ETSI White Paper No. 1
Security for ICT - the Work of ETSI

Authors:
Carmine Rizzo (ETSI) and
Charles Brookson (Zeata Security)

Fourth edition – January 2012

ETSI
World Class Standards
European Telecommunications Standards Institute
F-06921 Sophia Antipolis Cedex, France
Tel +33 4 92 94 42 00 Fax +33 4 93 65 47 16
info@etsi.org www.etsi.org

Disclaimer
This White Paper is issued for information only. It does not constitute an official or agreed position of the European Telecommunications Standards Institute (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.

Copyright Notification
No part of this document may be reproduced except as authorised by written permission. The copyright and the foregoing restriction extend to reproduction in all media.
© European Telecommunications Standards Institute 2011. All rights reserved.
DECT™, PLUGTESTS™, UMTS™, TIPHON™, IMS™, INTEROPOLIS™, FORAPOLIS™, LTE™ and the TIPHON and ETSI logos are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organisational Partners.
GSM™, the Global System for Mobile communication, is a registered Trade Mark of the GSM Association.

About the authors

Dr. Carmine Rizzo, *CISA CISM CISSP CMP ITIL PRINCE2*

ETSI Security Standardisation Projects, ETSI Secretariat

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

He obtained a Degree (Laurea) 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 organisation 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, *CEng FIET FRSA M.Inst.ISP*

Director Zeata Security 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 that.

He is Chairman of the NISSG, a group that was set up to co-ordinate security standards amongst the three European Standards Organizations and other bodies outside Europe. He was also on the Permanent Stakeholders group of ENISA, the European Network and Information Security Agency.

He is also Chairman of ETSI OCG Security, which is responsible for security standardisation 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.

Security for ICT - the Work of ETSI

January 2012

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 fourth 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. New areas of work which have, or will have, security aspects have been included: Machine-to-Machine (M2M) Communications, Identity and Access Management for Networks and Services (INS) and new developments in 3GPP. Some details on Plugtests™ events related to security matters have been added.

CONTENTS

Page		ETSI Technical Committee / Partnership Project
3	**Foreword**	
4	**Introduction - The Organisation of Work in ETSI**	
5	**ETSI Security Workshops**	
6	**Mobile and Wireless Telecommunications**	
6	**GSM™ - background and achievements**	3GPP* - SMG**
8	**GSM™ - current work**	
9	**UMTS™**	3GPP*
10	**LTE™**	3GPP*
11	**HNB/H(e)NB**	3GPP*
12	**IP Multimedia Subsystem (IMS)**	3GPP*
13	**Relay Nodes**	3GPP*
14	**TETRA**	TETRA
16	**DECT™**	DECT
17	**Radio Frequency Identification (RFID)**	ERM (TG 34)
18	**Reconfigurable Radio Systems**	RRS
19	**Satellite**	SES
20	**Intelligent Transport Systems**	ITS
21	**Machine to Machine**	M2M
22	**Lawful Interception**	LI
23	**Data Retention**	LI
25	**Electronic Signatures**	ESI
29	**Algorithms**	SAGE
31	**Quantum Key Distribution**	QKD***
32	**Identity and Access Management for Networks and Services**	INS***
33	**Information Security Indicators**	ISI***
34	**Smart Cards**	SCP
37	**Next Generation Networks**	TISPAN (WG 7)
40	**Emergency and Safety Telecommunications**	
40	**EMTEL**	EMTEL
41	**MESA**	MESA* **
42	**Aeronautics**	AERO
43	**Broadcasting**	BROADCAST
45	**Media Content Delivery**	MCD
46	**IPv6**	MTS
47	**ePassport Readers**	MTS
48	**IPCablecom™**	ATTM
49	**Mobile Commerce**	M-COMM**
50	**Other Security Issues**	
51	**Conclusions**	
52	**Publications**	
72	**Glossary**	

* MESA and 3GPP are Partnership Projects of which ETSI is a co-founder
** MESA, SMG and M-COMM are closed, having successfully completed their work
*** QKD, INS and ISI are ETSI Industry Specification Groups (ISGs)

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

As a response to such challenges, Information 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 organisations, research bodies and universities.

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

ETSI 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.

Standardisation 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 Standardisation Projects, ETSI Secretariat

Charles Brookson, Chairman, ETSI OCG Security

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;
- Paul Reid and Ultan Mulligan for their help with the editorial content;
- For their precious and indispensable inputs and contributions, colleagues within and outside the ETSI Secretariat: Andrea Lorelli, Antoinette van Tricht, Bernt Mattsson, Chantal Bonardi, David Boswarthick, Dionisio Zumerle (special thanks as co-author of the first edition of this paper), Estelle Mancini, Igor Minaev, John Meredith, Laurent Velez, Francois Ennesser, Martin Arndt, Nathalie Martin, Scott Cadzow, Sonia Compans, Steve Babbage and Xavier Piednoir.

Carmine Rizzo

INTRODUCTION - THE ORGANISATION OF WORK IN ETSI

ETSI's work is organised into Technical Committees (TCs) and ETSI Partnership Projects. Supported by Working Groups (WG), each is responsible for producing and maintaining standards in its own technical area. The scope of some TCs is closely related to security aspects; others, including the Partnership Projects, 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 related to security cover Mobile/Wireless Communications, Emergency Telecommunications, Information Technology Infrastructure, Smart Cards, Fixed Communications and Security Algorithms. 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 group to co-ordinate security matters across the ETSI work areas. For this reason ETSI has created an Operational Co-ordination Group on Security (OCG SEC). Its primary role is to provide a horizontal co-ordination structure for security issues that will ensure that this work is considered appropriately in each ETSI TC and that any duplicate or conflicting work is detected and managed accordingly.

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 third edition of the ETSI Security White Paper published in December 2009.

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
DECT	Digital Enhanced Cordless Telecommunications
EMTEL	Special Committee on Emergency Telecommunications
ERM	Electromagnetic Compatibility and Radio Spectrum Matters
ESI	Electronic Signatures and Infrastructures
INS (ISG)	Identity and Access Management for Networks and Services
ISI (ISG)	Information Security Indicators
ITS	Intelligent Transport Systems
LI	Lawful Interception
M2M	Machine to Machine
M-COMM (closed TC)	Mobile Commerce
MCD	Media Content Distribution
MSG	Mobile Standards Group
MTS	Methods for Testing and Specification
QKD (ISG)	Quantum Key Distribution (Industry Specification Group)
RRS	Reconfigurable Radio Systems
RT	Railways Telecommunications
SAGE	Security Algorithms Group of Experts
SCP	Smart Card Platform
SES	Satellite Earth Stations and Systems
SMG (closed TC)	Special Mobile Group
TETRA	Terrestrial Trunked Radio
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking

ETSI Security Workshops

Each year, in January, ETSI organises a Security Workshop in its premises in Sophia Antipolis, France, attracting a large number of experts from all over the world. These events are highly appreciated for the quality and relevance of the presentations, many of them focusing on standardisation issues. They also provide valuable co-operation opportunities, and help set the direction for future standardisation work, in line with the requirements of ETSI Members. In recent years the discussions have focused increasingly on the broad issue of security innovation, and the role that security standards can and should play in such context.

Speakers are selected from a call for contributions, which is announced at

http://www.etsi.org/SECURITYWORKSHOP.

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

Information about all ETSI Security Workshops is available from the above link.

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 standardisation 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 standardisation 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).

Standardisation 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].

Standardisation 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.

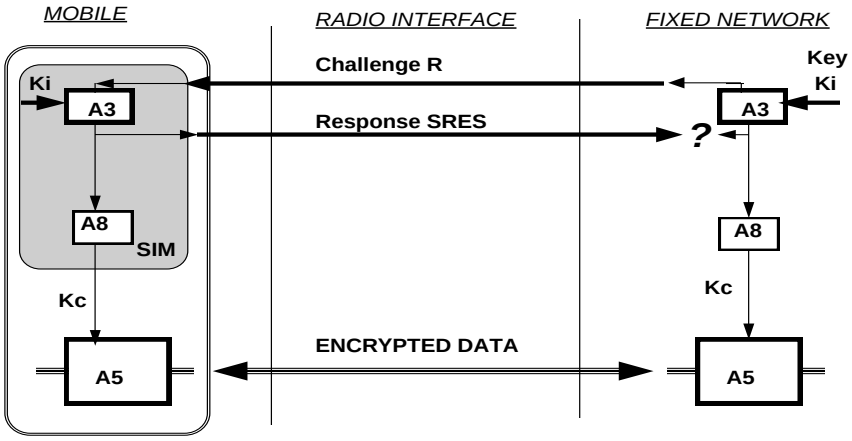
Anonymity - Anonymity entails preventing the tracking of the location of the user and preventing the identification of calls made to or from the user by eavesdropping on the radio path. Anonymity in GSM and UMTS is provided by using temporary identifiers when the feature is activated by the operator. 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 authorised 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 run up 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 standardisation 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 standardised by the joint ETSI group ERM/MSG GSMOBA, established in 2006. The European Harmonised 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 utilisation needs to be controlled by GSM (and GSM-R) operators. Properly controlled and authorised 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 standardisation organisations in Asia and the USA, plus organisations 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.

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 optimised 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 User Equipment (such as a mobile terminal) and the eNodeB (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).

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-optimised 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.

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-optimised 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 standardised 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 standardised 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.

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 recognised 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 standardisation 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.

Relay Nodes

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

Relay Node Security is addressed in Annex D of TS 133 401 for Release 10 [81], where a solution for Relay Node Security architecture and authentication is provided. 3GPP also published TR 33.816, a report providing guidance on Relay Node Security matters.

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 is responsible for producing specifications for TErrestrial Trunked RAdio (TETRA), a mobile radio communications infrastructure 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 standardisation 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 bombings in 2007), in the logistic support to the Olympic Games in Athens in 2004 and will be key to the management of the Olympic Games in London in 2012.

Based on digital, trunked radio technology, TETRA is the next-generation architecture and standard for current analogue PMR and PAMR markets taking lessons learned from mobile radio, digital cellular telephony, paging and wireless data to offer a multi-user secure infrastructure 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 [83], [84] and [85]):

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. Air interface security is intended to secure the connection between mobile stations and the network. This interface is essential to provide certain security functions in a mobile network. In addition, end-to-end security can be provided to offer a higher level of security. The use of several encryption algorithms, both standard and proprietary, is supported.

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 customised 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 of TETRA are currently being produced in which the extensions required to ensure TETRA remains at the leading edge of security provisions with the move to a data-centric, rather than voice-centric, network.

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 standardisation 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). In the latest version of the base standard DSAA2 and DSC2 have been introduced. These two algorithms strengthen the overall security of DECT.

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 unauthorised radio eavesdropping by third parties.

For an overview of the security features in DECT see [90].

Ongoing activities

TC DECT is currently working on "DECT New Gen", an upgrade of the DECT technology which will add more features to the base standard such as Wideband Speech, Broadband Data, Audio Streaming and Ultra Low Energy (ULE). New security mechanisms will be included.

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, RFID tags carry a relatively low amount of computational resources within the tag itself, which makes the use of standard cryptographic techniques 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 ([96] and [97]) and are updated regularly as necessary. A Technical Report providing guidelines for the installation and commissioning of RFID equipment at UHF was also published [98].

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 [99] published by TISPAN WG7. The future of this work is being actively pursued in a number of ETSI committees (TCs ERM TG34, TISPAN, Human Factors (HF)) in collaboration with partners in CEN.

ERM published a report [100] 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 [99].

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 standardisation 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 [101].

Ongoing activities

TC RRS is working on 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.

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 ([102], [103] and [104]) 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 ([105] to [107]). Similarly, another working group within TC SES has produced a Technical Specification for security aspects of the satellite component of UMTS [108]. 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 deals with security aspects in ITS. This group is developing standards focusing on securing vehicular communications, such as to prevent eavesdropping and distribution of malware to vehicles. The communications architectures 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 credential and identity management, privacy enhancing technologies and applications (providing pseudonymity and anonymity), integrity protection, authentication and authorisation.

The primary aim of the current work in ITS at ETSI is to provide improved road safety through collaborative working of vehicles. In this mode vehicles act as sensor nodes and inform, by broadcast, their current position. A receiving vehicle can then calculate speed and trajectory of all vehicles in the local vicinity and use the data as part of collision avoidance warning applications. The radio connection in this early ITS mode is short range 5.9GHz based on IEEE 802.11p technology for all informed networks, which obviously poses problems of key distribution. These are circumvented in the absence of an infrastructure by use of IEEE 1609.2 public key certificates and message sets backed by an elliptical curve asymmetric key set of processing algorithms. This may be able to raise trust in the data received but may also pose some privacy issues (tracking of vehicles is of particular concern), thus significant effort is being expended in ITS in resolving the issue of ensuring privacy of drivers and vehicles whilst ensuring viability of the core safety applications that require short term tracking of vehicles.

Future work in ITS will extend from the early work to cover media other than 5.9GHz and therefore incorporate the mechanisms from IP, 3G and other technologies to the security suite of ITS. In the area of malware prevention this will take the work of ETSI TC ESI in particular for the application of signed certificates and apply it to secure distribution of software to the ITS Station (ITS-S).

Machine to Machine (M2M)

ETSI TC Machine-to-Machine (M2M) specifies 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. TC M2M WG4 is in charge of the related security and privacy aspects.

Achievements

In 2011 TC M2M published its release 1 deliverables which support mutual authentication, key agreement and optional secure connection establishment between the Service layers of the Devices/Gateways and the supporting network [109], [110] and [111].The security may rely on the 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. One of the main challenges addressed by the TC M2M architecture relates to the bootstrapping of security credentials to a multitude of objects across various environments, potentially with different constraints in terms of computing resources. This is addressed in M2M release 1 by offering several options suitable for different scenarios.

Ongoing activities

Release 2 of TC M2M specifications may extend this scheme to provide end-to-end security to M2M applications, which is not covered in Release 1. TC M2M WG4 also provides specific inputs such as Threat analysis to support the work in European standardisation mandates where TC M2M is involved.

LAWFUL INTERCEPTION

Lawful Interception (LI) is the legally authorised process by which a network operator or service provider gives law enforcement officials access to the communications (telephone calls, e-mail messages etc) of private individuals or organisations. Lawful Interception is becoming crucial to preserve national security, to combat terrorism and in the investigation of serious criminal activities.

The standardisation of Lawful Interception is vital to provide an economically and technically feasible solution that complies with national and international conventions and legislation. ETSI has played a leading role in LI standardisation since 1991; today the work is concentrated in Technical Committee Lawful Interception (TC LI), which has the active participation of the major telecom manufacturers, network operators and regulatory authorities of Europe and from around the world.

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

NOTE: Handover in the context of LI and DR means the passing of data from the (Communication Service Provider) CSP to the Authorised Organisation (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 [117] and ES 201 671 [112]. 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 TISPAN, the committee in charge of creating the specifications for Next Generation Networks (NGN) in ETSI, as well as TC TETRA (who have passed the maintenance of the TETRA LI specification to TC LI), 3GPP and TC ATTM ([133] to [139]).

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

ETSI TC LI has standardised the general requirement placed on European network operators, service providers and access providers [113] 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 [118] relating to handover interfaces for the interception provides guidance for law enforcement agencies on the co-operation required by network operators/service providers with the lawful interception of telecommunications.

The specifications are subject to regular review and updating within ETSI to accommodate emerging needs, and are being used as the basis for specifying the procedures for LI. The increasing trend in the use of packet-switched technologies has necessitated the

production of standards for the delivery of IP-based interception. As a result, since LI has to be possible on several specific services that make use of the IP framework, a multi-part ETSI TS on the 'Handover Interface and Service-Specific Details (SSD) for IP delivery' has been published. This currently contains seven parts:

- part 1: Handover specification for IP delivery [123]
- part 2: SSD for e-mail services [124]
- part 3: SSD for Internet access services [125]
- part 4: SSD for Layer 2 services [126]; 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 [127]
- part 6: SSD for PSTN/ISDN services [128]
- part 7: SSD for Mobile Packet Services [129]

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 [122].

Two other TRs, published in 2006, cover Lawful Interception of public Wireless LAN Internet Access [115] and the Lawful Interception domain architecture for IP networks [116].

TC LI has produced a TR ([130]), which was published at the end of 2008, defining a security framework for securing Lawful Interception and Retained Data environment (see below) of the CSP and the Handover of the information.

ETSI organised two Plugtests™ events for TC LI in order to test the interoperability of equipment from different vendors against a number of TC LI specifications. During the first LI Plugtests™ event in 2006, the following TSs were tested: [123], [124], [125]. During the second LI Plugtests™ event in 2007, the following TSs were tested: [117], [123], [124], [127], [128]. The outcome of both events highlighted issues which were looked after by the TC LI through a number of updates to the relevant publications.

Data Retention

Data Retention is another vital subject for TC LI. The ability for Law Enforcement Agencies to request, and for operators and service providers to deliver, retained data are requirements of European Directive 2006/24/EC on the retention of data. TC LI has produced a TS [114] which deals with the requirements from Law Enforcement Agencies for the handling of Retained Data (RD). This document gives guidance for the delivery and associated issues of retained data of telecommunications and subscribers. It provides a set of requirements relating to handover interfaces for the retained traffic data and subscriber data by law enforcement and state security agencies and other authorised requesting authorities.

TC LI's work on Retained Data has been intense, and is now widely recognised worldwide. At the end of 2008 a Technical Specification was published ([131]) which standardises the Handover Interface (HI) for the request and delivery of retained subscriber and traffic data from a Network Operator, an Access Provider or a Service Provider (NWO/AP/SvP) to the Requesting Authority.

A report [132] on System Architecture and Internal Interfaces for Data Retention 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 Data Retention publications by updating them regularly.

In 2009 work started on a new TS providing a standardised mechanism for the dynamic triggering and revocation of the interception of communications content 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.

A TR is being drafted to provide generic recommendations for requests for handover and delivery of real-time or stored information referred to as an eWarrant Implementation Interface.

TC LI has started new work on DR/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 are intended to identify any DR/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.

Liaisons and Co-operations - As noted earlier, effective co-operation between organisations and committees working on Lawful Interception is imperative. TC LI works closely with other committees outside and within ETSI, including:

- The International Organisation for Standardisation (ISO) TC 204 on building an open dialogue on LI matters
- ETSI's TISPAN committee on LI in core networks
- ETSI's Operational Co-ordination 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 standardisation of Next Generation Networks (NGN)
- TC TISPAN on the provision of Retained Data in core networks.

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, and to protect against forgery of the data by the recipient.

Standards to support the use of electronic signatures and public key certificates are a key driver in enabling the successful evolution of electronic commerce. ETSI's Electronic Signatures and Infrastructures Technical Committee (TC ESI) is responsible for standardisation in the areas of electronic signatures and Public Key Infrastructure (PKI) to support electronic commerce 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. This addresses the issue of establishing a harmonised infrastructure for electronic signatures and the deployment of new vendor-specific infrastructures. In December 2009 the European Commission issued a standardisation mandate (M/460) aiming at achieving the interoperability of electronic signatures throughout Europe, by providing a rationalised European electronic signature standardisation framework which will allow mutual recognition and cross-border interoperability.

Achievements

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 [149]. An analogous twin specification was published defining XML Advanced Electronic Signature (XAdES) formats [157]. These documents were followed by two TSs on CAdES and XAdES profiles ([150] and [158]).

ETSI has organised several XAdES and CAdES Plugtests™ 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. It consists of 5 parts: Part 1 is a framework document for PAdES [180]. Part 2 describes how to use ISO 32000-1 for advanced and qualified electronics signatures satisfying the above-mentioned European Directive [181]. Parts 3 to 5 are profiles for advanced electronic signatures in PDF, equivalent to the profiles for CAdES and XAdES, and they support long-term validation features [182 to 184]. An additional part 6 [185] was created in 2010 to address the visual representation of electronic signatures, which enables untrained users to understand an electronic signature in its visible forms. A TR [186] 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 [187]. The Committee's work on PAdES has been forwarded to the International Organisation for Standardisation (ISO), specifically as input for new versions of ISO specifications on the use of the PDF and PDF Archive formats in electronic documents. The first PAdES remote Plugtests™ interoperability event was held at the end of 2011 with more than 35 participating organisations.

The following topics have been addressed by TC ESI, with a dual purpose: to provide electronic signature users with secure, and therefore reliable, tools, and to provide them with interoperable specifications to foster the uptake of, and trust in, electronic signatures:

- organisational and security requirements for Certificate Service Providers (CSPs) issuing qualified [153] and non-qualified [155] certificates (these documents are now in widespread use both within and beyond the bounds of the European Community); since 2008 the document [155] has been continually updated to include the policy requirements for issuing Extended Validation Certificates (EVCs) and for ensuring alignment of the Certification Authorities (CA) with the EVC guidelines issued by the CAB Forum (EVCs include standardised procedures for verifying and expressing the identity of the certificate holder); in 2010 the CAB Forum recognised the ETSI specification on policy requirements for certification authorities issuing public key certificates. This allows CAs to issue Extended Validation certificates in compliance with ETSI's policy requirements; see also [154], a TR which provides guidance on [153] and [188], a TR which provides guidance on [155] for Issuing Extended Validation Certificates for Auditors and CSPs;
- organisational and security requirements for Certificate Service Providers issuing attribute certificates [146] and for Time Stamping Authorities issuing Time Stamp Tokens [163];
- profiles for Qualified Certificates meeting the requirements laid down in the European Directive [159], to streamline Qualified Certificate based transactions, and for Time Stamp Tokens [164]; the profile for Qualified Certificates was subsequently supported by another TS [151] on profiling certificates issued to natural persons.

A number of Technical Reports (TRs) were also created to explain 'Signature Policy' to users ([141], [154], [162] and [165]).

Interoperation among the European Union member states is necessary to allow a user based in one state, relying on its rules, to ascertain whether certificates issued in another state are issued in compliance with that state's rules. This matter is addressed by a TS [145], which defines a standard for Trust-service Status Lists (TSLs). A TSL provides a harmonised 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. This TS was updated in 2009 to include Uniform Resouce Identifiers (URIs) and extensions to be used for the EU Member States' national Trusted Lists of supervised/accredited Certification Service Providers

In the final months of 2009 ETSI organised remote Plugtests™ events in order to verify the interoperability of tools supporting the various forms of TSLs as specified in [145]. This work was funded by the European Commission and had two phases: the first aimed at verifying that the TSLs published by each EU member state complies with [145]; the second sought to test that each EU member state can validate electronic signatures by using each others' TSLs. The outcome of these Plugtests™ events resulted in an update of [145].

TC ESI has worked on Digital Accounting, which is fundamental for boosting the advent of paperless accounting documentation (such as eInvoicing). This will increase business efficiency and reduce the potential for fraud. An ETSI TR was published in 2007 on best practices for handling signatures and signed data relevant for accounting [170], and an ETSI TS on policies of Trust Service Providers (TSPs) signing and/or storing data for accounting [171].

In recent years TC ESI has finalised its work on the creation of a Registered E-Mail (REM) framework for registered email services. In 2007 a TR was published [169] which provides a report on requirements survey for REMs. The REM framework specifications consists of 6 parts (TSs). In 2008 the first three parts were published [172 to 174] which provide a framework for origin authentication, proof of delivery and long term availability. The work specifies the format of the signatures to be applied on registered emails, In 2009, the work was completed with the definition of conformance and interoperability profiles in parts 4 and 5 [175 and 176]. In 2010 TC ESI's work on Registered Email (REM) has entered a new phase with part 6 consisting in three sub-parts [177] to [179] which specify interoperability between REM solutions based on different transport protocols. The specifications cover the interoperability of the ESI's REM solution using Simple Mail Transfer Protocol (SMTP) with the Universal Postal Union (UPU) [177], Business Document Exchange Network (BUSDOX) [179], and Simple Object Access Protocol (SOAP) [179] solutions. In addition, ESI developed test suites for future REM interoperability tests [189].

TC ESI initiated new work in 2010 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, 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). A TS was published in 2011 [190] to define system security provisions to ensure implementation and management of reliable long term information preservation systems based on time-stamping and/or electronic signatures. A TR was also published [191] to provide conformity assessment guidance, based on internationally recognised standards, addressing how to audit the systems by which Long Term Information Preservation services are provided.

In 2011, TC ESI also published a new TS [192] on Associated Signature containers, a package format for associating advanced electronic signatures with one or more files to which the signature applies.

The latest work focused on the execution of mandate M/460. The first deliverables have been produced with an updated set of hash functions and asymmetric algorithms for Advanced Electronic Signatures [160] and the publication of the update of 4 AdES baseline profiles. They will 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.

Ongoing activities

ETSI ESI current work focuses mainly on the execution of the European Commission (EC) Mandate on Electronic Signature Standardisation (M/460) for which CEN and ETSI are co-operating to ensure the alignment of standards and avoid overlapping work. ETSI ESI work covers:

- The definition of a rationalised standardisation framework (in collaboration with CEN). The deliverable includes an inventory of eSignature standards, a rationalised structure for the European e-signatures standardisation documents, a gap analysis, and a future work plan;
- Profiles for advanced electronic signatures in the context of the "Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market". After publication of the short term profiles, ESI is working on long-term profiles;
- CSP conformance assessment;
- An upgrade of the policy requirements for certification authorities issuing qualified certificates and public key certificates and their migration to EN status;
- An update to the qualified certificate profile and the certificate profile for natural persons;
- Procedures for signature verification;
- PAdES and ASiC interoperability tests specifications;
- XAdES Baseline profile conformance checker tool;

In addition, ESI is evaluating approaches to a governance and audit regime for assessment of CAs issuing EV certificates within the existing European framework for accreditation of CAs, as well as the existing framework for accreditation of IT Security auditors.

ALGORITHMS

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

Achievements

Accomplishments include algorithms for 3GPP [221], DECT, GSM and TETRA ([202] to [206], [216] and [217]), audiovisual services ([193], [194]), GPRS and Universal Personal Telecommunications (UPT) [199]. SAGE also collaborates with other ETSI committees to produce encryption algorithms.

All of the standardised 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 Organisational 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 ([222] to [226]). 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 also specified standardised 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 [227] to [230]. These algorithms (not published yet when this paper was published) 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 recent 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 relay on recently standardised changes to other network nodes to deliver a 128-bit key. Again, all of these algorithms were developed in collaboration with the 3GPP organisational partners ([59] to [63], [211], [212] and [219]), and are closely based on the UMTS algorithm UEA1.

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 utilisation 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.

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 standardisation 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 [231];

A definition of properties of components and internal interfaces of QKD Systems [232];

An evaluation of application interfaces over which a QKD system is attached to a cryptographic information and communication technology (ICT) system [233];

A study and systematisation 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 [234];

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 [235].

Ongoing activities

The focus of the ISG QKD is on defining common ontology, vocabulary and terms of reference for the quantum cryptography domain as well as on the requisites for the integration of QKD devices within a shared standard optical network infrastructure.

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.

Achievements

ISG INS published a first set of GSs to support interoperability and incorporate privacy into the telecoms services and networks domain. The objectives of these 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 [236];
- To provide requirements on the use and application of distributed policy management, decision and enforcement in a hybrid environment (operator and services domains) [237];
- 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 [238];
- 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 [239];
- To provide the requirements on the enforcement of policies in a distributed environment supporting interoperability between different players [240];
- 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 [241].

Ongoing activities

ISG INS currently works on two GSs addressing User Consent provisioning mechanisms and the architecture of the distributed access control enforcement framework, a GS on security and privacy requirements for distributed network monitoring in order to identify gaps regarding distributed processing and computation, protocols, and anonymized data exchange, and a GS to identify the requirements to develop a global distributed discovery of identifiers, providers and capabilities.

INFORMATION SECURITY INDICATORS (ISI)

ETSI's Industry Specification Group (ISG) Information Security Indicators was created in 2011 with 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,

SMART CARDS

A smart card generally takes the form of a credit card-sized token 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 being 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 credentials 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 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 expensive technology, as a range of strong security features and countermeasures are usually implemented to prevent unauthorised access to smart cards and tempering with the contained data.

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

- Definition of the physical features, such as form factor, physical constraints (e.g. temperature, humidity, bending) and electrical interfaces
- Definition of the logical features, from a platform or 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 organisations 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 is evolving 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 standardised 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 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.

Major achievements in 2010 and 2011 include:

- Creation of an Application Programming Interface (API) specification for Java Card™ contactless applications in TS 102 705 [260]
- Realisation of test specifications for the interface to a contactless front-end in the Terminal. Five specifications have been produced:
    - TS 102 694-1 [261] testing the Terminal aspects of the Single Wire Protocol
    - TS 102 694-2 [262] testing the UICC aspects of the Single Wire Protocol
    - TS 102 695-1 [263] testing the Terminal aspects of the Host Controller Interface
    - TS 102 695-2 [264] testing the UICC aspects of the Host Controller Interface
    - TS 102 695-3 [265] testing the aspects of the Host Controller Interface related to the contactless front-end
- Realisation of test specifications for the high-speed interface. Two specifications have been produced:
    - TS 102 922-1 [266] testing the Terminal aspects of the high-speed interface
    - TS 102 922-2 [267] testing the UICC aspects of the high-speed interface
- Realisation of a test specification for the Smart Card Web Server API in TS 102 835 [268]
- 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 TS 102 671 [269].

Overview of the other main work and specifications previous to 2010:

- Addition of a high-speed, physical interface for use in contact-based operation. This new interface, based on the Inter-Chip USB, enables higher speed communication alongside the use of a more common software communication stack. This specification was approved as TS 102 600 [245]

- 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 a pair of specifications:
    - for the physical interface and lower communication layer, the Single Wire Protocol was created, TS 102 613 [246]
    - for the logical interface, high-level communication and administration layer, the Host Controller Interface was created, TS 102 622 [247]
- Definition of IP connectivity for the UICC, TS 102 483 [248]
- Specification of a Secure Channel between the UICC and an endpoint, either platform to platform or application to application oriented, TS 102 484 [249]
- Delivery of an Application Programming Interface for the Smart Card Web Server (SCWS, defined by the Open Mobile Alliance, OMA), TS 102 588 [250]
- TS 102 221 [251] 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 realisation 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: 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:

- Embedded UICC: TC SCP started a work targeting the 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. The main focus of this work is to deliver new methods and technical solutions in order to securely and remotely provide access credentials on these Embedded UICCs (eUICC) and managing subscription changes from one MNO to another;
- Definition of an additional, smaller form factor for the UICC;
- Testing of the Secure Channel: a team of experts has been set up in order to deliver test specifications for the Terminal and the UICC aspects of the Secure Channel;
- Creation of a test specification for the contactless API;
- Creation of a conformance testing specification for the UICC aspects of TS 102 221 [251]; the testing of the Terminal aspects is in TS 102 230 [256].

NEXT GENERATION 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 new converged and access-independent network model - dubbed Next Generation Networks (NGN) - is based on the extensive use of IP, and is designed to accommodate the diversity of applications inherent in emerging broadband technologies. ETSI is already heavily committed to, and is well advanced in, developing the necessary standards to bridge disparate networks and domains and enable them to interoperate. Our work on NGN is being managed by Technical Committee TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) and security is one of its core concerns.

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

Achievements

When designing new architectures, security must be built in from the beginning - not patched on later. TC TISPAN established the security requirements for the subsystems of Next Generation Networks [276] in its first version (NGN Release 1) of the general network and service specifications for the convergence between the traditional public switched telephone networks (PSTNs) and the new IP-based networks.

In addition, TC TISPAN has produced a set of Security Design Guides ([270], [271] and [272]) which should be followed in the design of any new component of the network. This work references the guidelines on the use of the Common Criteria for the evaluation of IT security (ISO/IEC 15408). 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 unauthorised disclosure, modification or loss.

The publications deal with the issue of the application of the Common Criteria framework in the ETSI standardisation process and the development of protocols and architecture standards [272]. 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 [270] 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.

TC TISPAN has also provided additional guidance on the preparation of Security Targets (STs) based upon ETSI communication standards. 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 [273] 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).

TISPAN has addressed the challenge of security in Next Generation Networks with an analysis of risks and threats [278] and by defining an extensible NGN security architecture [279] (revision published in 2009).

TISPAN has also published an ETSI Guide on the application of security countermeasures to service capabilities [282], an analysis of security mechanisms for customer networks connected to TISPAN NGN Release 2 [283], a feasibility study on Media Security in TISPAN NGN [284], a NAT traversal feasibility study report [285], a feasibility study on the prevention of unsolicited communication in NGN [286], a report on the security of identity in NGN [287], and a report on the application of ISO 15408-2 requirements to ETSI standards (method and application with examples) [288].

For the purposes of Lawful Interception and data retention, TC TISPAN has identified appropriate interfaces, reference points and entities in the NGN architecture (see TS [277]) and has published a TR [290] providing guidance on compliance to the data retention directive (see section on Lawful Interception / Data Retention).

A TR providing guidance on the use of the ETSI eTVRA (electronic Threat Vulnerability and Risk Analysis) web application ([289]) acts as a tool for entering analysis results obtained through the ETSI TVRA method defined in [280].

Below are the new publications since the previous edition of this paper (December 2009):

- A report [291] 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 [292] 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 [293] on Identity Protection (Protection Profile) to provide countermeasures 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 [294] on a feasibility study of security of NGN interconnection at the NNI (Network to Network Interface), which addresses security issues related to inter-operator NNI interface interconnection and between the different subsystems of the NGN;

- A specification [295] 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 [296] on Operational Security Assurance Profile, which analyzes 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

TISPAN WG7 has work in progress in various areas for the security of the NGN, by updating previously published deliverables and working on the following new ones:

WG7 works in close collaboration with TC LI to publish a specification on Data Retention (DR) for the NGN. As already done for Lawful Interception [277], this document on Data Retention will include a mapping to the handover capabilities defined in TC LI for DR.

WG7 started a new TR on Smart Metering TVRA and Security Requirements. Measures need to be in place to ensure public acceptance of smart metering data security and privacy safeguards, so that consumers can be confident that their data is secure. Due account will be taken of work in other Standard Developing Organisations (SDOs) and ETSI TCs.

EMERGENCY AND SAFETY TELECOMMUNICATIONS

Emergency Telecommunications and Public Safety are areas requiring considerable standardisation 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 co-operating with other organisations around the globe.

EMTEL

Special Committee on Emergency Telecommunications (EMTEL) is the focal point in ETSI for the co-ordination 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 TC TISPAN, TC ERM, 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, National Emergency Number Association (NENA) and European projects. One example of this collaboration has been with TISPAN on the definition of protocols for the location identification of emergency calls.

Achievements

Among EMTEL's earliest achievements was the publication of two ETSI Technical Reports (TRs): on emergency call handling [297] and on the European regulations covering communication during emergency situations [298]. In collaboration with TC TETRA, EMTEL has been heavily involved with work on communications between authorities and organisations, leading to the publication of a Technical Specification (TS) on related matters [299], and a TS on communications from authorities/organisations to individuals, groups or the general public during emergencies [300].

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 ([301], [302], [303] and [304]).

EMTEL has also contributed to Public Warning System, as initially defined by 3GPP, with European requirements [305].

Ongoing activities

The four main EMTEL deliverables described above, [297], [298], [299] and [300] are considered as key documents for EMTEL and therefore regularly revised.

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 revolutionise 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 ([306] to [308]), whilst the MESA Technical Specification Group published a system overview [309], a system and network architecture document [310] and the system's functional requirements definition [311].

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 co-operation with the European Aviation Safety agency (EASA).

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 Standardisation (CENELEC). JTC Broadcast co-ordinates the drafting of standards for broadcasting and related fields. It is particularly active in response to the European Commission Mandate M/331 on Interactive Digital Television, which aims to improve interoperability and support the roll-out of digital interactive television.

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 personalised 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 250 broadcasters, manufacturers, network operators, software developers, regulatory bodies and others, in over 35 countries, 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. Approved by the Steering Board of the DVB Project, 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. A new version, known as CSA3, has recently been approved and is now available from ETSI. The various agreements, together with the licensing conditions, are available on the ETSI website at:

http://www.etsi.org/WebSite/OurServices/Algorithms/DVBCSA3Algorithm.aspx

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 [317] 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 102822 series.

A European Standard has been published on the Interaction channel for satellite distribution systems [318] known as DVB-RCS (Return Channel via Satellite).

An ETSI TR has been published related to production scrambling algorithms and IP or higher layer security mechanisms [319]. This TR has been revised [TS 100 289] 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.

The DVB Project has prepared the specifications that will form a multipart collection of TR and TS deliverables (14 parts, TR/TS 102 825-x) on CPCM (Content Protection and Copy Management). The 14 parts have been published [321] to [330] and [334].

An EN on Lower Layers for Satellite was published [335] as one of a multipart specification (3 parts) for a Second Generation DVB Interactive Satellite System (commonly named DVB-RCS2). The other two parts are TSs (see below).

Ongoing activities

Work is ongoing on two TSs which are Part 1 (an Overview and System Level specification) and part 3 (a Higher Layers for Satellite specification) for DVB-RCS2.

MEDIA CONTENT DISTRIBUTION

ETSI TC Media Content Distribution (MCD) has been created end of 2008 and addresses 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.

Ongoing activities

TC MCD is currently addressing MCD security aspects with a TR on the Architecture, Requirements and Mechanisms covering service and content interoperability of multimedia Customer Premises Equipment (CPE) with respect to Conditional Access and Digital Rights Management (CA/DRM) solutions. MCD Working Group Content Delivery Network-Interconnection (WG CDN-I) has started joint sessions with TISPAN WG7 in order to work on a new TS covering the security aspects of the MCD on CDN Interconnection uses cases and requirements.

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.

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.

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 [336]
- A Test Suite Structure and Test Purposes (TSS&TP) ([337]) for conformance tests of the security IPv6 protocol based on the requirements defined in [336]
- A specification for interoperability tests for IPv6 security [338]
- An Abstract Test Suite (ATS) [339] for the mobility functions of IPv6, based on [336] and [337]; 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 standardised 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 [340]. 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 standardised 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).

Security is a key issue for IPCablecom, since it is a shared network providing valuable content. As well as the standards on Lawful Interception ([138] and [139]), TC AT has produced a security specification for the technology [341], covering security for the entire IPCablecom architecture, identifying security risks and specifying mechanisms to secure the architecture.

MOBILE COMMERCE

ETSI undertook work on electronic payment for Mobile Commerce in its TC M-COMM.
Having successfully completed its work TC M-COMM has been closed in June 2003.

Achievements

ETSI produced specifications for the development of mobile signatures, which protect the end-user and the application provider from fraudulent behaviour from each other, and from third party hackers. Because a mobile signature is a universal method for using a mobile device to confirm the intention of a citizen to proceed with a transaction, the mobile signature service becomes a crucial security element within the architecture of the application provider itself.

ETSI's deliverables specify the requirements which must be fulfilled by a telecommunications system to support a payment system in a mobile commerce environment ([342] to [346]). They provide a wide and common understanding of the security considerations for mobile signatures and identify the level of security a mobile signature service provider should provide.

M-COMM deliverables are now attached to TC SCP who is in charge of any maintenance work, should it be required.

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 ([347] and [354])
- a guide for the selection and application of basic security mechanisms ([357] and [361])
- a guide for ETSI Technical Committees on the inclusion of security features in their Technical Specifications and Reports ([351] and [352])
- a guide to specifying requirements for cryptographic algorithms ([348], [349], [358], [359] and [360])
- a report providing guidance to the availability and use of methods for the development of ETSI security standards ([364]).

In addition, to maintain coherence and co-ordination within ETSI, the Institute has produced documents offering an overall assessment of work done in the field of security ([355] and [363]).

CONCLUSIONS

This latest edition of the ETSI Security White Paper illustrates how, since its inception, ETSI has steadily advanced the standardisation 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 standardisation. 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 standardisation 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 emphasise 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 standardisation, 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 standardisation 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] (pda.etsi.org/pda). Each ETSI document number in the list below links to the ETSI deliverable available **on line**, where the **latest published version** at the time of your search can be downloaded, as well as any previous versions.

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)".

TETRA

[83] ETSI TR 102 021-7: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 7: Security".
[84] ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
[85] ETSI EN 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".
[86] ETSI ES 202 109: "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption".
[87] 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".
[88] 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".
[89] 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

[90] ETSI EN 300 175-7: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features".
[91] ETSI EN 300 176-1: "Digital Enhanced Cordless Telecommunications (DECT); Test specification; Part 1: Radio".
[92] ETSI ETS 300 759: "Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM); Test specification for DAM".
[93] ETSI ETS 300 760: "Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM); Implementation Conformance Statement (ICS) proforma specification".
[94] ETSI ETS 300 825: "Digital Enhanced Cordless Telecommunications (DECT); 3 Volt DECT Authentication Module (DAM)".
[95] ETSI EN 300 175-6: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing".

RFID

[96] 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".
[97] 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".

[98] 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".

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

[100] 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

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

Satellite

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

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

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

[105] 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".

[106] 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".

[107] 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".

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

Machine to Machine

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

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

[111] ETSI TS 102 921 - NOT AVAILABLE FOR DOWNLOAD: "Machine-to-Machine communications (M2M); mIa, dIa and mId interfaces".

Lawful interception

Published by TC LI

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

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

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

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

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

[117] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".
[118] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".
[119] ETSI TR 102 053: "Telecommunications security; Lawful Interception (LI); Notes on ISDN lawful interception functionality".
[120] ETSI TR 101 944: "Telecommunications security; Lawful Interception (LI); Issues on IP Interception".
[121] ETSI TR 101 943: "Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture".
[122] ETSI TR 102 503: "Lawful Interception (LI); ASN.1 Object Identifiers in Lawful Interception Specifications".
[123] 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".
[124] ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for E-mail services".
[125] 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".
[126] 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".
[127] 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".
[128] 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".
[129] 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".
[130] ETSI TR 102 661: "Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment".
[131] ETSI TS 102 657: "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".
[132] ETSI TR 103 657: "Lawful Interception (LI); Retained data handling; System Architecture and Internal Interfaces".

Published by other ETSI Technical Committees[2]

[133] ETSI EG 201 781 (TC SPAN): "Intelligent Network (IN); Lawful interception".
[134] 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".
[135] ETSI TR 101 750 (EP TIPHON): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; Studies into the Impact of lawful interception".
[136] ETSI EN 301 040 (EP TETRA): "Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface".

---

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

[137] ETSI EG 201 040 (EP TETRA): "Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface; Feasibility study report" (This document has been made *historical*).
[138] 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".
[139] 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

[140] ETSI TR 102 044: "Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates".
[141] ETSI TR 102 045: "Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model".
[142] ETSI TR 102 046: "Electronic Signatures and Infrastructures (ESI); Maintenance report".
[143] ETSI TR 102 047: "Electronic Signatures and Infrastructures (ESI); International Harmonization of Electronic Signature Formats".
[144] ETSI TR 102 040: "Electronic Signatures and Infrastructures (ESI); International Harmonization of Policy Requirements for CAs issuing Certificates".
[145] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".
[146] ETSI TS 102 158: "Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates".
[147] ETSI TR 102 153: "Electronic Signatures and Infrastructures (ESI); Pre-study on certificate profiles".
[148] ETSI SR 002 176: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures".
[149] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".
[150] ETSI TS 102 734: "Electronic Signatures and Infrastructures; Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES)".
[151] ETSI TS 102 280: "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".
[152] ETSI TR 102 272: "Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies".
[153] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".
[154] ETSI TR 102 437: "Electronic Signatures and Infrastructures (ESI); Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates)".
[155] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".
[156] ETSI TR 102 317: "Electronic Signatures and Infrastructures (ESI); Process and tool for maintenance of ETSI deliverables".
[157] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".
[158] ETSI TS 102 904: "Electronic Signatures and Infrastructures; Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)".
[159] ETSI TS 101 862: "Electronic Signatures and Infrastructures (ESI); Qualified Certificate profile".

[160] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".
[161] 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".
[162] ETSI TR 102 041 (SEC ESI): "Signature Policies Report".
[163] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities".
[164] ETSI TS 101 861: "Electronic Signatures and Infrastructures (ESI); Time stamping profile".
[165] ETSI TR 102 038 (SEC ESI): "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".
[166] ETSI TR 102 030 (SEC ESI): "Provision of harmonized Trust Service Provider status information".
[167] ETSI TR 102 438: "Electronic Signatures and Infrastructures (ESI); Application of Electronic Signature Standards in Europe".
[168] 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)".
[169] ETSI TR 102 605: "Electronic Signatures and Infrastructures (ESI); Registered E-Mail".
[170] ETSI TR 102 572: "Best Practices for handling electronic signatures and signed data for digital accounting".
[171] ETSI TS 102 573: "Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data for digital accounting".
[172] ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture".
[173] ETSI TS 102 640-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM".
[174] ETSI TS 102 640-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains".
[175] ETSI TS 102 640-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 4: REM-MD Assessment Profiles".
[176] ETSI TS 102 640-5: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles".
[177] 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".
[178] 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".
[179] 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".
[180] ETSI TS 102 778-1: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES".

[181] 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".
[182] 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".
[183] ETSI TS 102 778-4: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile".
[184] 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".
[185] ETSI TS 102 778-6: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 6: Visual Representations of Electronic Signatures".
[186] ETSI TR 102 923: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signatures (PAdES); Usage and implementation guidelines".
[187] ETSI SR 003 232: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles (PAdES); Printable Representations of Electronic Signatures".
[188] ETSI TR 101 564: "Electronic Signatures and Infrastructures (ESI); Guidance on ETSI TS 102 042 for Issuing Extended Validation Certificates for Auditors and CSPs".
[189] ETSI TR 103 071: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Test suite for future REM interoperability test events".
[190] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management".
[191] ETSI TR 101 533-2: "Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors".
[192] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

Security Algorithms

[193] ETSI TCTR 003 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); European Encryption Algorithm for the use in audiovisual systems".
[194] 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".
[195] 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".
[196] ETSI TCTR 004 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); Cryptographic Algorithm for the European Multi-Application IC-Card".
[197] ETSI TCTR 005 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); UPT Authentication Algorithm for the use in DTMF Devices".
[198] ETSI TCRTR 032: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TESA-7 algorithm".
[199] ETSI TCRTR 031: "Security Algorithms Group of Experts (SAGE); Universal Personal Telecommunication (UPT) authentication; Rules for the management of the USA-4".

[200] MI/SAGE-0008 - NOT AVAILABLE FOR DOWNLOAD: "Cryptographic algorithm for Public Network Operators".
[201] ETSI TCRTR 035: "Security Algorithms Group of Experts (SAGE); Rules for the management of the Baras algorithm".
[202] ETSI TR 101 053-1: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 1: TEA1".
[203] MI/SAGE-00010-2 - NOT AVAILABLE FOR DOWNLOAD: "Standard Trans European Trunked RAdio (TETRA) air interface encryption algorithm TEA1 and TEA2".
[204] ETSI TR 101 053-2: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 2: TEA2".
[205] 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".
[206] MI/SAGE-00011-2 - NOT AVAILABLE FOR DOWNLOAD: "Standard Trans European Trunked RAdio (TETRA) set of air interface authentication and key management algorithms TAA1".
[207] ETSI TR 101 054: "Security Algorithms Group of Experts (SAGE); Rules for the management of the HIPERLAN Standard Encryption Algorithm (HSEA)".
[208] MI/SAGE-00012-2 - NOT AVAILABLE FOR DOWNLOAD: "Standard air interface encryption algorithm for HIPERLAN".
[209] ETSI ETR 277 (Edition 1): "Security Algorithms Group of Experts (SAGE); Requirements specification for an encryption algorithm for use in audio visual systems".
[210] ETSI ETR 278 (Edition 1): "Security Algorithms Group of Experts (SAGE); Report on the specification and evaluation of the GSM cipher algorithm A5/2".
[211] ETSI TR 101 375: "Security Algorithms Group of Experts (SAGE); Report on the specification, evaluation and usage of the GSM GPRS Encryption Algorithm (GEA)".
[212] MI/SAGE-00015-2 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); GPRS encryption algorithm".
[213] 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)".
[214] MI/SAGE-00016-2 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); CTS Authentication and Key Generation Algorithm".
[215] MI/SAGE-00017-2 - NOT AVAILABLE FOR DOWNLOAD: "Security Algorithms Group of Experts (SAGE); TEA3 and TEA4 Security Algorithms".
[216] ETSI TR 101 053-3: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 3: TEA3".
[217] ETSI TR 101 053-4: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 4: TEA4".
[218] MI/SAGE-00018 - NOT AVAILABLE FOR DOWNLOAD: "Design of the 3GPP Encryption and Integrity algorithms".
[219] ETSI TR 101 740: "Security algorithms Group of Experts (SAGE); Rules of the management of the standard GSM GPRS Encryption Algorithm 2 (GEA2)".
[220] MI/SAGE-00019-2 - NOT AVAILABLE FOR DOWNLOAD: "Design of a Standard GSM GPRS Encryption algorithm 2 (GEA2)".
[221] MI/SAGE-00020-2 - NOT AVAILABLE FOR DOWNLOAD: "Design of authentication algorithm for UMTS".
[222] 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)".

[223] 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)".
[224] 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)".
[225] 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)".
[226] 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)".
[227] ETSI TS 135 221 (3GPP SA 3) - NOT AVAILABLE FOR DOWNLOAD: "Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications (3GPP TS 35.221)".
[228] ETSI TS 135 222 (3GPP SA 3) - NOT AVAILABLE FOR DOWNLOAD: "Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 2: ZUC specification (3GPP TS 35.222)".
[229] ETSI TS 135 223 (3GPP SA 3) - NOT AVAILABLE FOR DOWNLOAD: "Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data (3GPP TS 35.223)".
[230] ETSI TR 135 924 (3GPP SA 3) - NOT AVAILABLE FOR DOWNLOAD: "Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 4: Design and Evaluation Report (3GPP TS 35.921)".

Quantum Key Distribution

[231] ETSI GS QKD 002: "Quantum Key Distribution (QKD); Use Cases".
[232] ETSI GS QKD 003: "Quantum Key Distribution (QKD); Components and Internal Interfaces".
[233] ETSI GS QKD 004: "Quantum Key Distribution (QKD); Application Interface".
[234] ETSI GS QKD 005: "Quantum Key Distribution (QKD); Security Proofs".
[235] ETSI GS QKD 008: "Quantum Key Distribution (QKD); QKD Module Security Specification".

Identity and Access Management for Networks and Services

[236] ETSI GS INS 001: "Identity and access management for Networks and Services; IdM Interoperability between Operators or ISPs with Enterprise".
[237] ETSI GS INS 002: "Identity and access management for Networks and Services; Distributed Access Control for Telecommunications; Use Cases and Requirements".
[238] ETSI GS INS 003: "Identity and access management for Networks and Services; Distributed User Profile Management; Using Network Operator as Identity Broker".
[239] ETSI GS INS 004: "Identity and access management for Networks and Services; Dynamic federation negotiation and trust management in IdM systems".
[240] ETSI GS INS 005: "Identity and access management for Networks and Services; Requirements of an Enforcement Framework in a Distributed Environment".
[241] ETSI GS INS 006: "Identity and access management for Networks and Services; Study to Identify the need for a Global, Distributed Discovery Mechanism".

Smart Cards

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[268] ETSI TS 102 835: "Smart Cards; Test Specification for SCWS Application Invocation API for Java CardTM; Tests Environment and Annexes".
[269] ETSI TS 102 671: "Smart Cards; Machine to Machine UICC; Physical and logical characteristics".

Next Generation Networks

[270] 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".
[271] 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".
[272] 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".
[273] ETSI TR 102 419: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security analysis of IPv6 application in telecommunications standards".
[274] ETSI TR 102 420: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of activity on security".
[275] ETSI TR 102 055: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); ENUM scenarios for user and infrastructure ENUM".
[276] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".
[277] 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".
[278] 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".
[279] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".
[280] 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".
[281] 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".
[282] ETSI EG 202 549: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Design Guide; Application of security countermeasures to service capabilities".
[283] 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".
[284] ETSI TR 187 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study on Media Security in TISPAN NGN".
[285] ETSI TR 187 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NAT traversal feasibility study report".

[286] 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".
[287] 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".
[288] 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".
[289] ETSI TR 187 014: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); eSecurity; User Guide to eTVRA web-database".
[290] 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".
[291] ETSI TR 187 013: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study on IPTV Security Architecture".
[292] ETSI TR 187 015: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Prevention of Unsolicited Communication in the NGN".
[293] ETSI TS 187 016: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Identity Protection (Protection Profile)".
[294] 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".
[295] 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".
[296] ETSI TR 187 023 - NOT AVAILABLE FOR DOWNLOAD: "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

[297] ETSI TR 102 180: "Basis of requirements for communication of individuals with authorities/organizations in case of distress (Emergency call handling)".
[298] ETSI TR 102 299: "Emergency Communications; Collection of European Regulatory Texts and orientations".
[299] ETSI TS 102 181: "Emergency Communications (EMTEL); Requirements for communication between authorities/organizations during emergencies".
[300] ETSI TS 102 182: "Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies".
[301] ETSI TR 102 410: "Emergency Communications (EMTEL); Basis of requirements for communications between individuals and between individuals and authorities whilst emergencies are in progress".
[302] 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".

[303] ETSI TR 102 445: "Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness".
[304] ETSI TR 102 476: "Emergency Communications (EMTEL); Emergency calls and VoIP: possible short and long term solutions and standardization activities".
[305] ETSI TS 102 900:" Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service".
[306] ETSI TS 170 001: "Project MESA; Service Specification Group - Services and Applications; Statement of Requirements (SoR)".
[307] ETSI TR 170 002: "Project MESA; Service Specification Group - Services and Applications; Definitions, symbols and abbreviations".
[308] ETSI TR 170 003: "Project MESA; Service Specification Group - Services and Applications; Basic requirements".
[309] ETSI TR 170 012: "Project MESA; Technical Specification Group - System; System Overview".
[310] ETSI TR 102 653: "Project MESA; Technical Specification Group - System; System and Network Architecture".
[311] ETSI TS 170 016: "Project MESA; Technical Specification Group - System; Functional Requirements Definition".

Broadcasting

[312] ETSI TS 101 197-1 (Broadcast): "Digital Video Broadcasting (DVB); DVB SimulCrypt; Part 1: Head-end architecture and synchronization".
[313] ETSI EN 300 744 (Broadcast): "Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television".
[314] ETSI EN 301 192 (Broadcast): "Digital Video Broadcasting (DVB); DVB specification for data broadcasting".
[315] ETSI TS 102 201 (Broadcast): "Digital Video Broadcasting (DVB); Interfaces for DVB Integrated Receiver Decoder (DVB-IRD)".
[316] ETSI TS 103 197 (Broadcast): "Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt".
[317] 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".
[318] ETSI EN 301 790 (Broadcast): "Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems".
[319] ETSI ETR 289 (Broadcast): "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems".
[320] ETSI TS 102 812 (Broadcast): "Digital Video Broadcasting (DVB); Multimedia Home Platform (MHP) Specification 1.1.1".
[321] ETSI TS 102 825-1 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 1: CPCM Abbreviations, Definitions and Terms ".
[322] ETSI TS 102 825-2 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 2: CPCM Reference Model".
[323] ETSI TS 102 825-3 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 3: CPCM Usage State Information".
[324] ETSI TS 102 825-4 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 4: CPCM System Specification".
[325] ETSI TS 102 825-5 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 5: CPCM Security Toolbox".

[326] ETSI TR 102 825-6 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 6: CPCM Security Test Vectors".
[327] ETSI TS 102 825-7 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 7: CPCM Authorized Domain Management".
[328] ETSI TR 102 825-8 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 8: CPCM Authorized Domain Management scenarios".
[329] ETSI TS 102 825-9 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 9: CPCM System Adaptation Layers".
[330] 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".
[331] ETSI TR 102 825-11 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 11: CPCM Content Management Scenarios".
[332] ETSI TR 102 825-12 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 12: CPCM Implementation Guidelines".
[333] ETSI TR 102 825-13 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 13: CPCM Compliance Framework".
[334] ETSI TS 102 825-14 (Broadcast): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 14: CPCM Extensions".
[335] 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".

IPv6

[336] ETSI TS 102 558: "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT): IPv6 Security; Requirements Catalogue".
[337] 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)".
[338] ETSI TS 102 597: "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT): IPv6 Security; Interoperability Test Suite".
[339] 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

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

Terminals

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

Mobile Commerce

[342] ETSI TR 102 203: "Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements".

[343] ETSI TS 102 204: "Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface".

[344] ETSI TR 102 206: "Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework".

[345] ETSI TS 102 207: "Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services".

[346] ETSI TR 102 071: "Mobile Commerce (M-COMM); Requirements for Payment Methods for Mobile Commerce".

Generic Security Issues

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

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

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

[350] 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".

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

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

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

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

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

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

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

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

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

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

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

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

[363] 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"".

[364] 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 3rd Edition of this White Paper (December 2009)

[64] [99] [100] [109] [110] [111] [132] [177] [178] [179] [185] [186] [187]
[188] [189] [190] [191] [192] [227] [228] [229] [230] [231] [232] [233] [234]
[235] [236] [237] [238] [239] [240] [241] [260] [261] [262] [263] [264] [265]
[266] [267] [268] [269] [291] [292] [293] [294] [295] [296] [305] [331] [332]
[333] [334] [335] [340]

GLOSSARY

3DES	Triple Data Encryption Standard
3GPP™	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorisation and Accounting
AES	Advanced Encryption Standard
AH	Authentication Header
AKA	Authentication and Key Agreement
API	Application Programming Interface
ATS	Abstract Test Suite
BUSDOX	Business Document Exchange Network
CA	Certification Authority
CA	Conditional Access *(broadcast systems)*
CAB	Certification Authority/Browser
CAdES	CMS Advanced Electronic Signatures
CDN	Content Delivery Network
CMS	Cryptographic Message Syntax
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
CSA3	Common Scrambling Algorithm version 3
CSG	Closed Subscriber Group
CSP	Communication Service Provider (*in Lawful Interception*)
DECT™	Digital Enhanced Cordless Telecommunications
DES	Data Encryption Standard
DMO	Direct Mode Operation
DRM	Digital Rights Management
DSAA	DECT Standard Authentication Algorithm
DSC	DECT Standard Cipher
DVB	Digital Video Broadcasting
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
GIBA GPRS IMS Bundled Authentication
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
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
ISO International Organisation for Standardisation
IT Information Technology
ITS Intelligent Transport System
JTC Joint Technical Committee
KDF Key Derivation Function
LI Lawful Interception
LTE™ Long Term Evolution
MBMS Multicast Broadcast Multimedia Service
MD Message Digest
MDF Mobile Device Functionality
MNO Mobile Network Operator
MME Mobility Management Entity
M2M Machine to Machine
NAS Non-Access Stratum
NASS Network Access SubSystem
NAT Network Address Translation
NENA National Emergency Number Association
NFC Near Field Communication
NGN Next Generation Networks
NIST National Institute of Standards and Technology (USA)
NNI Network to Network Interface
PAdES PDF Advanced Electronic Signatures
PAMR Public Access Mobile Radio
PIN Personal Identification Number
PKI Public Key Infrastructure
PLMN Public Land Mobile Network
PMR Private Mobile Radio
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
SAE	System Architecture Evolution
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
ST	Security Target
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	Transport Layer Security
TR	ETSI Technical Report
TS	ETSI Technical Specification
TSL	Trust-service Status List
TSS&TP	Test Suite Structure and Test Purposes
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
WG	Working Group of an ETSI TC
WLAN	Wireless Local Area Network
XAdES	XML Advanced Electronic Signature
XML	eXtended Mark up Language
ZUC	Zu Chongzhi