enabling IP and HTTP connectivity. A Secure Channel was also specified to be used over either the legacy or the high-speed interface. Since then TC SCP has further evolved and enhanced the Smart Card Platform specifications, with a special focus on delivering test specifications for all the new features. Release 12 will also be a milestone with the current work on embedded UICC.

Major recent achievements include:

- Creation of an Application Programming Interface (API) specification for Java Card™ contactless applications in [311]
- Realization of test specifications for the interface to a contactless front-end in the Terminal. Five specifications have been produced:
  - [312] testing the Terminal aspects of the Single Wire Protocol
  - [313] testing the UICC aspects of the Single Wire Protocol
  - [314] testing the Terminal aspects of the Host Controller Interface
  - [315] testing the UICC aspects of the Host Controller Interface
  - [316] testing the aspects of the Host Controller Interface related to the contactless front-end
- Realization of test specifications for the high-speed interface. Two specifications have been produced:
  - [317] testing the Terminal aspects of the high-speed interface
  - [318] testing the UICC aspects of the high-speed interface
- Realization of a test specification for the Smart Card Web Server API [319]
- M2M-oriented UICC: a UICC capable of being operated in M2M (Machine to Machine) communications, taking into account some of the very specific constraints of industrial environments. This M2M-oriented UICC can be implemented in two new form factors specified in [320]
- Delivery of a technical specification for a fourth UICC form factor (part of [302]), now used by all major manufacturers

- Realization of test specifications for the Secure Channel between the UICC and a Terminal endpoint. Two specifications have been produced:
  - [321] testing the Terminal aspects of the Secure Channel
  - [322] testing the UICC aspects of the Secure Channel.
- Delivery of requirements and a technical solution in order to address the challenges resulting from embedding a UICC in a device, making it not easily accessible or replaceable [323]. The main focus of this work is to deliver new methods and technical solutions in order to securely and remotely provide access credentials on the embedded UICCs (eUICC) and to manage subscription changes from one MNO to another.

Overview of the other main work and specifications:

- Addition of a high-speed, physical interface based on the Inter-Chip USB, and, enabling higher speed communication alongside the use of a more modern software communication stack. It is specified in [296]
- Addition of a dedicated interface for the UICC to be used as a secure element in contactless communications such as Near Field Communication (NFC). This feature is specified in two specifications:
  - for the physical interface and lower communication layer, the Single Wire Protocol was specified [297]
  - for the logical interface, high-level communication and administration layer, the Host Controller Interface was specified [298]
- Definition of IP connectivity for the UICC, specification [299]
- Specification of a Secure Channel between the UICC and an endpoint, either platform to platform or application to application oriented [300]
- Delivery of an Application Programming Interface for the Smart Card Web Server (SCWS, defined by the Open Mobile Alliance, OMA), specification [301]
- Specification [302] is a comprehensive presentation of all the mandatory security features a UICC smart card must have. The UICC security architecture is designed so as to be able to provide, if necessary, a multi-verification environment, i.e. an environment in which the card can have more than one first level application and may support separate user verification requirements for each application. This specification defines the legacy interface.
- Technical realization of the UICC Security Service Module (USSM), which could add significant value to Digital Rights Management (DRM), secure e-mail, payments, banking and application download (to both the card and the terminal device)
- Confidential applications [306]: a toolbox and set of features to enable hosting of third party applications on the UICC without compromising the platform or the confidentiality of any applications running on the UICC.

Ongoing activities

In addition to the maintenance of the existing set of specifications, the committee is focusing on delivering specifications regarding:

- Creation of a test specification for the remote management of UICC applications
- Creation of a conformance testing specification for the UICC aspects of [302]; the testing of the Terminal aspects is in [307]
- Enhancement to [298] for the interworking of the two main protocols linking the NFC controller to secure elements and the Terminal with special care being given to the management of the NFC controller resources when used by multiple components (secure element or applications in the Terminal)
- Mechanisms enabling the UICC initialization in a Terminal, and optimization in order to reduce the overall boot time
- Delivery of a technical specification meeting the requirements listed in [323].

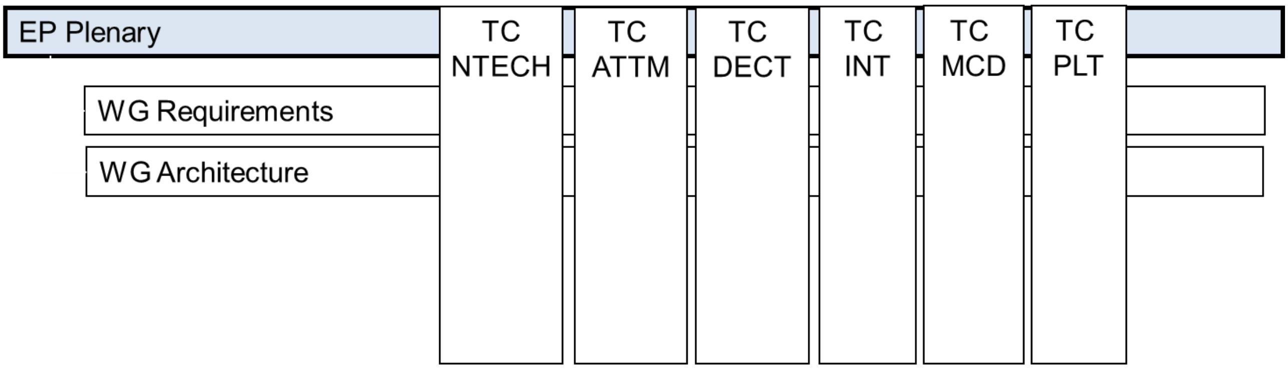
Future Networks

Communication services can now be delivered over multiple technology platforms and received via a broad range of terminals - using fixed and mobile, terrestrial and satellite systems. 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. This opens the door to a new range of security risks.

The converged and access-independent network model which has been referred to popularly as 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. 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. The work on NGN has been looked at in the ETSI Project on End-to-End Network Architectures (EP E2NA) that aimed to foster an environment in which the technologies and standards necessary to achieve inclusive end-to-end communication are managed. In addition, TC NTECH (Network Technologies) worked on NGN standardization.

The ETSI Board decided to close EP E2NA in March 2015.

EP E2NA aimed to bring together a wide set of standards and technologies to ensure they integrate in delivering end to end services. The driver behind this is to ensure that technologies which enable any part of the end-to-end chain are driven by a common set of requirements and are able to plug into a common architecture. The scope of this includes security.



Achievements

The aim of EP E2NA and TC NTECH was to start from the platform established by TC TISPAN WG7 in establishing the security requirements for the subsystems of Next Generation Networks [330] and the related Security Design Guides ([324], [325] and [326]. This work references the guidelines on the use of the Common Criteria for the evaluation of IT security (ISO/IEC 15408). The Common Criteria are a set of drivers to be used as the basis for the evaluation of security properties of IT products and systems, establishing the framework for an IT security evaluation that is meaningful to a wide audience. The Common Criteria primarily address the protection of information from unauthorized disclosure, modification or loss.

The publications deal with the issue of the application of the Common Criteria framework in the ETSI standardization process and the development of protocols and architecture standards [326]. 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.

One of the Design Guides [324] provides guidelines for the preparation of Protection Profiles. A Protection Profile defines an implementation-independent set of security requirements for a category of communication equipment or system which is subject to evaluation under the Common Criteria. The Protection Profile relevant to an ICT product could be used without modification to specify the security requirements of a specific product or service. This ETSI Standard describes the steps necessary to create such a Protection Profile.

Additional guidance on the preparation of Security Targets (STs) based upon ETSI communication standards was also provided. The concept of Common Criteria evaluation involves the preparation of an ST that specifies the security requirements for an identified IT product and describes the functional and assurance security measures offered by that component to meet the stated requirements.

A TR [327] provides an analysis of the security provisions made in IPv6 and outlines how they may be used to support the implementation of Public Key Infrastructure (PKI) solutions and the further deployment of IPv6 and IP security (IPsec).

The challenge of security in Next Generation Networks was addressed with an analysis of risks and threats [332] and by defining an extensible NGN security architecture [333].

Other publications include an ETSI Guide on the application of security countermeasures to service capabilities [336], an analysis of security mechanisms for customer networks connected to TISPAN NGN Release 2 [337], a feasibility study on Media Security in TISPAN NGN [338], a NAT traversal feasibility study report [339], a feasibility study on the prevention of unsolicited communication in NGN [340], a report on the security of identity in NGN [341], and a report on the application of ISO 15408-2 requirements to ETSI standards (method and application with examples) [342].

For the purposes of Lawful Interception and retained data, TC TISPAN identified appropriate interfaces, reference points and entities in the NGN architecture (see TS [331]) and published a TR [344].

Publications include:

- A report [345] on a feasibility study on IPTV security architecture, which details study models and key management systems for service protection, a study of functional entities and mechanisms for service protection and a study of a framework open to the integration of content protection solutions;
- A report [346] on prevention of unsolicited communication in the NGN, which addresses the methodologies for preventing the terminating party from receiving Unsolicited Communication (UC) and also addresses the legal implications. A UC detection & handling framework for entities of the NGN is proposed;
- A specification [347] on Identity Protection (Protection Profile) to provide countermeasures in order to assure that users of the NGN have protection from abuse of identity. It covers Identity protection, authentication and integrity, and defines credential management;

- A report [348] on a feasibility study of security of NGN interconnection at the NNI (Network to Network Interface), which addresses security issues related to interoperator NNI interface interconnection and between the different subsystems of the NGN;
- A specification [349] on security services and mechanisms for customer premises networks connected to the NGN. It specifies the functional models, information flows and protocols. The secure mechanism for an update of the service protection and content protection engines within customer equipment will allow an end user to switch to another service provider while keeping his equipment;
- A report [350] on Operational Security Assurance Profile, which analyses the needs related to which equipment vendors, solution providers and service integrators or operators can define a common set of security assurance metrics that need to be deployed in operational systems.

Ongoing activities

The work in TC NTECH is based on a new vision of future networks with greater autonomy, virtualization, and changes to the ways in which services are both used and offered to customers that modify the single vision of threat and countermeasures to a much more nuanced protection model for users and providers.

Emergency and Public Safety Telecommunications

Emergency Telecommunications and Public Safety are areas requiring considerable standardization activity. Existing infrastructures and services have been shown to be inadequate when faced with widespread disruption due to natural disasters and other emergency situations. ETSI is heavily committed in this area and is cooperating with other organizations around the globe.

EMTEL

Special Committee on Emergency Telecommunications (EMTEL) is the focal point in ETSI for the coordination and collection of European requirements for emergency service communications. The committee's scope includes issues related to user needs, network architectures, network resilience, contingency planning, priority communications, priority access technologies and network management, national security and Public Protection and Disaster Relief (PPDR).

EMTEL works mainly with ETSI TCs such as NTECH, previously HF and MSG, 3GPP and entities such as the European Commission COCOM EGEA (Committee on Communications Expert Group on Emergency Access), European Emergency Number Association (EENA), IETF Working Group on Emergency Context Resolution with Internet Technologies (IETF-ECRIT), ITU-T and European projects.

Achievements

Public protection and emergency preparedness is a key topic for EMTEL, and the committee has examined communications networks and the requirements for telecommunication and data transmission to enable the efficient functioning of the emergency services in response to disasters. These studies have resulted in the publication of a series of related TRs ([355], [356], [357] and [358]).

EMTEL has also contributed to Public Warning System, as initially defined by 3GPP, with European requirements [359].

Ongoing activities

Four main EMTEL deliverables are considered as key documents and therefore regularly revised: [351] on emergency call handling, [352] on the European regulations covering communication during emergency situations, [353] on communications between authorities and organizations and [354] on communications from authorities/organizations to individuals, groups or the general public during emergencies.

MESA

Project MESA (Mobility for Emergency and Safety Applications) was a transatlantic partnership project, established in 2000 by ETSI and the North American Telecommunications Industry Association (TIA). The Project's membership expanded to include members in Canada, India, Korea, Australia and Japan. Its aim was to define a digital mobile broadband system which would revolutionize the efficiency of first responders and rescue squads during an emergency or a disaster. In such scenarios, the data rates needed for advanced services, together with the demand for mobility, reach far beyond the scope of current established wireless standards.

Having achieved its mission Project MESA has been closed at the end of 2010.

MESA-capable communications systems directly improve the effectiveness of law enforcement, disaster response, fire fighting, peacekeeping and emergency medical services. Typical applications include the sending of vital information about operators, the transmission of building maps and plans, video monitoring, robotic control, suspect identification and the sensing of hazardous material. To provide a speedier solution than the development of brand new technologies, Project MESA adopted a 'System of Systems' approach, which involves linking together a variety of existing and foreseen technologies and systems. The key factor is interoperability.

Project MESA's Service Specification Group published the system technical requirements ([360] to [362]), whilst the MESA Technical Specification Group published a system overview [363], a system and network architecture document [364] and the system's functional requirements definition [365].

Aeronautics

The creation of the ETSI TC AERO was approved by the ETSI Board in June 2009. TC AERO has the primary responsibility to develop European Standards satisfying the essential requirements and/or implementing the rules of the Single European Sky (SES) interoperability regulation (552/2004/EC) following a Community Specification development Mandate by the EC.

In this context safety aspects are taken into account in cooperation with the European Aviation Safety agency (EASA).

The SES interoperability regulation gives standards a central role in achieving the objectives of the SES Programme, and requires the production and adoption of European Standards (ENs) to be referenced in the Official Journal of the European Union as "Community Specifications", which are always drafted in response to requests ("Mandates") from the European Commission.

Safety requirements are essential requirements of the interoperability regulation and therefore safety aspects are extensively considered. TC AERO has already produced "Community Specifications" on A-CDM (Airport Collaborative Decision Making), A-SMGCS (Advanced- Surface Movement Guidance and Control System) and DLS (Data Link Services). In addition, a task force between TC ERM and TC AERO is responsible for harmonized standards for ground Air Traffic Management (ATM) equipment.

Maritime

Work related to maritime safety is carried out in the ETSI maritime group (ERM TG 26) which takes care of maritime radiocommunication equipment and systems, including the Global Maritime Distress and Safety System (GMDSS)

GMDSS is an integrated communications system using satellite and terrestrial radiocommunications to ensure that whenever a ship is in distress, aid can be dispatched.

Ongoing work in the ETSI maritime group (ERM TG26) includes:

- Digital Selective Calling (DSC)
- Harmonized Standards for maritime personal locating devices employing DSC and AIS (Automatic Identification System)
- Harmonized Standards for radars: navigation radars for use on non-SOLAS (Safety Of Life At Sea) vessels as well as well as radars for Coastal Surveillance, Vessel Traffic Systems and Harbours.

Broadcasting

Broadcasting technologies distribute audio and video signals to a large group of recipients, delivering radio, television and data services. The delivery of some services (such as pay-per-view or subscription-based channels) requires a payment. In these instances, the contents of the broadcasting must be protected with an encryption technique.

ETSI is performing security work in this area in its Joint Technical Committee (JTC) Broadcast, which brings the Institute together with the European Broadcasting Union (EBU) and the European Committee for Electrotechnical Standardization (CENELEC). JTC Broadcast coordinates the drafting of standards for broadcasting and related fields.

Two areas in which JTC Broadcast is involved address specific security features: TV-Anytime and the Digital Video Broadcasting (DVB) Project. TV-Anytime is a set of specifications for the controlled delivery of multimedia content to a user's personal device (Personal Video Recorder). It seeks to exploit the evolution in the convenient, high capacity storage of digital information to provide consumers with a highly personalized TV experience. Users will have access to content from a wide variety of sources, tailored to their needs and personal preferences. ETSI standards for TV-Anytime have been developed in JTC Broadcast, based on proposals from the TV-Anytime Forum, which has now closed after publishing the TV-Anytime specifications. The documents are regularly updated by JTC Broadcast.

The DVB Project is an industry-led consortium of over 200 broadcasters, manufacturers, network operators, software developers, regulatory bodies and others from around the world, committed to designing global specifications for the delivery of digital television and data services. ETSI standards for DVB systems are developed in JTC Broadcast, based on proposals from the DVB Project.

Achievements

A major achievement of the DVB Project has been the release of the DVB Common Scrambling Algorithm. The Common Scrambling Algorithm is composed of the Common Descrambling System and the Scrambling Technology. The specification for each is distributed separately under arrangements with ETSI, which acts as Custodian for the companies which developed the Common Scrambling Algorithm. The last version, known as CSA3, is also available from ETSI. The various agreements, together with the licensing conditions, are available on the ETSI website at:

www.etsi.org/about/what-we-do/security-algorithms-and-codes/csa3-licences

The TV-Anytime specifications were developed in two phases. Phase 1 has been published by ETSI in 2003 as the multi-part TS 102 822. Part 7 of this standard [371] specifies how the TLS (Transport Layer Security) Protocol is used in TV-Anytime to protect the delivery of data: the primary goal of the protocol is to provide privacy and data integrity between two communicating applications. TLS also provides choices of cipher suites where data encryption may be disabled. It can thus be used to ensure the data integrity of metadata conveyed between service provider (server) and user (client).

At the request of the TV-Anytime Forum, JTC Broadcast has worked on the second phase, incorporating an enhanced feature set. These Phase 2 specifications have now also been published by ETSI within the same TS 102 822 series.

TV-Anytime specifications are regularly updated when needed.

A European Standard has been published on the Interaction channel for satellite distribution systems [372] known as DVB-RCS (Return Channel via Satellite).

Since then a five-part standard for a Second Generation DVB Interactive Satellite System (commonly named DVB-RCS2) has been published. Part 1 is a specification for an Overview and System Level specification [388], part 2 is an EN on Lower Layers for Satellite [389], part 3 is a Higher Layers for Satellite specification [390], part 4 [391] provides the Guidelines for Implementation and use of part 2 [389] and part 5 [392] provides the Guidelines for Implementation and use of part 3 [390].

An ETSI TS [393] has been published related to production scrambling algorithms and IP or higher layer security mechanisms, to specify the new common DVB Conditional Access elements (DVB-CSA3); specifically those aspects which are required for co-existence of multiple Conditional Access Systems in a single data stream.

Also a specification on Content Scrambling Algorithms for DVB-IPTV Services using MPEG2 Transport Streams [394] has been published.

The DVB Project has published a multipart collection of TR and TS deliverables (14 parts, [374] to [387]) on CPCM (Content Protection and Copy Management).

DVB has defined a specification for CI (Common Interface) Plus LLP (Limited Liability Partnership) published as CI Plus v1.4, in which security aspects are taken into account [395].

Media Content Distribution

Media Content Distribution (MCD) standardization was carried out in the last phases by ETSI EP E2NA. It addressed the issues induced by the fragmentation and non-interoperability of solutions for content distribution across platforms in a converged environment, supporting IPTV, web TV, Mobile TV and broadcast TV.

The ETSI Board decided to close EP E2NA in March 2015.

EP E2NA addressed MCD security aspects with an analysis of the mechanisms addressing interoperability of multimedia service and content distribution and consumption, with respect to a CA/DRM (Conditional Access / Digital Rights Management) solution [396].

Security Testing

ETSI's Technical Committee for Methods for Testing and Specification (TC MTS) is responsible for the evaluation of available methods and techniques for the advanced and/or formal specification of standards with respect to efficiency and quality, with particular focus on testability. It is also responsible for the provision of methodologies for the generation, processing and verification of test suites.

As parts of its overall responsibilities, TC MTS also addresses issues related to security testing.

Achievements

In 2014 TC MTS published a report [397] on the application of model-based security testing in different industrial domains. The document focuses on the results and conclusions from such work, thus giving an insight into how applicable such methods are today for testing, and indicating their strengths and weaknesses.

In 2015 TC MTS published a report [398] on basic terminology for security testing, which provides the basis for a common understanding of security testing techniques that can be used to test communication products and systems. The document provides information to practitioners on techniques used in testing, and assessment of security, robustness and resilience throughout product and system development lifecycles.

Ongoing activities

TC MTS is working on the two following ETSI Guides (EGs):

- Guidance related to security assurance activities during the phases of the system lifecycle (to be published as EG 203 250)
- Guidance on a set of methodologies that combine risk assessment and testing. It distinguishes between risk-based testing - risk assessment to improve testing, and test-based risk assessment - testing to improve risk assessment- (to be published as EG 203 251).

IPv6

IPv6 is regarded as the main protocol for the next generation internet. It provides vastly increased address space, takes into account the necessary security features and allows "plug-and-play" connection to the network. Due to the complexity of implementing the IPv6 technology, effective testing of IPv6 products is one of the key factors to ensure successful deployment, interoperability, reliability and security of the IPv6 infrastructure.

TC MTS has produced the following ETSI TSs dealing with IPv6 security aspects:

- A catalogue of all of the security-related IPv6 requirements extracted from Internet Engineering Task Force (IETF) specifications [399]
- A Test Suite Structure and Test Purposes (TSS&TP) ([400]) for conformance tests of the security IPv6 protocol based on the requirements defined in [399]
- A specification for interoperability tests for IPv6 security [401]
- An Abstract Test Suite (ATS) [402] for the mobility functions of IPv6, based on [399] and [400]; this document provides a basis for conformance tests for IPv6 equipment to achieve a high probability of interoperability between IPv6 equipment from different manufacturers.

In the years 2004-2006 TC MTS has carried out an IPv6 Testing project co-funded by ETSI, the EC and EFTA (European Free Trade Association), taking into account the needs of bodies such as 3GPP and ETSI TC TISPAN. This project provided a publicly available test development framework for four key areas of IPv6: core protocols, security, mobility and migration from IPv4 to IPv6.

The security part of this work resulted in a conformance test suite containing 90 tests, covering IETF RFC 4306, i.e. Internet Key Exchange version 2 (IKEv2) later updated as RFC 5282, RFC 4302 i.e. Authentication Header (AH) and RFC 4303, i.e. Encapsulating Security Payload (ESP). The tests were based on authentication and hash algorithms such as HMAC-SHA1 (Hash-based Message Authentication Code – Secure Hash Algorithm 1) and HMAC-MD5 (Hash-based Message Authentication Code – Message Digest 5), and encryption algorithms such as DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard) and AES (Advanced Encryption Standard).

ePassport Readers

From January 2010 to August 2011 ETSI conducted a project, co-financed by the European Union (EU) and European Free Trade Association (EFTA), to develop a Test System Prototype for Conformance Testing of ePassport readers.

The objective of this project was to design, build and test a TTCN-3 based Test System Prototype for ePassport Reader Conformance Testing. This project was a joint effort between the EC Joint Research Centre (JRC) and ETSI.

TTCN-3 (Testing and Test Control Notation Version 3) is an internationally standardized programming language that has been specifically designed for use in specifying and controlling testing scenarios. TTCN-3 has been developed and is maintained by the ETSI TC Methods for Testing and Specification (MTS).

As an outcome of the ePassport Readers project, ETSI TC MTS published a report on ePassport Readers Interoperability Support; Framework for Developing Conformance Test Specifications [403]. This deliverable contains an extended selection of test purposes, the Abstract Test Suite of the sample test cases, a report on the validation of the prototype and the lab procedure for standardized test reporting.

IPCablecom™

IPCablecom is a technology which provides high quality, secure communications using IP over the cable television network. ETSI has set standards defining the protocols and functional requirements for this technology in its Technical Committee for Access and Terminals (TC AT), which was merged with the TC Transmission and Multiplexing (TM) in January 2007, to become Technical Committee for Access, Terminals, Transmission and Multiplexing (TC ATTM).

In 2012, ETSI has placed a renewed focus on IPCablecom standardization, with the creation of a dedicated Technical Committee on the subject, TC Cable. IPCablecom work ongoing in TC ATTM was then moved to the new committee.

Security is a key issue for IPCablecom, since it is a shared network providing valuable content. As well as the standards on Lawful Interception ([158] and [159]), TC AT has produced a security specification for the technology [404], covering security for the entire IPCablecom architecture, identifying security risks and specifying mechanisms to secure the architecture.

TC CABLE has delivered an ETSI standard for requirements for both CMTSs (Cable Modem Termination Systems) and CMs (Cable Modems) in order to implement a DOCSIS (Data-Over Cable Service Interface Specifications) Layer-2 Virtual Private Network (DOCSIS L2VPN) feature [405]. The L2VPN feature allows cable operators to offer a Layer 2 Transparent LAN Service (TLS) to commercial enterprises.

Other Security Issues

Over the years, ETSI has produced numerous standards, specifications and reports covering generic security aspects including:

- a comprehensive glossary for security terminology ([406] and [413])
- a guide for the selection and application of basic security mechanisms ([416] and [420])
- a guide for ETSI Technical Committees on the inclusion of security features in their Technical Specifications and Reports ([410] and [411])
- a guide to specifying requirements for cryptographic algorithms ([407], [408], [417], [418] and [419])
- a report providing guidance to the availability and use of methods for the development of ETSI security standards ([423]).

In addition, to maintain coherence and coordination within ETSI, the Institute has produced documents offering an overall assessment of work done in the field of security ([414] and [422]).

Conclusions

This latest edition of the ETSI Security White Paper illustrates how, since its inception, ETSI has steadily advanced the standardization of security across the whole spectrum of ICT, from algorithms to smart cards, from mobile and mobile telecommunication infrastructures to electronic signatures, from Lawful Interception to broadcasting and lately Machine to Machine and Smart Grids among others. As a result, ETSI has developed exceptional expertise along with a unique vision of security in ICT as a whole.

As ICT becomes ever more essential for business, public administration, public safety and commercial needs, a vast number of new technologies are being developed and becoming mature for standardization. Security is not an additional feature that can be patched on after the adoption of a technology: it must be taken into account from the beginning of the standardization process. Indeed, in many cases it can be a winning driver that enables the overall success of the technology, and with increasing demands of privacy and integrity of data it is legally essential for businesses which generate and handle user or customer data.

The threat to the security of our ICT systems grows daily. There is increased interest in defending national and critical infrastructure through Cybersecurity, and innovations such as cloud computing emphasize the need for good security. Experience has revealed many breaches of security that have had a significant impact on ICT systems, whether the causes were deliberate or accidental. Ways must be found to protect customers. There has also been a noticeable increase in legislation world-wide, driven by growing security concerns in recent years. These continue to drive our activities.

Solutions will certainly include a reliable and secure network infrastructure. But they will also depend on trust on the part of users - both citizens and businesses - that privacy, confidentiality, secure identification and other issues are rightly addressed. Security standardization, sometimes in support of legislative actions, therefore has an important role to play in the future development of ICT.

Technology is constantly evolving. Criminals are becoming ever more inventive. The personal security of the individual citizen is far too frequently at risk from privacy threats, terrorism and natural disasters. Security standardization must evolve too to keep pace with the developing risks and threats. Throughout its lifetime, ETSI has already proved it can adapt to changing situations; it will continue to do so, moving into new technical areas as they emerge and tackling new issues.

Publications

The following publications are ETSI documents, available for download free from the ETSI website[1] (www.etsi.org/specifications). Each ETSI document number in the list below links to the verison of the ETSI deliverable available on line at the time of writing.

GSM and UMTS

[1] ETSI TR 101 105 (SMG 10): "Digital cellular telecommunications system (Phase 2+); Fraud Information Gathering System (FIGS); Service requirements - Stage 0 (GSM 01.31)".

[2] ETSI TR 101 514 (SMG 10): "Digital cellular telecommunications system (Phase 2+); Lawful interception requirements for GSM (GSM 01.33)".

[3] ETSI TS 101 106 (SMG 10): "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements (GSM 01.61)".

[4] ETSI TS 100 920 (SMG 01): "Digital cellular telecommunications system (Phase 2+); Security aspects (3GPP TS 02.09)".

[5] ETSI TS 101 107 (SMG 10): "Digital cellular telecommunications system (Phase 2+) (GSM); Fraud Information Gathering System (FIGS); Service description - Stage 1 (GSM 02.31)".

[6] ETSI TS 101 749 (SMG 10): "Digital cellular telecommunications system (Phase 2+); Immediate Service Termination (IST) Service description - Stage 1 (GSM 02.32)".

[7] ETSI TS 101 507 (SMG 10): "Digital cellular telecommunications system (Phase 2+); Lawful interception - Stage 1 (GSM 02.33)".

[8] ETSI TS 100 929 (SMG 03): "Digital cellular telecommunications system (Phase 2+); Security-related network functions (3GPP TS 03.20)".

[9] ETSI TS 101 509 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+) (GSM); Lawful interception; Stage 2 (3GPP TS 03.33)".

[10] ETSI TS 101 967 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Immediate Service Termination (IST) (3GPP TS 03.35)".

[11] ETSI ETR 363 (SMG 10): "Digital cellular telecommunications system; Lawful interception requirements for GSM (GSM 10.20)".

[12] ETSI TS 121 133 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); 3G security; Security threats and requirements (3GPP TS 21.133)".

[13] ETSI TS 122 022 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Personalisation of Mobile Equipment (ME); Mobile functionality specification (3GPP TS 22.022)".

[14] ETSI TS 122 031 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Fraud Information Gathering System (FIGS); Service description; Stage 1 (3GPP TS 22.031)".

[1] Some deliverables that are relevant to security algorithms, or that are for internal use, are only available on a restricted basis. This is made explicit for each of these deliverables with the statement "NOT AVAILABLE FOR DOWNLOAD".

[15] ETSI TS 122 032 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Immediate Service Termination (IST); Service description; Stage 1 (3GPP TS 22.032)".

[16] ETSI TS 123 031 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Fraud Information Gathering System (FIGS); Service description; Stage 2 (3GPP TS 23.031)".

[17] ETSI TS 123 035 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Immediate Service Termination (IST); Stage 2 (3GPP TS 23.035)".

[18] ETSI TS 133 102 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Security architecture (3GPP TS 33.102)".

[19] ETSI TS 133 103 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); 3G Security; Integration Guidelines (3GPP TS 33.103)".

[20] ETSI TS 133 105 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; Cryptographic algorithm requirements (3GPP TS 33.105)".

[21] ETSI TS 133 106 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); Lawful interception requirements (3GPP TS 33.106)".

[22] ETSI TS 133 107 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Lawful interception architecture and functions (3GPP TS 33.107)".

[23] ETSI TS 133 108 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)".

[24] ETSI TS 133 120 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); 3G Security; Security Principles and Objectives (3GPP TS 33.120)".

[25] ETSI TS 133 141 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; Presence service; Security (3GPP TS 33.141)".

[26] ETSI TS 133 200 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); 3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security (3GPP TS 33.200)".

[27] ETSI TS 133 203 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Access security for IP-based services (3GPP TS 33.203)".

[28] ETSI TS 133 210 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

[29] ETSI TS 133 220 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Generic bootstrapping architecture (3GPP TS 33.220)".

[30] ETSI TS 133 221 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Support for subscriber certificates (3GPP TS 33.221)".

[31] ETSI TS 133 222 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (3GPP TS 33.222)".

[32] ETSI TS 133 234 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234)".

[33] ETSI TS 133 246 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS) (3GPP TS 33.246)".

[34] ETSI TS 133 310 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310)".

[35] ETSI TS 142 009 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Security aspects (3GPP TS 42.009)".

[36] ETSI TS 133 204 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) user security (3GPP TS 33.204)".

[37] ETSI TR 133 980 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA) (3GPP TR 33.980)".

[38] ETSI TR 133 901 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); 3G Security - Criteria for cryptographic Algorithm design process (3G TR 33.901)".

[39] ETSI TR 133 902 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol (3GPP TR 33.902)".

[40] ETSI TR 133 908 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms (3GPP TR 33.908)".

[41] ETSI TR 133 909 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); 3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions (3GPP TR 33.909)".

[42] ETSI TR 133 919 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Generic Authentication Architecture (GAA); System description (3GPP TR 33.919)".

[43] ETSI TR 133 918 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Early implementation of Hypertext Transfer Protocol over Transport Layer Security (HTTPS) connection between a Universal Integrated Circuit Card (UICC) and a Network Application Function (NAF) (3GPP TR 33.918)".

[44] ETSI TR 133 978 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; Security aspects of early IP Multimedia Subsystem (IMS) (3GPP TR 33.978)".

[45] ETSI TS 135 201 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specification (3GPP TS 35.201)".

[46] ETSI TS 135 202 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification (3GPP TS 35.202)".

[47] ETSI TS 135 203 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data (3GPP TS 35.203)".

[48] ETSI TS 135 204 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data (3GPP TS 35.204)".

[49] ETSI TS 135 205 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General (3GPP TS 35.205)".

[50] ETSI TS 135 206 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification (3GPP TS 35.206)".

[51] ETSI TS 135 207 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors’ test data (3GPP TS 35.207)".

[52] ETSI TS 135 208 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data (3GPP TS 35.208)".

[53] ETSI TR 135 909 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation (3GPP TR 35.909)".

[54] ETSI TR 141 031 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Fraud Information Gathering System (FIGS); Service requirements; Stage 0 (3GPP TR 41.031)".

[55] ETSI TR 141 033 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Lawful Interception requirements for GSM (3GPP TR 41.033)".

[56] ETSI TS 142 033 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 1 (3GPP TS 42.033)".

[57] ETSI TS 143 020 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Security-related network functions (3GPP TS 43.020)".

[58] ETSI TS 143 033 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); 3G security; Lawful Interception; Stage 2 (3GPP TS 43.033)".

[59] ETSI TS 155 205 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8 (3GPP TS 55.205)".

[60] ETSI TS 155 216 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Specification of the A5/3 encryption algorithms for GSM and ECSD, and the GEA3 encryption algorithm for GPRS; Document 1: A5/3 and GEA3 specification (3GPP TS 55.216)".

[61] ETSI TS 155 217 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Specification of the A5/3 encryption algorithms for GSM and ECSD, and the GEA3 encryption algorithm for GPRS; Document 2: Implementors' test data (3GPP TS 55.217)".

[62] ETSI TS 155 218 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Specification of the A5/3 encryption algorithms for GSM and ECSD, and the GEA3 encryption algorithm for GPRS; Document 3: Design and conformance test data (3GPP TS 55.218)".

[63] ETSI TR 155 919 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Specification of the A5/3 encryption algorithms for GSM and ECSD, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report (3GPP TR 55.919)".

[64] ETSI TS 155 226 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); 3G Security; Specification of the A5/4 Encryption Algorithms for GSM and ECSD, and the GEA4 Encryption Algorithm for GPRS (3GPP TS 55.226)".

[65] ETSI TS 122 016 (3GPP SA 1): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; International Mobile Equipment Identities (IMEI) (3GPP TS 22.016)".

[66] ETSI TS 123 003 (3GPP CT 4): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003)".

[67] ETSI TS 122 242 (3GPP SA 1): "Universal Mobile Telecommunications System (UMTS); LTE; Digital Rights Management (DRM); Stage 1 (3GPP TS 22.242)".

[68] ETSI TR 122 950 (3GPP SA 1): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Priority service feasibility study (3GPP TR 22.950)".

[69] ETSI TR 122 952 (3GPP SA 1): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Priority service guide (3GPP TR 22.952)".

[70] ETSI TS 101 513 (3GPP SA 5): "Digital cellular telecommunications system (Phase 2+) (GSM); Location Services (LCS); Location services management (GSM 12.71)".

[71] ETSI TS 101 724 (3GPP SA 2): "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Functional description; Stage 2 (3GPP TS 03.71)".

[72] ETSI TS 101 726 (3GPP GERAN 2): "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Serving Mobile Location Centre - Base Station System (SMLC-BSS) interface; Layer 3 (3GPP TS 08.71)".

[73] ETSI TS 101 725 (3GPP GERAN 2): "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Mobile radio interface layer 3 specification (3GPP TS 04.71)".

[74] ETSI TS 123 119 (3GPP CT 4): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Gateway Location Register (GLR); Stage2 (3GPP TS 23.119)".

[75] ETSI TS 124 008 (3GPP CT 1): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008)".

[76] ETSI TS 100 614 (SMG 06): "Digital cellular telecommunications system (Phase 2+) (GSM); Security management (GSM 12.03)".

[77] ETSI ETS 300 506 (SMG 01): "Digital cellular telecommunications system (Phase 2) (GSM); Security aspects (GSM 02.09)".

[78] ETSI EN 302 480 (ERM/MSG GSMOBA): "Electromagnetic compatibility and Radio spectrum Matters (ERM); Harmonized EN for the GSM onboard aircraft system covering the essential requirements of Article 3.2 of the R&TTE Directive".

[79] ETSI TR 122 907: "Universal Mobile Telecommunications System (UMTS); Terminal and smart card concepts (3G TR 22.907)".

[80] ETSI TS 133 320 (3GPP SA 3): "Universal Mobile Telecommunications System (UMTS); LTE; Security of Home Node B (HNB) / Home evolved Node B (HeNB) (3GPP TS 33.320)".

[81] ETSI TS 133 401 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401)".

[82] ETSI TS 133 402 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses (3GPP TS 33.402)".

[83] ETSI TS 122 228 (3GPP SA1): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1 (3GPP TS 22.228)".

[84] ETSI TS 122 278 (3GPP SA1): "Universal Mobile Telecommunications System (UMTS); LTE; Service requirements for the Evolved Packet System (EPS) (3GPP TS 22.278)".

[85] ETSI TS 133 328 (3GPP SA3): "Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS) media plane security (3GPP TS 33.328)".

[86] ETSI TS 135 231: ""Universal Mobile Telecommunications System (UMTS); LTE; Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm specification (3GPP TS 35.231)".

[87] ETSI TS 135 232: "Universal Mobile Telecommunications System (UMTS); LTE; Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Implementers' test data (3GPP TS 35.232)".

[88] ETSI TS 135 233: "Universal Mobile Telecommunications System (UMTS); LTE; Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Design conformance test data (3GPP TS 35.233)".

[89] ETSI TS 133 187: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements (3GPP TS 33.187)".

[90] ETSI TS 133 303: "Universal Mobile Telecommunications System (UMTS); LTE; Proximity-based Services (ProSe); Security aspects (3GPP TS 33.303)".

[91] ETSI TR 133 871: "Universal Mobile Telecommunications System (UMTS); LTE; Study on Security for WebRTC IMS Client access to IMS (3GPP TR 33.871)".

TETRA

[92] ETSI TR 102 021-7: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 7: Security".

[93] ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[94] ETSI EN 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

[95] ETSI ES 202 109: "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption".

[96] ETSI EN 300 812: "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 3: Integrated Circuit (IC); Physical, logical and TSIM application characteristics".

[97] ETSI ES 200 812-1: "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (TSIM-ME) interface; Part 1: Universal Integrated Circuit Card (UICC); Physical and logical characteristics".

[98] ETSI ES 200 812-2: "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (TSIM-ME) interface; Part 2: Universal Integrated Circuit Card (UICC); Characteristics of the TSIM application".

DECT

[99] ETSI EN 300 175-7: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features".

[100] ETSI EN 300 176-1: "Digital Enhanced Cordless Telecommunications (DECT); Test specification; Part 1: Radio".

[101] ETSI ETS 300 759: "Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM); Test specification for DAM".

[102] ETSI ETS 300 760: "Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM); Implementation Conformance Statement (ICS) proforma specification".

[103] ETSI ETS 300 825: "Digital Enhanced Cordless Telecommunications (DECT); 3 Volt DECT Authentication Module (DAM)".

[104] ETSI EN 300 175-6: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing".

RFID

[105] ETSI EN 302 208-1 (ERM TG34): "Electromagnetic compatibility and Radio spectrum Matters (ERM); Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W; Part 1: Technical requirements and methods of measurement".

[106] ETSI EN 302 208-2 (ERM TG34): "Electromagnetic compatibility and Radio spectrum Matters (ERM); Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W; Part 2: Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive".

[107] ETSI TR 102 436 (ERM TG34): "Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD) intended for operation in the band 865 MHz to 868 MHz; Guidelines for the installation and commissioning of Radio Frequency Identification (RFID) equipment at UHF".

[108] ETSI TR 187 020 (TISPAN WG7): "Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436".

[109] ETSI TR 101 543 (ERM TG34): "Electromagnetic compatibility and Radio spectrum Matters (ERM); RFID evaluation tests undertaken in support of M/436 Phase 1".

RRS

[110] ETSI TR 102 745 (RRS WG4): "Reconfigurable Radio Systems (RRS); User Requirements for Public Safety".

Satellite

[111] ETSI TR 102 287: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); IP Interworking over satellite; Security aspects".

[112] ETSI TS 102 465 (SES BSM): "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); General Security Architecture".

[113] ETSI TS 102 466 (SES BSM): "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Multicast Security Architecture".

[114] ETSI TS 101 376-3-9: "GEO-Mobile Radio Interface Specifications; Part 3: Network specifications; Sub-part 9: Security related Network Functions; GMR-1 03.020".

[115] ETSI TS 101 377-2-3 (SES GMR): "GEO-Mobile Radio Interface Specifications; Part 2: Service specifications; Sub-part 3: Security Aspects; GMR-2 02.009".

[116] ETSI TS 101 377-3-10 (SES GMR): "GEO-Mobile Radio Interface Specifications; Part 3: Network specifications; Sub-part 10: Security related Network Functions; GMR-2 03.020".

[117] ETSI TS 102 442-6: "Satellite Earth Stations and Systems (SES); Satellite Component of UMTS/IMT-2000; Multimedia Broadcast/Multicast Services; Part 6: Security".

Intelligent Transport Systems

[118] ETSI TS 102 867: "Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2".

[119] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

[120] ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".

[121] ETSI TS 102 942: "Intelligent Transport Systems (ITS); Security; Access Control".

[122] ETSI TS 102 943: "Intelligent Transport Systems (ITS); Security; Confidentiality services".

[123] ETSI TS 103 096-1: "Intelligent Transport Systems (ITS); Testing; Conformance test specification for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)".

[124] ETSI TS 103 096-2: "Intelligent Transport Systems (ITS); Testing; Conformance test specification for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS&TP)".

[125] ETSI TS 103 096-3: "Intelligent Transport Systems (ITS); Testing; Conformance test specification for ITS Security; Part 3: Protocol Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".

[126] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[127] ETSI TR 103 099: "Intelligent Transport Systems (ITS); Architecture of conformance validation framework".

Machine to Machine

[128] ETSI TR 103 167: "Machine to Machine (M2M); Threat analysis and counter measures to M2M service layer".

[129] ETSI TS 102 690: "Machine-to-Machine communications (M2M); Functional architecture".

[130] ETSI TS 102 921: "Machine-to-Machine communications (M2M); mIa, dIa and mId interfaces".

[131] ETSI TS 118 103: "Security solutions" (oneM2M).

[132] ETSI TR 118 508: "Analysis of Security Solutions for the oneM2M System" (oneM2M).

Lawful interception

Published by TC LI

[133] ETSI ES 201 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[134] ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".

[135] ETSI TS 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".

[136] ETSI TR 102 519: "Lawful Interception of public Wireless LAN Internet Access".

[137] ETSI TR 102 528: "Lawful Interception (LI) Interception domain Architecture for IP networks".

[138] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[139] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[140] ETSI TR 101 944: "Telecommunications security; Lawful Interception (LI); Issues on IP Interception".

[141] ETSI TR 102 503: "Lawful Interception (LI); ASN.1 Object Identifiers in Lawful Interception Specifications".

[142] 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".

[143] ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for messaging services".

[144] 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".

[145] 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".

[146] 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".

[147] 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".

[148] 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".

[149] ETSI TR 102 661: "Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment".

[150] ETSI TS 102 657: "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".

[151] ETSI TR 103 657: "Lawful Interception (LI); Retained data handling; System Architecture and Internal Interfaces".

[152] ETSI TR 103 690: "Lawful Interception (LI); eWarrant Interface".

Published by other ETSI Technical Committees[2]

[153] ETSI EG 201 781 (TC SPAN): "Intelligent Network (IN); Lawful interception".

[154] ETSI TR 101 772 (EP TIPHON): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service independent requirements definition; Lawful interception - top level requirements".

[155] ETSI TR 101 750 (EP TIPHON): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; Studies into the Impact of lawful interception".

[156] ETSI EN 301 040 (EP TETRA): "Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface".

[157] ETSI EG 201 040 (EP TETRA): "Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface; Feasibility study report" (This document has been made *historical*).

[158] ETSI TS 101 909-20-1 (AT Digital): "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based Voice Telephony Services".

[159] 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".

Electronic Signatures

[160] ETSI TR 102 044: "Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates".

[161] ETSI TR 102 045: "Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model".

[162] ETSI TR 102 046: "Electronic Signatures and Infrastructures (ESI); Maintenance report".

[163] ETSI TR 102 047: "Electronic Signatures and Infrastructures (ESI); International Harmonization of Electronic Signature Formats".

[164] ETSI TR 102 040: "Electronic Signatures and Infrastructures (ESI); International Harmonization of Policy Requirements for CAs issuing Certificates".

[165] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

[2] The lawful interception references for GSM and UMTS can be found among the GSM and UMTS references

[166] ETSI TS 102 158: "Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates".

[167] ETSI TR 102 153: "Electronic Signatures and Infrastructures (ESI); Pre-study on certificate profiles".

[168] ETSI SR 002 176: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures".

[169] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[170] ETSI TS 102 734: "Electronic Signatures and Infrastructures; Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES)".

[171] ETSI TS 102 280: "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".

[172] ETSI TR 102 272: "Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies".

[173] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[174] ETSI TR 102 437: "Electronic Signatures and Infrastructures (ESI); Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates)".

[175] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

[176] ETSI TR 102 317: "Electronic Signatures and Infrastructures (ESI); Process and tool for maintenance of ETSI deliverables".

[177] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[178] ETSI TS 102 904: "Electronic Signatures and Infrastructures; Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)".

[179] ETSI TS 101 862: "Electronic Signatures and Infrastructures (ESI); Qualified Certificate profile".

[180] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

[181] ETSI TS 102 176-2: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices".

[182] ETSI TR 102 041 (SEC ESI): "Signature Policies Report".

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

[184] ETSI TS 101 861: "Electronic Signatures and Infrastructures (ESI); Time stamping profile".

[185] ETSI TR 102 038 (SEC ESI): "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".

[186] ETSI TR 102 030 (SEC ESI): "Provision of harmonized Trust Service Provider status information".

[187] ETSI TR 102 438: "Electronic Signatures and Infrastructures (ESI); Application of Electronic Signature Standards in Europe".

[188] ETSI TR 102 458: "Electronic Signatures and Infrastructures (ESI); Mapping Comparison Matrix between the US Federal Bridge CA Certificate Policy and the European Qualified Certificate Policy (TS 101 456)".

[189] ETSI TR 102 605: "Electronic Signatures and Infrastructures (ESI); Registered E-Mail".

[190] ETSI TR 102 572: "Best Practices for handling electronic signatures and signed data for digital accounting".

[191] ETSI TS 102 573: "Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data for digital accounting".

[192] ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture".

[193] ETSI TS 102 640-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM".

[194] ETSI TS 102 640-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains".

[195] ETSI TS 102 640-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 4: REM-MD Assessment Profiles".

[196] ETSI TS 102 640-5: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles".

[197] ETSI TS 102 640-6-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 1: REM-MD UPU PReM Interoperability Profile".

[198] ETSI TS 102 640-6-2: " Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 2: REM-MD BUSDOX Interoperability Profile".

[199] ETSI TS 102 640-6-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 3: REM-MD SOAP Binding Profile".

[200] ETSI TS 102 778-1: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES".

[201] ETSI TS 102 778-2: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1".

[202] ETSI TS 102 778-3: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles".

[203] ETSI TS 102 778-4: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile".

[204] ETSI TS 102 778-5: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures".

[205] ETSI TS 102 778-6: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 6: Visual Representations of Electronic Signatures".

[206] ETSI TR 102 923: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signatures (PAdES); Usage and implementation guidelines".

[207] ETSI SR 003 232: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles (PAdES); Printable Representations of Electronic Signatures".

[208] ETSI TR 101 564: "Electronic Signatures and Infrastructures (ESI); Guidance on ETSI TS 102 042 for Issuing Extended Validation Certificates for Auditors and CSPs".

[209] ETSI TR 103 071: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Test suite for future REM interoperability test events".

[210] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[211] ETSI TR 101 533-2: "Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors".

[212] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

[213] ETSI SR 001 604: "Electronic Signatures and Infrastructures (ESI); Rationalised Framework for Electronic Signature Standardisation".

[214] ETSI TR 103 123:"Electronic Signatures and Infrastructures (ESI); Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates".

[215] ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

[216] ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[217] ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[218] ETSI TS 103 174: "Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile".

[219] ETSI TS 102 853: "Electronic Signatures and Infrastructures (ESI); Signature validation procedures and policies".

[220] ETSI TS 119 134-5: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signature (XAdES) Testing Compliance & Interoperability; Part 5: Conformance Testing for XAdES Baseline Profile".

[221] ETSI TS 119 144-2: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature (PAdES) Testing Compliance & Interoperability; Part 2: Test Suite for PAdES interoperability test events".

[222] ETSI TS 119 164-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) Testing Compliance & Interoperability; Part 2: Test Suite for ASiC interoperability test events".

[223] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures".

[224] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates".

[225] ETSI EN 319 411-3: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates".

[226] ETSI SR 003 091: "Electronic Signatures and Infrastructures (ESI); Recommendations on Governance and Audit Regime for CAB Forum Extended Validation and Baseline Certificates".

[227] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile".

[228] ETSI TS 119 412-2: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons".

[229] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[230] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[231] ETSI TS 119 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[232] ETSI SR 019 050: "Electronic Signatures and Infrastructures (ESI); Rationalized framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures".

Cyber Security

[233] ETSI TR 103 305: "Security Assurance by Default; Critical Security Controls for Effective Cyber Defence".

Network Functions Virtualisation

[234] ETSI GS NFV-SEC 001: "Network Functions Virtualisation (NFV); NFV Security; Problem Statement".

[235] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

Security Algorithms

[236] ETSI TCTR 003 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); European Encryption Algorithm for the use in audiovisual systems".

[237] ETSI TCTR 001 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); Requirements specification for an encryption algorithm for use in audio visual systems".

[238] ETSI TCTR 002 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); Report on the specification and evaluation of the GSM cipher algorithm A5/2".

[239] ETSI TCTR 004 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); Cryptographic Algorithm for the European Multi-Application IC-Card".

[240] ETSI TCTR 005 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); UPT Authentication Algorithm for the use in DTMF Devices".

[241] ETSI TCRTR 032: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TESA-7 algorithm".

[242] ETSI TCRTR 031: "Security Algorithms Group of Experts (SAGE); Universal Personal Telecommunication (UPT) authentication; Rules for the management of the USA-4".

[243] MI/SAGE-0008 - NOT AVAILABLE FOR DOWNLOAD: "Cryptographic algorithm for Public Network Operators".

[244] ETSI TCRTR 035: "Security Algorithms Group of Experts (SAGE); Rules for the management of the Baras algorithm".

[245] ETSI TR 101 053-1: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 1: TEA1".
NB: *the next version will be published as TS*

[246] MI/SAGE-00010-2 - NOT AVAILABLE FOR DOWNLOAD: "Standard Trans European Trunked RAdio (TETRA) air interface encryption algorithm TEA1 and TEA2".

[247] ETSI TS 101 053-2: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 2: TEA2".

[248] ETSI TR 101 052: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard authentication and key management algorithm set TAA1".

[249] MI/SAGE-00011-2 - NOT AVAILABLE FOR DOWNLOAD: "Standard Trans European Trunked RAdio (TETRA) set of air interface authentication and key management algorithms TAA1".

[250] ETSI TR 101 054: "Security Algorithms Group of Experts (SAGE); Rules for the management of the HIPERLAN Standard Encryption Algorithm (HSEA)".

[251] MI/SAGE-00012-2 - NOT AVAILABLE FOR DOWNLOAD: "Standard air interface encryption algorithm for HIPERLAN".

[252] ETSI ETR 277 (Edition 1): "Security Algorithms Group of Experts (SAGE); Requirements specification for an encryption algorithm for use in audio visual systems".

[253] ETSI ETR 278 (Edition 1): "Security Algorithms Group of Experts (SAGE); Report on the specification and evaluation of the GSM cipher algorithm A5/2".

[254] ETSI TR 101 375: "Security Algorithms Group of Experts (SAGE); Report on the specification, evaluation and usage of the GSM GPRS Encryption Algorithm (GEA)".

[255] MI/SAGE-00015-2 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); GPRS encryption algorithm".

[256] ETSI TR 101 690: "Security Algorithms Group of Experts (SAGE); Rules for the management of the GSM CTS standard Authentication and Key Generation Algorithms (CORDIAL)".

[257] MI/SAGE-00016-2 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); CTS Authentication and Key Generation Algorithm".

[258] MI/SAGE-00017-2 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); TEA3 and TEA4 Security Algorithms".

[259] ETSI TR 101 053-3: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 3: TEA3".
NB: *the next version will be published as TS.*

[260] ETSI TR 101 053-4: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 4: TEA4".
NB: *the next version will be published as TS*

[261] MI/SAGE-00018 - NOT AVAILABLE FOR DOWNLOAD: "Design of the 3GPP Encryption and Integrity algorithms".

[262] ETSI TR 101 740: "Security algorithms Group of Experts (SAGE); Rules of the management of the standard GSM GPRS Encryption Algorithm 2 (GEA2)".

[263] MI/SAGE-00019-2 - NOT AVAILABLE FOR DOWNLOAD: "Design of a Standard GSM GPRS Encryption algorithm 2 (GEA2)".

[264] MI/SAGE-00020-2 - NOT AVAILABLE FOR DOWNLOAD: "Design of authentication algorithm for UMTS".

[265] ETSI TS 135 215 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications (3GPP TS 35.215)".

[266] ETSI TS 135 216 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 2: SNOW 3G specification (3GPP TS 35.216)".

[267] ETSI TS 135 217 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 3: Implementors' test data (3GPP TS 35.217)".

[268] ETSI TS 135 218 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 4: Design conformance test data (3GPP TS 35.218)".

[269] ETSI TR 135 919 (3GPP SA 3): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 5: Design and evaluation report (3GPP TR 35.919)".

[270] ETSI TS 135 221 (3GPP SA 3): "Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications (3GPP TS 35.221)".

[271] ETSI TS 135 222 (3GPP SA 3): "Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 2: ZUC specification (3GPP TS 35.222)".

[272] ETSI TS 135 223 (3GPP SA 3): "Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data (3GPP TS 35.223)".

[273] ETSI TR 135 924 (3GPP SA 3): "Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 4: Design and Evaluation Report (3GPP TS 35.921)".

Quantum Key Distribution

[274] ETSI GS QKD 002: "Quantum Key Distribution (QKD); Use Cases".

[275] ETSI GS QKD 003: "Quantum Key Distribution (QKD); Components and Internal Interfaces".

[276] ETSI GS QKD 004: "Quantum Key Distribution (QKD); Application Interface".

[277] ETSI GS QKD 005: "Quantum Key Distribution (QKD); Security Proofs".

[278] ETSI GS QKD 008: "Quantum Key Distribution (QKD); QKD Module Security Specification".

Identity and Access Management for Networks and Services

[279] ETSI GS INS 001: "Identity and access management for Networks and Services; IdM Interoperability between Operators or ISPs with Enterprise".

[280] ETSI GS INS 002: "Identity and access management for Networks and Services; Distributed Access Control for Telecommunications; Use Cases and Requirements".

[281] ETSI GS INS 003: "Identity and access management for Networks and Services; Distributed User Profile Management; Using Network Operator as Identity Broker".

[282] ETSI GS INS 004: "Identity and access management for Networks and Services; Dynamic federation negotiation and trust management in IdM systems".

[283] ETSI GS INS 005: "Identity and access management for Networks and Services; Requirements of an Enforcement Framework in a Distributed Environment".

[284] ETSI GS INS 006: "Identity and access management for Networks and Services; Study to identify the need for a Global, Distributed Discovery Mechanism".

[285] ETSI GS INS 008: "Identity and access management for Networks and Services; Distributed access control enforcement framework; Architecture".

[286] ETSI GS INS 009: "Identity and access management for Networks and Services; Security and privacy requirements for collaborative cross domain network monitoring".

[287] ETSI GS INS 010: "Identity and access management for Networks and Services; Requirements of a global distributed discovery mechanism of identifiers, providers and capabilities".

Information Security Indicators

[288] ETSI GS ISI 001-1: "Information Security Indicators (ISI); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture".

[289] ETSI GS ISI 001-2: "Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1".

[290] ETSI GS ISI 002: "Information Security Indicators (ISI); Event Model; A security event classification model and taxonomy".

[291] ETSI GS ISI 003: "Information Security Indicators (ISI);
Key Performance Security Indicators (KPSI) for the evaluation of maturity detection of security events".

[292] ETSI GS ISI 004: "Information Security Indicators (ISI); Guidelines for event detection implementation".

Smart Cards

[293] ETSI TS 101 220: "Smart Cards; ETSI numbering system for telecommunication application providers".

[294] ETSI TS 102 124: "Smart Cards; Transport Protocol for UICC based Applications; Stage 1".

[295] ETSI TR 102 151: "Smart Cards; Measurement of Electromagnetic Emission of SIM Cards".

[296] ETSI TS 102 600: "Smart Cards; UICC-Terminal interface; Characteristics of the USB interface".

[297] ETSI TS 102 613: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics".

[298] ETSI TS 102 622: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) ".

[299] ETSI TS 102 483: "Smart cards; UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal".

[300] ETSI TS 102 484: "Smart Cards; Secure channel between a UICC and an end-point terminal".

[301] ETSI TS 102 588: "Smart Cards; Application invocation Application Programming Interface (API) by a UICC webserver for Java Card™ platform; ".

[302] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[303] ETSI TS 102 223: "Smart Cards; Card Application Toolkit (CAT) ".

[304] ETSI TS 102 224: "Smart Cards; Security mechanisms for UICC based Applications - Functional requirements".

[305] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications".

[306] ETSI TS 102 226: "Smart Cards; Remote APDU structure for UICC based applications".

[307] ETSI TS 102 230: "Smart cards; UICC-Terminal interface; Physical, electrical and logical test specification".

[308] ETSI TS 102 240: "Smart Cards; UICC Application Programming Interface and Loader Requirements; Service description".

[309] ETSI TS 102 222: "Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications".

[310] ETSI TS 102 310: "Smart Cards; Extensible Authentication Protocol support in the UICC (Release 6)".

[311] ETSI TS 102 705: "Smart Cards; UICC Application Programming Interface for Java Card™ for Contactless Applications".

[312] ETSI TS 102 694-1: "Smart Cards; Test specification for the Single Wire Protocol (SWP) interface; Part 1: Terminal features".

[313] ETSI TS 102 694-2: "Smart Cards; Test specification for the Single Wire Protocol (SWP) interface; Part 2: UICC features".

[314] ETSI TS 102 695-1: "Smart Cards; Test specification for the Host Controller Interface (HCI) Part 1: Terminal features".

[315] ETSI TS 102 695-2: "Smart Cards; Test specification for the Host Controller Interface (HCI);Part 2: UICC features".

[316] ETSI TS 102 695-3: "Smart Cards; Test specification for the Host Controller Interface (HCI) Part 3: Host Controller features".

[317] ETSI TS 102 922-1: "Smart Cards; Test specification for the ETSI aspects of the IC USB interface; Part 1: Terminal features".

[318] ETSI TS 102 922-2: "Smart Cards; Test specification for the ETSI aspects of the IC USB interface; Part 2: UICC features".

[319] ETSI TS 102 835: "Smart Cards; Test Specification for SCWS Application Invocation API for Java CardTM; Tests Environment and Annexes".

[320] ETSI TS 102 671: "Smart Cards; Machine to Machine UICC; Physical and logical characteristics".

[321] ETSI TS 103 484-1: "Smart Cards; Test specification for the Secure Channel interface; Part 1: Terminal features (Release 9)".

[322] ETSI TS 103 484-2: "Smart Cards; Test specification for the Secure Channel interface; Part 2: UICC features (Release 9)".

[323] ETSI TS 103 383: "Smart Cards; Embedded UICC; Requirements Specification (Release 12)".

Future Networks

[324] 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".

[325] 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".

[326] 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".

[327] ETSI TR 102 419: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security analysis of IPv6 application in telecommunications standards".

[328] ETSI TR 102 420: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of activity on security".

[329] ETSI TR 102 055: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); ENUM scenarios for user and infrastructure ENUM".

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

[331] 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".

[332] 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".

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

[334] 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".

[335] ETSI TS 102 165-2: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

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

[337] 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".

[338] ETSI TR 187 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study on Media Security in TISPAN NGN".

[339] ETSI TR 187 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NAT traversal feasibility study report".

[340] 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".

[341] 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".

[342] 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".

[343] ETSI TR 187 014: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); eSecurity; User Guide to eTVRA web-database".

[344] 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".

[345] ETSI TR 187 013: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study on IPTV Security Architecture".

[346] ETSI TR 187 015: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Prevention of Unsolicited Communication in the NGN".

[347] ETSI TS 187 016: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Identity Protection (Protection Profile)".

[348] ETSI TR 187 019: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility Study of Security of NGN Interconnection at the NNI for Release 3; Interconnection security".

[349] ETSI TS 187 021: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security services and mechanisms for customer premises networks connected to TISPAN NGN".

[350] ETSI TR 187 023: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Operational Security Assurance Profile; Statement of needs for security assurance measurement in operational telecom infrastructures".

Emergency Telecommunications

[351] ETSI TR 102 180: "Basis of requirements for communication of individuals with authorities/organizations in case of distress (Emergency call handling)".

[352] ETSI TR 102 299: "Emergency Communications; Collection of European Regulatory Texts and orientations".

[353] ETSI TS 102 181: "Emergency Communications (EMTEL); Requirements for communication between authorities/organizations during emergencies".

[354] ETSI TS 102 182: "Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies".

[355] ETSI TR 102 410: "Emergency Communications (EMTEL); Basis of requirements for communications between individuals and between individuals and authorities whilst emergencies are in progress".

[356] ETSI TR 102 444: "Emergency Communications (EMTEL); Analysis of the Short Message Service (SMS) and Cell Broadcast Service (CBS) for Emergency Messaging applications; Emergency Messaging; SMS and CBS".

[357] ETSI TR 102 445: "Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness".

[358] ETSI TR 102 476: "Emergency Communications (EMTEL); Emergency calls and VoIP: possible short and long term solutions and standardization activities".

[359] ETSI TS 102 900:" Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service".

[360] ETSI TS 170 001: "Project MESA; Service Specification Group - Services and Applications; Statement of Requirements (SoR)".

[361] ETSI TR 170 002: "Project MESA; Service Specification Group - Services and Applications; Definitions, symbols and abbreviations".

[362] ETSI TR 170 003: "Project MESA; Service Specification Group - Services and Applications; Basic requirements".

[363] ETSI TR 170 012: "Project MESA; Technical Specification Group - System; System Overview".

[364] ETSI TR 102 653: "Project MESA; Technical Specification Group - System; System and Network Architecture".

[365] ETSI TS 170 016: "Project MESA; Technical Specification Group - System; Functional Requirements Definition".

Broadcasting

[366] ETSI TS 101 197-1 (Broadcast): "Digital Video Broadcasting (DVB); DVB SimulCrypt; Part 1: Head-end architecture and synchronization".

[367] ETSI EN 300 744 (Broadcast): "Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television".

[368] ETSI EN 301 192 (Broadcast): "Digital Video Broadcasting (DVB); DVB specification for data broadcasting".

[369] ETSI TS 102 201 (Broadcast): "Digital Video Broadcasting (DVB); Interfaces for DVB Integrated Receiver Decoder (DVB-IRD)".

[370] ETSI TS 103 197 (Broadcast): "Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt".

[371] ETSI TS 102 822-7 (Broadcast): Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime Phase 1"); Part 7: Bi-directional metadata delivery protection".

[372] ETSI EN 301 790 (Broadcast): "Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems".

[373] ETSI TS 102 812 (Broadcast): "Digital Video Broadcasting (DVB); Multimedia Home Platform (MHP) Specification 1.1.1".

[374] ETSI TS 102 825-1 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 1: CPCM Abbreviations, Definitions and Terms ".

[375] ETSI TS 102 825-2 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 2: CPCM Reference Model".

[376] ETSI TS 102 825-3 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 3: CPCM Usage State Information".

[377] ETSI TS 102 825-4 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 4: CPCM System Specification".

[378] ETSI TS 102 825-5 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 5: CPCM Security Toolbox".

[379] ETSI TR 102 825-6 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 6: CPCM Security Test Vectors".

[380] ETSI TS 102 825-7 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 7: CPCM Authorized Domain Management".

[381] ETSI TR 102 825-8 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 8: CPCM Authorized Domain Management scenarios".

[382] ETSI TS 102 825-9 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 9: CPCM System Adaptation Layers".

[383] ETSI TS 102 825-10 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 10: CPCM Acquisition, Consumption and Export Mappings".

[384] ETSI TR 102 825-11 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 11: CPCM Content Management Scenarios".

[385] ETSI TR 102 825-12 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 12: CPCM Implementation Guidelines".

[386] ETSI TR 102 825-13 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 13: CPCM Compliance Framework".

[387] ETSI TS 102 825-14 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 14: CPCM Extensions".

[388] ETSI TS 101 545-1 (Broadcast): "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 1: Overview and System Level specification".

[389] ETSI EN 301 545-2 (Broadcast): "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 2: Lower Layers for Satellite standard".

[390] ETSI TS 101 545-3 (Broadcast): "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 3: Higher Layers Satellite specification".

[391] ETSI TR 101 545-4 (Broadcast): "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 4: Guidelines for Implementation and Use of EN 301 545-2".

[392] ETSI TR 101 545-5 (Broadcast): "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 5: Guidelines for the Implementation and Use of TS 101 545-3".

[393] ETSI TS 100 289 (Broadcast): "Digital Video Broadcasting (DVB); Support for use of the DVB Scrambling Algorithm version 3 within digital broadcasting systems ".

[394] ETSI TS 103 127 (Broadcast): "Digital Video Broadcasting (DVB); Content Scrambling Algorithms for DVB-IPTV Services using MPEG2 Transport Streams".

[395] ETSI TS 103 205 (Broadcast): "Digital Video Broadcasting (DVB); Extensions to the CI PlusTM Specification".

Content Media Distribution

[396] ETSI TR 101 532: "End-to-End Network Architectures (E2NA); Mechanisms addressing interoperability of multimedia service and content distribution and consumption with respect to CA/DRM solutions".

Security Testing

[397] ETSI TR 101 582: "Methods for Testing and Specification (MTS); Security Testing; Case Study Experiences".

[398] ETSI TR 101 583: "Methods for Testing and Specification (MTS); Security Testing; Basic Terminology".

IPv6

[399] ETSI TS 102 558: "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT): IPv6 Security; Requirements Catalogue".

[400] ETSI TS 102 593: "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT); IPv6 Security; Conformance Test Suite Structure and Test Purposes (TSS&TP)".

[401] ETSI TS 102 597: "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT): IPv6 Security; Interoperability Test Suite".

[402] ETSI TS 102 594: "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT): IPv6 Security; Conformance Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT) proforma".

ePassport Readers

[403] ETSI TR 103 200: "Methods for Testing and Specification (MTS); ePassport Readers Interoperability Support; Framework for Developing Conformance Test Specifications".

IP Cablecom

[404] ETSI TS 101 909-11: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 11: Security".

[405] ETSI ES 203 385: ""CABLE; DOCSIS® Layer 2 Virtual Private Networking"".

Generic Security Issues

[406] ETSI ETR 232 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Glossary of security terminology".

[407] ETSI TCRTR 037 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Requirements specification for an encryption algorithm for operators of European public telecommunications networks".

[408] ETSI ETR 235 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Requirements specification for an encryption algorithm for operators of European public telecommunications networks".

[409] ETSI ETR 331 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".

[410] ETSI TCRTR 038 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); A guide to the ETSI security standards policy".

[411] ETSI ETR 236 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); A guide to the ETSI security standards policy".

[412] ETSI TCRTR 049 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Security requirements capture".

[413] ETSI TCRTR 028 (Network Aspects (NA)): "Network Aspects (NA); Security Techniques Advisory Group (STAG); Glossary of security terminology".

[414] ETSI TCRTR 029 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); A directory of security features in ETSI standards".

[415] ETSI ETR 332 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Security requirements capture".

[416] ETSI TCRTR 042 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms".

[417] ETSI TCRTR 030 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); A guide to specifying requirements for cryptographic algorithms".

[418] ETSI ETR 234 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); A guide to specifying requirements for cryptographic algorithms".

[419] ETSI EG 200 234 (Network Aspects (NA)): "Telecommunications security; A guide to specifying requirements for cryptographic algorithms".

[420] ETSI ETR 237 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms".

[421] ETSI ETR 330 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); A guide to legislative and regulatory environment".

[422] ETSI SR 002 298: "Response from CEN and ETSI to the "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach"".

[423] ETSI TR 102 780: "Methods for Testing and Specification (MTS); Security; Guide to the use of methods in development of ETSI security standards".

Reference numbers of security-related documents added since the 6th Edition of this White Paper (January 2014):

[86], [87], [88], [89], [90], [91], [126], [127], [131], [132], [230], [231], [232], [233], [234], [235], [247], [287], [291], [391], [392], [393], [394], [395], [396], [397], [398] and [405].

Glossary

3DES	Triple Data Encryption Standard
3GPP™	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorization and Accounting
A-CDM	Airport Collaborative Decision Making
AES	Advanced Encryption Standard
AH	Authentication Header
AIS	Automatic Identification System
AKA	Authentication and Key Agreement
API	Application Programming Interface
ARIB	Association of Radio Industries and Businesses, Japan
AS	Application Server
ASiC	Associated Signature Containers
A-SMGCS	Advanced Surface Movement Guidance and Control System
ATIS	Alliance for Telecommunications Industry Solutions, US
ATM	Air Traffic Management
ATS	Abstract Test Suite
BUSDOX	Business Document Exchange Network
CA	Certification Authority
CA	Conditional Access *(broadcast systems)*
CAB	Certification Authority/Browser
CAB	Conformity Assessment Bodies
CAdES	CMS Advanced Electronic Signatures
CA/DRM	Conditional Access / Digital Rights Management
CCSA	China Communications Standards Association
CDN	Content Delivery Network
CM	Cable Modem
CMS	Cryptographic Message Syntax
CMTS	Cable Modem Termination System
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CEPT	European Conference of Posts and Telecommunications Administrations
CPCM	Content Protection and Copy Management
CPE	Customer Premises Equipment
CR	Cognitive Radio
CS	Circuit Switched
CSA3	Common Scrambling Algorithm version 3
CSG	Closed Subscriber Group
CSP	Communication Service Provider (*in Lawful Interception*)
CTI	Centre for Testing and Interoperability
DECT™	Digital Enhanced Cordless Telecommunications
DES	Data Encryption Standard

DLS	Data Link Services
DMO	Direct Mode Operation
DOCSIS	Data-Over Cable Service Interface Specifications
DRM	Digital Rights Management
DSAA	DECT Standard Authentication Algorithm
DSC	DECT Standard Cipher
DSC	Digital Selective Calling
DVB	Digital Video Broadcasting
E2NA	End-to-End Network Architectures
EAP	Extensible Authentication Protocol
EASA	European Aviation Safety Agency
EC	European Commission
ECMA	European Computer Manufacturers Association
EDGE	Enhanced Data Rates for GSM Evolution
EEA1	Evolved Packet System Encryption Algorithm 1
EFTA	European Free Trade Association
EIA1	Evolved Packet System Integrity Algorithm 1
EMTEL	Emergency Telecommunications (ETSI Special Committee)
ENISA	European Network and Information Security Agency
EP	ETSI Project
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
eTVRA	electronic Threat Vulnerability and Risk Analysis
EU	European Union
EVC	Extended Validation Certificate
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
FIGS	Fraud Information Gathering System
GAA/GBA	Generic Authentication Architecture / Generic Bootstrapping Architecture
GC	Group Communication
GCSE	Group Communication Enablers for LTE
GIBA	GPRS IMS Bundled Authentication
GMDSS	Global Maritime Distress and Safety System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GS	ETSI Group Specification
GSM™	Global System for Mobile Communication™
GSMOBA	GSM Onboard Aircraft
HMAC	Hash-based Message Authentication Code
HNB	Home Node B
H(e)NB	Home (e) Node B
HSDPA	High Speed Downlink Packet Access
HSUPA	High Speed Uplink Packet Access
ICT	Information and Communication Technologies

ID	Identification
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange version 2
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IOPS	Isolated E-UTRAN Operation for Public Safety
IoT	Internet of Things
IP	Internet Protocol
IPSec	IP Security
IPTV	Internet Protocol Television
IPv6	Internet Protocol version 6
ISG	Industry Specification Group of ETSI
ISIM	IMS Subscriber Identity Module
ISO	International Organisation for Standardisation
IT	Information Technology
ITS	Intelligent Transport System
JTC	Joint Technical Committee
KDF	Key Derivation Function
KMS	Key Management Server
L2VPN	Layer 2 Virtual Private Network
LI	Lawful Interception
LTE™	Long Term Evolution
M2M	Machine to Machine
MBMS	Multicast Broadcast Multimedia Service
MCPTT	Mission Critical Push To Talk over LTE
MD	Message Digest
MDF	Mobile Device Functionality
MNO	Mobile Network Operator
MME	Mobility Management Entity
MTC	Machine Type Communications
NAS	Non-Access Stratum
NASS	Network Access SubSystem
NAT	Network Address Translation
NENA	National Emergency Number Association
NFC	Near Field Communication
NFV	Network Functions Virtualization
NGN	Next Generation Networks
NIST	National Institute of Standards and Technology (USA)
NNI	Network to Network Interface
NSO	National Standard Organization
NTECH	Network Technologies
PAdES	PDF Advanced Electronic Signatures
PAMR	Public Access Mobile Radio

PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMR	Private Mobile Radio
PoF	Proof of Concept
ProSe	Proximity Services
PWS	Public Warning System
QKD	Quantum Key Distribution
RCS	Return Channel via Satellite
REM	Registered Electronic Mail
RFC	Request for Comment
RFID	Radio Frequency Identification
RN	Relay Node
RRC	Radio Resource Control
RRS	Reconfigurable Radio System
RTP	Real Time Protocol
SAE	System Architecture Evolution
SAS	Security Assurance Specification
SDES	Session Description Protocol Security Descriptions for Media Streams
SDN	Software Defined Network
SDR	Software Defined Radio
SES	Satellite Earth Stations & systems (ETSI Technical Committee)
SES	Single European Sky *(in Aeronautical)*
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SOLAS	Safety Of Life At Sea
SPI	Subscriber Privacy Impact
SR	Special Report
SRVCC	Single Radio Voice Call Continuity
SSL	Secure Socket Layer
ST	Security Target
STF	Specialist Task Force
TC	Technical Committee of ETSI
TDMA/TDD	Time Division Multiple Access/Time Division Duplex
TETRA	TErrestrial Trunked RAdio
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking (ETSI Technical Committee)
TLS	Transparent LAN Service

TLS	Transport Layer Security
TR	ETSI Technical Report
TS	ETSI Technical Specification
TSDSI	Telecommunications Standards Development Society, India
TSL	Trust-service Status List
TSS&TP	Test Suite Structure and Test Purposes
TTA	Telecommunications Technology Association, Korea
TTC	Telecommunication Technology Committee, Japan
TTCN-3	Testing and Test Control Notation Version 3
TVRA	Threat Vulnerability and Risk Analysis
UC	Unsolicited Communication
UE	User Equipment
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
ULE	Ultra Low Energy
UHF	Ultra High Frequency
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
UPU	Universal Postal Union
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
WebRTC	Web Real Time Communication
WFA	Wi-Fi Alliance
WG	Working Group of an ETSI TC
WLAN	Wireless Local Area Network
XAdES	XML Advanced Electronic Signature
XML	eXtensible Markup Language
ZUC	Zu Chongzhi

ETSI (European Telecommunications Standards Institute)
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

This White Paper is issued for information only. It does not constitute an official or agreed position of ETSI, nor of its Members. The views expressed are entirely those of the author(s).

ETSI declines all responsibility for any errors and any loss or damage resulting from use of the contents of this White Paper.

ETSI also declines responsibility for any infringement of any third party's Intellectual Property Rights (IPR), but will be pleased to acknowledge any IPR and correct any infringement of which it is advised.