ETSI White Paper No. 1

Security for ICT - the Work of ETSI

Authors:

Charles Brookson (DTI UK) and

Dionisio Zumerle (ETSI)

January 2006

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.

About the authors

Charles Brookson CEng FIEE FRSA

Standards, Assistant Director, UK Department of Trade and Industry

Charles Brookson works in the UK Department of Trade and Industry and is a Professional Electronic Engineer. He previously was Head of Security for one2one (now T-Mobile UK), 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 Security Standards Organisations and other bodies outside Europe. He is 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 within ETSI, has been Chairman on the GSM Association Security Group (representing operators in over 200 countries) for many years, and has been involved in GSM and 3GPP security standards.

Dionisio Zumerle

Technical Officer, ETSI Secretariat

Dionisio Zumerle works in the Fixed Competence Centre of ETSI, where he is Technical Officer for the Technical Committees that deliver standards concerning IT and Telecommunications Security and Quality of Service aspects.

He received his MSc in Telecommunications Engineering from *La Sapienza* University of Rome. In the past he has worked in the ICT Central Directorate of *Poste Italiane*, as Programme Management Officer for Service Oriented Architecture design and implementation.

Security for ICT – the Work of ETSI

January 2006

This 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 standardisation of security in that area. Some of the Institute's major achievements are then highlighted and ongoing activities are described. At the end of the paper, all ETSI's specifications and standards for security standardisation are listed. Reference to individual deliverables in the text is indicated by its listing number in [ ].

CONTENTS

Page

2 Foreword
3 Introduction – The Organisation of Work in ETSI
4 Mobile and Wireless Communications

- **GSM™**
- **UMTS™**
- **TETRA**
- **DECT™**

10 Lawful Interception
13 Electronic Signatures
16 Next Generation Networks
17 Algorithms
18 Emergency Telecommunications

- **EMTEL**
- **MESA**

20 Smart Cards
21 Radio Frequency Identification (RFID)
22 Mobile Commerce
22 Broadcasting
24 Satellite
24 IPCablecom
24 Other Security Issues
25 Conclusions
26 Publications
40 Glossary

FOREWORD

Security is vital for ICT systems and infrastructures. Information has to be secured to ensure that it cannot be read or modified by unauthorised parties, and that its origin and destination can be proved. In addition, the networks themselves have to be securely managed and protected against compromise or attack; criminals have to be prevented from misusing them and the potential for fraud has to be blocked. The increasing complexity and rapid development of new systems present a real challenge to us when securing ICT systems.

ETSI has been a leader in setting security standards since its foundation in1988. The Institute achieved outstanding success with the standardisation of GSM™, the Global System for Mobile communication, which included authentication, anonymity and customer privacy – the first full world-wide commercial deployment of encryption and smart cards. Many other standards have built on ETSI's expertise in encryption used for authentication, privacy and integrity of information.

Other major achievements have included Digital Enhanced Cordless Telecommunications (DECT™), Terrestrial Trunked Radio (TETRA), video standards, Multimedia Internet Protocol (IP) and subsequent mobile and fixed services.

Today ETSI's standardisation activities cover a broad spectrum of security issues, from lawful interception (LI) to algorithms, from electronic signatures to smart cards, and they relate to every aspect of ICT. In addition, ETSI is working towards the establishment of effective telecommunications systems to protect citizens in an emergency (EMTEL) and on security issues in Next Generation Networks.

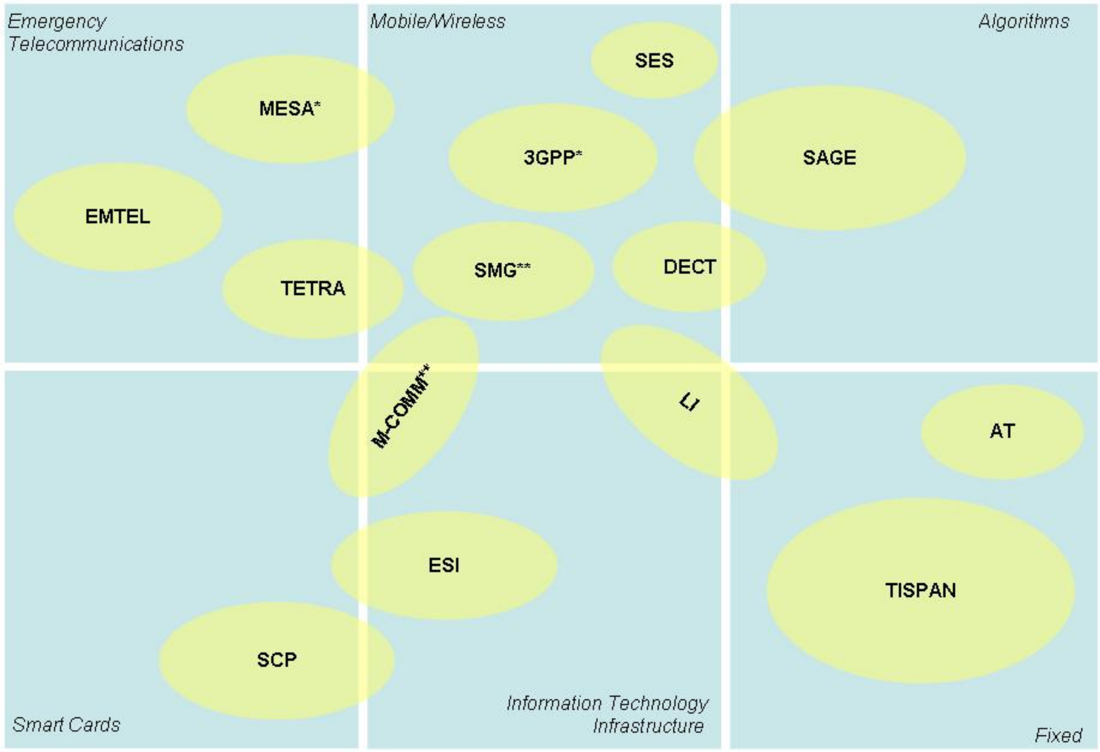
This paper provides a historical overview of ETSI's work since its establishment, catalogues current activities and highlights what are likely to be key issues in the future.

Charles Brookson
Chairman ETSI OCG Security

INTRODUCTION – THE ORGANISATION OF WORK IN ETSI

ETSI’s work is organised into Technical Committees (TCs) and ETSI Partnership Projects. 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. ETSI Members may attend meetings and influence ETSI’s work in any technical area.

The figure below illustrates the areas in which these committees operate.



* ETSI is a founding partner for this partnership project
** Closed Committee

KEY

3GPP	Third Generation Partnership Project
AT	TC Access and Terminals
DECT	TC Digital Enhanced Cordless Telecommunications
EMTEL	Special Committee Emergency Telecommunications
ESI	TC Electronic Signatures and Infrastructures
LI	TC Lawful Interception
MESA	ETSI Partnership Project Mobility for Emergency and Safety Applications
M-COMM	ETSI Project Mobile Commerce
SAGE	Special Committee Security Algorithms Group of Experts
SES	TC Satellite Earth Stations and Systems
SCP	TC Smart Card Platform
SMG	TC Special Mobile Group
TETRA	TC Terrestrial Trunked Radio
TISPAN	TC Telecommunications and Internet converged Services and Protocols for Advanced Networking

The following pages outline ETSI’s work in each of these fields. A complete list of the relevant publications for each field is included at the end of this document.

MOBILE AND WIRELESS TELECOMMUNICATIONS

Mobile and wireless technologies are enormously flexible. Applications include public safety and military communications, as well as widespread commercial use (eg cellular telephones, wireless networks and cordless home telephones).

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

ETSI works on the following mobile and wireless technologies:

- **GSM**

  Shortly after its creation in 1988, ETSI took over the task of specifying GSM from the European Conference of Posts and Telecommunications Administrations (CEPT). Subsequently, 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 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, to allow encryption and authentication, to control payment for copyright material downloading and to respond to many other security threats. The general description of the security functions can be found in [60].

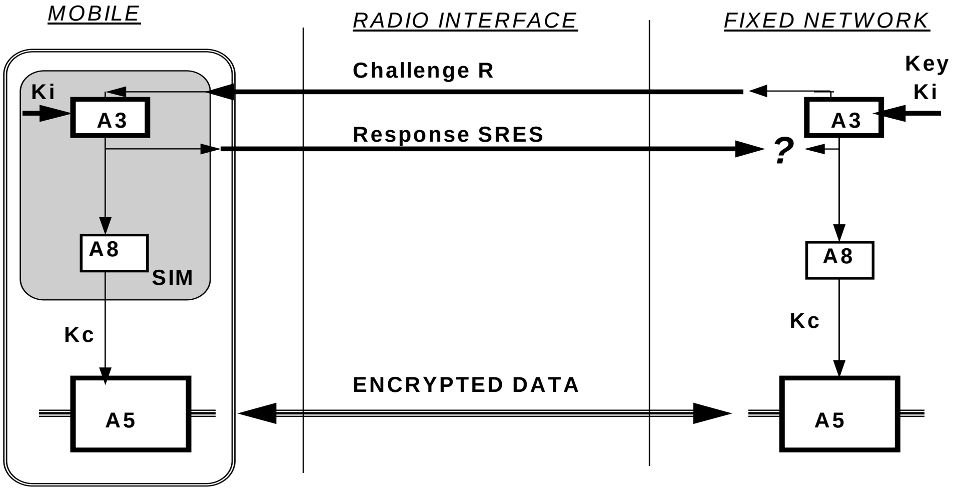
  The major characteristics of security in GSM are described below:

  Anonymity – Anonymity consists in preventing the tracking of the location of the user or identifying 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 radio set, the real identity is used and a temporary identifier is then issued. From then on, the temporary identifier is used, until the network requests the real identity again. Only by tracking the user is it possible to determine the temporary identity being used (see [68], [77], [78] and [26]).

Authentication and Signalling Protection – Authentication is used to identify the user (or holder of a Smart 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 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. 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 (also see [63] to [66]):



IMEI – Mobile terminals are, by their nature attractive (often described by the acronym CRAVED (Concealable, Removable, Available, Valuable, Enjoyable and Disposable)) objects, at great risk of theft. ETSI has created a set of standards (see [67] and [68]) 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. IMEI is also useful to identify the 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], [9], [14], [16] and [55]). 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 [11]).

Priority – GSM specifications include a public safety service called Priority (see [70], [71]). 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.

- **UMTS**
  3GPP, of which ETSI is a founding partner, brings ETSI together with five other regional standardisation organisations in Asia and the USA, plus market associations 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 including the following:

Authentication – To further enhance the security 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 [29], [30], [31], [34], [35], [39], [42]).

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 [72] to [76]). 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 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 so-called MBMS (Multicast Broadcast Multimedia Service, see [34]). This enables MNOs to transmit multimedia contents to a selected area of the mobile network, offering great potential for example in the area of public warnings.

Ongoing activities

3GPP activities related to security are now focused on the IP Multimedia Subsystem (IMS), which is an IP core network dedicated to the control and integration of multimedia services. Extensions to IMS security specifications to encompass the requirements of Next Generation Networks, enabling Fixed-Mobile Convergence, are currently being applied.

- **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.

y
ears, within disaster stricken areas, emergency response teams from several European nations have had difficulty communicating with each other, due in part to the lack of standardisation in their mobile radio equipment. The TETRA standards evolved to answer this and other communication challenges, including those anticipated by the European Commission in its efforts to unify communications across the different member states. The mission-critical effectiveness and operational efficiency of TETRA as a wireless communications technology was demonstrated during the Madrid railway bombings and the Olympic Games in Athens in 2004.

Based on digital, trunked radio technology, TETRA is believed to be the next-generation architecture and standard for current, analogue PMR and PAMR markets. TETRA actually uses features taken from several different technological areas: mobile radio, digital cellular telephone, paging and wireless data.

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 [82], [83], [84]):

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 preventing 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. (The mutual authentication security mechanism is available for Voice and Data and Packet Data Optimised mode. In Direct Mode Operation (DMO) an explicit authentication mechanism is not available; in this case the use of 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. Also, 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 , and these are described on the ETSI web portal (portal.etsi.org/dvbandca).

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, each time an identity is transmitted, it is encrypted in a different way, making it difficult to eavesdrop and identify active terminals.

Ongoing activities
The security requirements for the second release of TETRA are being produced.

In addition, TC TETRA is currently working to deliver the lawful interception specifications for this technology (see page 10 Lawful Interception).

- **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.

tandardisation started in CEPT, and was transferred into ETSI when the Institute was set up in 1988. Work today is the responsibility of Technical Committee DECT.

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
- user-related signalling information.

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

- authentication of terminals
- data confidentiality
- user authentication.

Among other achievements for DECT, ETSI has developed the DECT Standard Authentication Algorithm (DSAA) and the DECT Standard Cipher (DSC).

The combination of 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].

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 to investigate 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 the standardisation of lawful interception since 1991; today work is concentrated in Technical Committee Lawful Interception (TC LI), which enjoys 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 for law enforcement agencies.

Achievements

A major achievement of ETSI’s work in this area has been publication of the specifications for the handover procedure: TS 101 671 and ES 201 671 ([101] and [96]). These specifications illustrate the flow that the intercepted data should follow in telecommunication networks or services. In this context, they specify the network or service protocols necessary to provide lawful interception, as well as the physical or logical point at which the interception has to take place (the handover interface) both for packet data and switched-circuit communications. ETSI has also produced other important specifications on lawful interception in other Technical Committees. For this reason, TC LI is working in close collaboration with TC TISPAN, the Committee in charge of creating the specifications for NGN in ETSI (see page 16 NGN) as well as with other relevant committees (TC TETRA, 3GPP and TC Access and Terminals (TC AT), [108] to [123]).

The LI handover specifications are already widely used. They were first adopted in 2003 by the Netherlands regulation authority (Directorate General for Telecommunication and Post of the Ministry of Economic Affairs). Meanwhile a number of other countries are in the process of implementation or have expressed an interest in adopting the specifications.

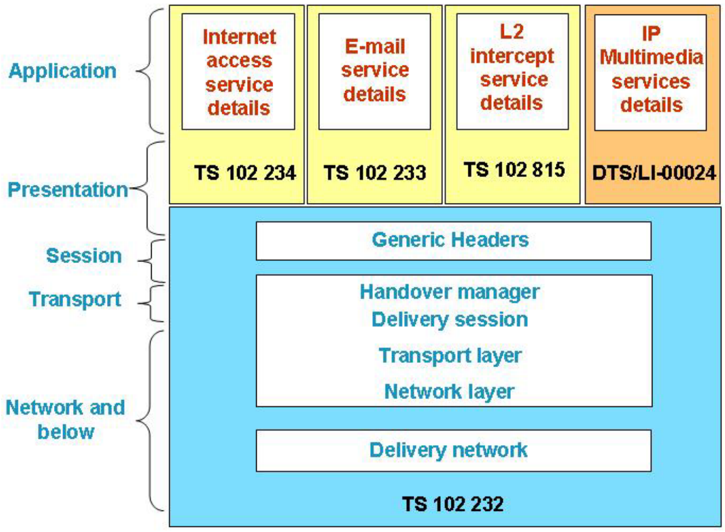
The specifications are subject to constant review and updating within ETSI to accommodate emerging needs, and are being used as the basis for specifying the procedures for lawful interception. The increasing trend in the use of packet-switched technologies has necessitated a standard for the delivery of IP-based interception: TS 102 232 ([98]) specifies the approach, the protocols and headers needed to perform lawful interception on an IP-based platform.

In addition, lawful interception has to be possible on specific services that make use of the IP framework: TS 102 233 ([99]) covers the service-specific details for e-mail services, describing the handover to the law enforcement authorities, whilst TS 102 234 ([100]) covers the service-specific details for Internet access.

ETSI has also standardised the general requirements of network operators, service providers and access providers ([97]) who are obliged to make available results of interception to the law enforcement agencies. Complementing this, a Technical Specification (TS) ([102]) 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.

Recent publications include a specification on service-specific details for layer 2 lawful interception ([106]). This specification applies to access providers having access to information on layer 2 session information. This TS is particularly important because, in many situations, information on higher layers is either not accessible or not stored.

The following figure summarises the deliverables produced and their placement in the overall architecture for lawful interception in relation to the ISO-OSI protocol stack.



(Adapted from a diagram produced by Peter van der Arend of KPN, Chairman of ETSI TC LI)

Ongoing activities

- A specification on the lawful interception of public Internet access by means of wireless LAN technology is being produced. This is a critical issue for lawful interception because the user cannot always be identified.

- IMS, the system created in 3GPP to enable the provision of multimedia services, and TISPAN specifications are being developed in tandem to allow the convergence of fixed and mobile networks over this common IP-based platform. The handover interface for lawful interception is being developed in TC LI to align with the latest TISPAN and 3GPP specifications for NGN.

- TC LI is also addressing Data Retention. European governments are becoming increasingly interested in preserving communications. The European Parliament's civil liberties committee recently voted in favour of new rules, whereby details on telephone calls and Internet use would be kept for six to 12 months. TC LI is producing a report (DTR/LI-00020) which will provide a simple architecture framework, interface and extensible syntax for the request and delivery of available or retained stored data between government authorities and providers of communication services or their agents, based on common global capability needs.

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 subject data and to protect against forgery of the data by the recipient. A digital signature is created by encrypting the component to be signed, or a unique derivation of this component, with the originator's private key. The digital signature is transmitted to the recipient of the message along with the message itself. The recipient then re-builds the derivation from the message and decrypts the digital signature with the originator's public key. If both derivations – the one obtained by the recipient and the one the recipient has decrypted – are identical, this provides proof of the message integrity. Where suitable organisational and security measures have been enforced to create a reliable connection between the signer and the public key, the message origin can also be reasonably trusted. Additional security and organisational measures are also employed to ensure the signature can be trusted in the long term.

Standards to support the use of electronic signatures and public key certificates are a key driver in enabling the evolution and take-up of electronic commerce. ETSI standards for electronic signatures are currently being developed in Technical Committee Electronic Signatures and Infrastructures (TC ESI) which is responsible within ETSI for standardisation in the area of electronic signatures and Public Key Infrastructure to support electronic commerce in open environments. As such, the committee has a special interest in interoperability as well as in aspects of trust relationships.

ETSI's involvement in this area began in September 1996, with the provision of specifications related to electronic signatures. The work, together with the contribution of CEN's Electronic Signature Workshop (CEN E-Sign WS), became part of the European Electronic Signature Standardisation Initiative (EESSI) in December 1998. Activities in this area intensified with the release of the 1999/93/EC Directive, addressing the issue of establishing a harmonised infrastructure for electronic signatures and the deployment of new vendor-specific infrastructures. Standards were required urgently to provide the basis for an open electronic commerce environment and to influence early developments. In response, EESSI established a legal and common European framework for the recognition of electronic signatures.

Work on electronic signatures and infrastructures continues, including some of the basic requirements to enable secure electronic commerce and electronic document exchange, for example, for purchase requisitions, contracts and invoicing.

Achievements

ETSI's publication of deliverables in support of Directive 1999/93/EC on a Community framework for electronic signatures began in 2000 with a standard on Electronic Signature Formats (TS 101 733, [133]). An analogous, twin specification was drafted defining XML Advanced Electronic Signature Formats (XAdES, [139]), which made a significant impact on the user community.

In subsequent years the following topics were 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 Certification Service Providers issuing qualified ([136]) and non-qualified ([137]) certificates (these documents are now in widespread use both within and beyond the bounds of the European Community)
- Organisational and security requirements for Certifications Service Providers issuing attribute certificates ([130]) and for Time Stamping Authorities issuing Time Stamp Tokens ([144])
- Profiles for Qualified Certificates meeting the requirements laid down in the relevant Directive ([140]), to streamline Qualified Certificate based transactions, and for Time Stamp Tokens ([145]).

A number of Technical Reports (TRs) were also drafted to explain 'Signature Policy' to users ([125], [137], [143] and [146]).

The Profile for Qualified Certificates was afterwards supported by another Technical Specification ([134]) focused on profiling certificates issued to natural persons. This specification helps identify the requirements related to qualified certificates for natural persons, issued in compliance with ISO/IEC 9594-8:2001 and with the IETF RFC 3280 specification.

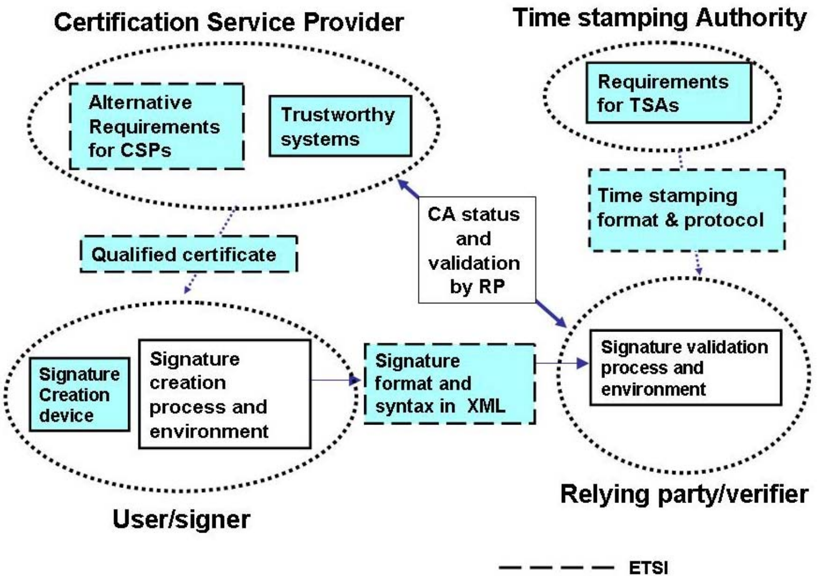
It also became clear that interoperation among the European Union member states would be necessary to allow a user based in one state, relying on its rules, to ascertain whether certificates issued in another state were issued in compliance with that state's rules. This requirement was addressed first by a Technical Report ([147]) that paved the way to a Technical Specification ([129]), which defined 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. The specifications [129] are applicable to scheme operators responsible for the approval of trust services and to those who wish to rely on such information.

Since 2002, TC ESI has been working to achieve harmonisation of the ETSI specifications at the global level, aligning with the work of the Internet Engineering Task Force (IETF), the Asia-Pacific Economic Community (APEC), the International Organisation for Standardisation (ISO), CEN etc. Reports have been, and are being, drafted on these various activities: see

[127], [128], [148].

Some of the most recent specifications on Electronic Signatures were the set of algorithm papers for Advanced Electronic Signatures [141], [142] that have been preceded, as a preparatory document, by a Special Report on Algorithms and Parameters for Secure Electronic Signatures [132]. These documents contain a set of security mechanisms and their parameters that can be used for advanced electronic signatures. The main issue is providing users with a sound and common basis for interoperability and security for signature applications as outlined in the Directive 1999/93/EC. TC ESI will also define maintenance mechanisms that allow for updating the algorithm list if required, for example if one of them becomes weaker or broken.

The following diagram summarises the entire work produced to date on electronic signatures and infrastructures.


Certification Service Provider
Alternative Requirements for CSPs
Trustworthy systems
Time stamping Authority
Requirements for TSAs
Time stamping format & protocol
CA status and validation by RP
Qualified certificate
Signature Creation device
Signature creation process and environment
Signature format and syntax in XML
Signature validation process and environment
User/signer
Relying party/verifier
ETSI

CA – Certification Authority
CSP – Certificate Service Provider
RP – Relying Party
TSA – Time Stamping Authority
XML – eXtended Markup Language

(Adapted from an ICT Standards Board diagram)

Ongoing activities

The work on electronic signatures in ETSI is currently focusing on the specification of profiles for specific e-Business needs, while TC ESI is also in the process of identifying the upcoming areas of interest (eg e-Invoicing and registered e-mail).

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. The Institute's work on NGN is being managed by its Technical Committee TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking). Security is one of its core concerns.

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

Achievements

Security is not an additional feature that can be patched on after the adoption of a new technology; when designing new architectures, security must be built in from the beginning. 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 data networks, TC TISPAN set the security requirements for the subsystems of Next Generation Networks ([155]).

In addition, TC TISPAN is producing a Security Design Guide ([149], [150], [151] and [153]) 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). Common Criteria are a set of drivers to be used as the basis for the evaluation of security properties of IT products and systems, which establishes the framework for an IT security evaluation that is meaningful to a wider audience. The Common Criteria primarily address the protection of information from unauthorised disclosure, modification or loss of use.

These publications address the issue of application of the Common Criteria framework in the ETSI standardisation process and the development of protocols and architecture standards (see [151]), describing 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 phase, to the actual definition of the subsystems, the modules and protocols that comprise the standard.

The same set of TISPAN deliverables contains the 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 ([149]) 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. TR 102 419 (see [152]) 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).

Ongoing activities

Ongoing work in TISPAN addresses the challenge of security in Next Generation Networks with an analysis of risks and threats ([157]) and by defining an extensible NGN security architecture ([158]). For lawful interception, TC TISPAN is identifying appropriate interfaces, reference points and entities in the NGN architecture.

TC TISPAN is also producing a specification to support emergency communication from citizen to authority within the NGN architecture.

ALGORITHMS

ETSI's Security Algorithms Group of Experts (SAGE) provides the Institute's 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 ([189]), DECT, GSM and TETRA ([170] to [174], [184] and [185]), audiovisual services ([161], [162]), GPRS and Universal Personal Telecommunications (UPT, [167]). SAGE also collaborates with other ETSI committees to produce encryption algorithms.

Recent achievements include the design of encryption algorithms for GSM, EDGE and GPRS (A5/3 for GSM and EDGE and GEA3 for GPRS) which provide users of GSM mobile phones with a higher level of protection against eavesdropping than previously available. The algorithms are being developed in collaboration with the 3GPP organisational partners ([62] to [66], [179], [180] and [187]).

SAGE was also responsible for the 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* ([50] to [54]), which was developed for UMTS.

The security algorithms for the UMTS radio interface (UTRA) – UEA1 and UIA1 –were also 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 are available (only for the development and operation of 3G Mobile Communications and services) and can be found in 3GPP TS 35.201 ([45] to [49]). For an overview of the overall algorithm mechanisms in UMTS, see [41].

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, among things, restricts their utilisation to the telecommunication equipment or service for which they have been designed. ETSI is acting as a Custodian for the algorithms developed, and is responsible for the distribution and licensing of the confidential information and documents.

Ongoing activities

New work has been initiated on the development of a second set of security algorithms for UTRA. Alternatives to the Kasumi-based algorithms are required in case of a possible future breach of security. SAGE has developed two completely different algorithms, UEA2 and UIA2, which are currently undergoing public evaluation. They are expected to become available early in 2006.

EMERGENCY TELECOMMUNICATIONS

Emergency Telecommunications and Public Safety are areas requiring considerable standardisation activity. The existing infrastructures and services are 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**

ETSI’s Special Committee on Emergency Telecommunications (EMTEL) is the focal point in ETSI for the co-ordination and collection of requirements for emergency service communication. 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).

Achievements
Two ETSI Special Reports have been published by EMTEL: the first on emergency call handling ([190]) and the second on the European regulations covering communication during emergency situations ([191]). EMTEL has been heavily involved with work on communication between authorities and organisations, which resulted in the publication of a Technical Specification (TS) during 2005 ([192]).

Ongoing activities
Further work on communication between citizens is ongoing. Public protection and emergency preparedness is a key topic for EMTEL, and the committee plans to examine communications networks and the requirements for telecommunication and data transmission to enable the efficient functioning of the emergency services in response to disasters.

EMTEL is working with ETSI TC TISPAN, TC ERM, Project MESA, 3GPP and others on the definition of protocols for the location identification of emergency calls. In particular, EMTEL is collaborating closely with TC TETRA on emergency communication between authorities (see page 8 TETRA).

EMTEL also plans to examine communication networks and the requirements for telecommunication and data transmission to enable the efficient functioning of the emergency services in response to disasters. A series of deliverables is planned to be published in 2006 ([193], [194], [195], [196]).

- **MESA**

Project MESA (Mobility for Emergency and Safety Applications) is a transatlantic partnership project, established in 2000 by ETSI and the North American Telecommunications Industry Association (TIA), although membership has expanded, and the Project now also has members in Canada, India, Korea, Australia and Japan. Its aim is to define a digital mobile broadband system which will revolutionise the efficiency of first responders and rescue squads during an emergency or a disaster. At these times, the data rates needed for advanced services, together with the demand for mobility, reach far beyond the scope of current established wireless standards.

MESA-capable communications systems will directly improve the effectiveness of law enforcement, disaster response, fire fighting, emergency medical services and peacekeeping. 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 has adopted a ‘System of Systems’ approach, which involves linking together a variety of existing and foreseen technologies and systems. The key factor is interoperability.

Ongoing activities
Project MESA has recently defined the system technical requirements ([197] to [199]) and, during 2006, expects to begin drawing up the final technical system specifications to produce a roadmap for future standardisation activities.

SMART CARDS

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

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

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

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

The main task of ETSI Technical Committee Card Platform (TC SCP) is to maintain and expand the smart card platform specifications for 2G and 3G mobile communication systems on which other committees and organisations can base their system-specific applications. Current work aims to allow users 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. The specifications of TC SCP are generic; they provide a true multi-application platform not just for mobile communication systems but for all applications using a smart card.

Achievements

ETSI standardised the Subscriber Identity Module (SIM) card for GSM, which is one of the most widely deployed smart cards ever. The work produced in the GSM specifications has also been imported into the 3GPP specifications to create the USIM (Universal SIM) card used in UMTS. Currently, work is also being done to introduce smart cards in TETRA.

An important milestone recently in the evolution of the smart card platform was the completion in 2004 of Release 6 of all specifications. Release 7 is currently being produced.

Also, a new Technical Specification on Extensible Authentication Protocol (EAP) support in the Universal Integrated Circuit Card (UICC) was recently approved. This specifies the use of a smart card as a secure access device to a WLAN ([212]).

TS 102 221 ([203]) 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, ie an environment in which the card can have more than one first level application and may support separate user verification requirements for each application.

RFID

Radio Frequency Identification (RFID) is a method of storing and remotely retrieving data. An RFID tag is an electronic device that holds data. An RFID transceiver is a device that can read this data by querying over radio an RFID tag. Typically the tags are attached to an item and contain a serial number or other data associated with that item.

RFID can be used as a technology to achieve authentication and access. As the technology can be used in company access badges and passports, for toll payments and other systems, it is potentially vulnerable to fraudulent or terrorist attack.

Security in RFID technology must prevent illicit tracking and cloning of tags. In addition, RFID tags present a rather low limit of computational resources within the tag, which makes the use of standard cryptographic techniques unfeasible. Lighter encryption algorithms must be created for the RFID tags.

Ongoing activities
ETSI Technical Committee Electromagnetic Compatibility and Radio Spectrum Matters (TC ERM) has recently established a Task Group (ERM TG34) to produce deliverables for future RFID technologies and products. Two specifications have already been published ([213] and [214]) along with a report (TR 102 436, the guidelines for the installation and commissioning of RFID equipment at UHF).

ERM TG34 has also responded to EC mandate M/355 (work programme to support product proofing against crime).

MOBILE COMMERCE

ETSI undertook work on electronic payment for Mobile Commerce in its M-COMM committee (which was closed in June 2003, having successfully completed its work).

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 ([215] to [219]). 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.

BROADCASTING

Broadcasting technologies distribute audio and video signals to a large group of recipients, delivering radio, television and data services. The deliveries of some services (such as pay-per-view or subscription-based channels) require 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 in the field of broadcasting and related fields. It is becoming increasingly 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.

Among the activities in which JTC Broadcast is involved are two that involve specific security features: TV-Anytime Forum and the Digital Video Broadcasting (DVB) Project. The DVB Project is an industry-led consortium of over 260 broadcasters, manufacturers, network operators, software developers, regulatory bodies and others in over 35 countries, all committed to designing global standards for the delivery of digital television and data services. ETSI standards for DVB systems are developed in the JTC Broadcast, based on proposals from the DVB Project.

Achievements

- A major achievement of the DVB Project is the release of the DVB Common Scrambling Algorithm (currently version 2.0 is available). Approved by the Steering Board of the DVB Project, the Common Scrambling Algorithm is comprised of the Common Descrambling System and Scrambling Technology. The specification for each is distributed separately under arrangements with ETSI, which acts as Custodian for the four companies which developed the Common Scrambling Algorithm.

- 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 are being developed in JTC Broadcast, based on proposals from the TV-Anytime Forum, which has now closed after publishing the TV-Anytime Specifications.

  The TV-Anytime specifications were developed in two phases. Phase one has been published as TS 102 822 (parts 1 to 9). Part 7 of this standard ([225]) specifies how the TLS (Transport Layer Security) protocol is used in TV-Anytime to protect the delivery of data: the primary goal of the TLS 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. TLS 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. Following the publication of the Phase 1 specifications in 2003, the Phase 2 specifications have now also been published by ETSI.

Ongoing activities

Current work involves security issues regarding satellite distribution systems, with the intention of protecting the user identity in terms of location, signalling and data traffic to prevent unauthorised use of the network.

This activity has resulted in the production of scrambling algorithms and IP or higher layer security mechanisms ([226]).

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 or user interfaces, and for protocols implemented in earth stations and satellite systems.

TC SES has produced specifications on network security for broadband satellite multimedia services ([229]). It is important that satellite networks are able to offer IP network services that remain comparable to and competitive with terrestrial services. These objectives can only be achieved if the development of satellite standards can keep pace with the rapid evolution of the terrestrial IP network standards.

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 ([232] to [234]).

Ongoing activities
TC SES is working on new specifications on network security ([230] and [231]) In the area of Broadband satellite multimedia services.

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).

Security is a key issue for IPCablecom, since it is a shared network providing valuable contents. Besides the standards on lawful interception ([122], [123]), TC AT has produced a security specification for the technology ([236]), covering security for the entire IPCablecom architecture, identifying security risks and specifying mechanisms to secure the architecture.

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 ([237], [244] and [246])

- a guide for the selection and application of basic security mechanisms ([248] and [251])
- a guide for ETSI Technical Committees on the inclusion of security features in their technical specifications or reports ([241], [242])
- a guide to specifying requirements for cryptographic algorithms ([238], [239], [249] and [250])

and many others.

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 ([245] and [253]).

CONCLUSIONS

This paper illustrates how, since its inception, ETSI has led the field in 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. As a result, the Institute has developed exceptional expertise along with a 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.

The threat to the security of our ICT systems grows daily. Terminal devices are under attack from viruses and Trojan horses, and ways must be found to protect customers. There has been a noticeable increase in legislation world-wide, driven by growing security concerns over the last few years. This has intensified activities for example in interception, communications during emergencies and the prevention of crime.

In areas such as e-Learning, e-Health, e-Government and e-Business, the challenge will be to ensure technology is not just implemented but is also widely used. This will require a reliable and secure network infrastructure. But it 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 safety of the individual citizen is far too frequently at risk from terrorism and natural disaster. 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

Except where otherwise indicated, all of the following publications are ETSI documents, available for download free from the ETSI website (pda.etsi.org/pda.)

Mobile Telecommunications
GSM and UMTS

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

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

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

[4] TS 100 920 SMG 01 Digital cellular telecommunications system (Phase 2+); Security aspects (GSM 02.09)

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

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

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

[8] TS 100 929 SMG 03 Global System for Mobile communication (GSM) (Phase 2+); Security related network functions (GSM 03.20)

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

[10] TS 101 509 3GPP SA 3 Digital cellular telecommunications system (Phase 2+); Lawful interception; Stage 2 (3GPP TS 03.33)

[11] TS 101 967 3GPP SA 3 Digital cellular telecommunications system (Phase 2+); Immediate Service Termination (IST) (3GPP TS 03.35)

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

[13] TS 121 133 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); 3G security; Security threats and requirements (3GPP TS 21.133)

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

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

[16] TS 122 032 3GPP SA 3 Digital cellular telecommunications system

(Phase 2+); Universal Mobile Telecommunications System (UMTS); Immediate Service Termination (IST); Service description; Stage 1 (3GPP TS 22.032)

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

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

[19] TS 133 102 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture (3GPP TS 33.102)

[20] TS 133 103 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); 3G Security; Integration Guidelines (3GPP TS 33.103)

[21] TS 133 105 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); Cryptographic algorithm requirements (3GPP TS 33.105)

[22] TS 133 106 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); Lawful interception requirements (3GPP TS 33.106)

[23] TS 133 107 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); 3G security; Lawful interception architecture and functions (3GPP TS 33.107)

[24] TS 133 108 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)

[25] TS 133 120 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); 3G Security; Security Principles and Objectives (3GPP TS 33.120)

[26] TS 133 141 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); Presence service; Security (3GPP TS 33.141)

[27] TS 133 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)

[28] TS 133 203 3GPP SA 3 Details and Download Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203)

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

[30] TS 133 220 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture (3GPP TS 33.220)

[31] TS 133 221 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Support for subscriber certificates (3GPP TS 33.221)

[32] TS 133 222 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (3GPP TS 33.222)

[33] TS 133 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234)

[34] TS 133 246 3GPP SA 3 Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS) (3GPP TS 33.246)

[35] TS 133 310 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); Network domain security; Authentication framework (NDS/AF) (3GPP TS 33.310)

[36] 3GPP TR 33.810 3G Security; Network Domain Security / Authentication Framework (NDS/AF); Feasibility Study to support NDS/IP evolution

[37] 3GPP TR 33.817 Feasibility study on (Universal) Subscriber Interface Module (U)SIM security reuse by peripheral devices on local interfaces

[38] 3GPP TR 33.900 Guide to 3G security

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

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

[41] 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)

[42] TR 133 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)

[43] TR 133 919 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); System description (3GPP TR 33.919)

[44] 3GPP TR 33.941 Presence service; Security

[45] TR 133 978 Universal Mobile Telecommunications System (UMTS); Security aspects of early IMS (3GPP TR 33.978)

[46] TS 135 201 3GPP SA 3 Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications (3GPP TS 35.201 version 6.0.0 Release 6)

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

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

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

35.204)
[50] TS 135 205 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 1: General (3GPP TS 35.205)
[51] TS 135 206 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 2: Algorithm specification (3GPP TS 35.206)
[52] 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)
[53] TS 135 208 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 4: Design conformance test data (3GPP TS 35.208)
[54] TR 135 909 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 5: Summary and results of design and evaluation (3GPP TR 35.909)
[55] 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)
[56] TR 141 033 3GPP SA 3 Digital cellular telecommunications system (Phase 2+); Lawful Interception requirements for GSM (3GPP TR 41.033)
[57] TR 141 033 3GPP SA 3 Digital cellular telecommunications system (Phase 2+); Lawful Interception requirements for GSM (3GPP TR 41.033)
[58] TR 141 033 3GPP SA 3 Digital cellular telecommunications system (Phase 2+); Lawful Interception requirements for GSM (3GPP TR 41.033)
[59] TS 142 033 3GPP SA 3 Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 1 (3GPP TS 42.033)
[60] TS 143 020 3GPP SA 3 Digital cellular telecommunications system (Phase 2+); Security-related network functions (3GPP TS 43.020)
[61] TS 143 033 3GPP SA 3 Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 2 (3GPP TS 43.033)
[62] 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)
[63] 3GPP TS 55.216 Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS;

Document 1: A5/3 and GEA3 specification
[64] 3GPP TS 55.217 Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 2: Implementors' test data
[65] 3GPP TS 55.218 Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 3: Design and conformance test data
[66] 3GPP TR 55.919 Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report
[67] TS 122 016 Technical Specification Group Services and System Aspects; International Mobile station Equipment Identities (IMEI) (3GPP TS 22.016)
[68] TS 123 003 Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Numbering, Addressing and Identification
[69] TS 122 242 Universal Mobile Telecommunications System (UMTS); Digital Rights Management (DRM); Stage 1 (3GPP TS 22.242)
[70] TR 122 950 Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Priority service feasibility study; (3GPP TR 22.950)
[71] TR 122 952 V6.2.0 (2005-01); Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Priority service guide; (3GPP TR 22.952)
[72] TS 101 513 3GPP SA 5; Details and Download Digital cellular telecommunications system (Phase 2+) (GSM); Location Services (LCS); Location services management; (GSM 12.71)
[73] TS 101 726 3GPP GERAN 2; Details and Download Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Serving Mobile Location Centre - Base Station System (SMLC-BSS) interface; Layer 3 specification; (3GPP TS 08.71)
[74] TS 101 724 3GPP SA 2; Details and Download Digital cellular telecommunications system (Phase 2+) (GSM); Location Services (LCS); (Functional description) - Stage 2 (GSM 03.71)
[75] TS 101 726 Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Serving Mobile Location Centre - Base Station System (SMLC-BSS) interface; Layer 3 specification (3GPP TS 08.71)
[76] TS 101 725; Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Mobile radio interface layer 3 Location Services (LCS) specification (3GPP TS 04.71)
[77] TS 123 119 Universal Mobile Telecommunications System (UMTS); Gateway Location Register (GLR); Stage2 (3GPP TS 23.119)
[78] 3GPP TS 24.008: "3GPP Technical Specification Group Core Network; Mobile radio interface Layer 3 specification, Core network protocol; Stage 3"
[79] TS 100 929 Global System for Mobile communication (GSM) (Phase 2+); Security related network functions (GSM 03.20)
[80] TS 100 614 Digital cellular telecommunications system (Phase 2+) (GSM); Security management

[81] ETS 300 506 Digital cellular telecommunications system (Phase 2) (GSM); Security aspects (GSM 02.09)

TETRA

[82] TR 102 021-7 Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 7

[83] EN 300 392-7 Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security Voice plus data

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

[85] EN 300 812 Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM-ME) interface

[86] ES 202 Terrestrial Trunked Radio (TETRA); Security; Synchronisation mechanism for end-to-end encryption

[87] EN 300 812 Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM-ME) interface

[88] ES 200 812-1 Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 1: Physical and logical characteristics

[89] ES 200 812-2 Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 2: Characteristics of the TSIM application

DECT

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

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

[92] ETS 300 759 Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM); Test specification for DAM

[93] ETS 300 760 Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM); Implementation Conformance Statement (ICS) proforma specification

[94] ETS 300 825 Digital Enhanced Cordless Telecommunications (DECT); 3 Volt DECT Authentication Module (DAM)

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

Lawful interception

Published by TC LI

[96] ES 201 671 Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic.

[97] ES 201 158 Lawful Interception (LI); Requirements for Network Functions

[98] TS 102 232 Lawful Interception (LI); Handover Specification for IP Delivery

[99] TS 102 233 Service-specific details for e-mail services

[100] TS 102 234 Lawful Interception (LI); Service-specific details for internet access services;

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

[102] TS 101 331; Lawful Interception (LI); Requirements of Law Enforcement Agencies

[103] TR 102 053 Lawful Interception (LI); Notes on ISDN lawful interception functionality.

[104] TR 101 944 Lawful Interception (LI); Issues on IP Interception.

[105] TR 101 943 Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture.

[106] TS 102 815 Lawful Interception (LI); Service-specific details for Layer 2 Lawful Interception

[107] ETSI TR 102 503 Lawful Interception (LI); ASN.1 tree structure of the Security Domain

Published by other technical bodies

[108] EG 201 781 Intelligent Networks (IN); Lawful Interception. [TC SPAN]

[109] TR 101 772 Telecommunications and Internet Protocol Harmonisation Over Networks (TIPHON) Release 3; Service independent requirements definition; Lawful interception – top level requirements. [EP TIPHON]

[110] TR 101 750 Telecommunications and Internet Protocol Harmonisation Over Networks (TIPHON™); Security; Studies into the Impact of lawful interception. [EP TIPHON]

[111] EN 301 040 Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface. [EP TETRA]

[112] EG 201 040 Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface; Feasibility study report. [EP TETRA]

[113] TR 101 514 Digital cellular telecommunications system (Phase 2+); Lawful interception requirements for GSM (GSM 01.33 version 8.0.0 Release 1999). [TC SMG]

[114] TS 101 507 Digital cellular telecommunications system (Phase 2+); Lawful interception - Stage 1 (GSM 02.33 version 8.0.1 Release 1999). [TC SMG]

[115] TS 143 033 Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 2 (3GPP TS 43.033 version 5.0.0 Release 5). [3GPP SA3]

[116] TS 142 033 Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 1 (3GPP TS 42.033 version 5.0.0 Release 5). [3GPP SA3]

[117] TR 141 033 Digital cellular telecommunications system (Phase 2+); Lawful Interception requirements for GSM (3GPP TR 41.033 version 5.0.0 Release 5). [3GPP SA3]

[118] TS 133 108 Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108 version 5.4.0 Release 5). [3GPP SA3]

[119] TS 133 107 Universal Mobile Telecommunications System (UMTS); 3G security; Lawful interception architecture and functions (3GPP TS 33.107 version 5.5.0 Release 5). [3GPP SA3]

[120] TS 133 106 Universal Mobile Telecommunications System (UMTS); Lawful interception requirements (3GPP TS 33.106 version 5.1.0 Release 5). [3GPP SA3]

[121] TS 101 509 Digital cellular telecommunications system (Phase 2+) (GSM); Lawful interception; Stage 2 (3GPP TS 03.33 version 8.1.0

Release 1999). [3GPP SA3]

[122] 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

[123] 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

[124] TR 102 044 Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates

[125] TR 102 045 Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model

[126] TR 102 046 Electronic Signatures and Infrastructures (ESI); Maintenance of ETSI standards from EESSI phase 2 and 3

[127] TR 102 047 Electronic Signatures and Infrastructures (ESI); International Harmonisation of Electronic Signature Formats

[128] TR 102 040 Electronic Signatures and Infrastructures (ESI); International Harmonisation of Policy Requirements for CAs issuing Certificates

[129] TS 102 231 Electronic Signatures and Infrastructures (ESI); Provision of harmonised Trust Service Provider status information

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

[131] TR 102 153 Electronic Signatures and Infrastructures (ESI); Pre-study on certificate profiles

[132] SR 002 176 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures

[133] TS 101 733 Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)

[134] TS 102 280 X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons

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

[136] TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates

[137] TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates

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

[139] TS 101 903 Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)

[140] TS 101 862 Electronic Signatures and Infrastructures (ESI); Qualified Certificate profile

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

[142] 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

[143] TR 102 041 SEC ESI; Signature Policies Report

[144] TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities

[145] TS 101 861 SEC ESI; Electronic Signatures and Infrastructures (ESI); Time stamping profile

[146] TR 102 038 XML format for signature policies

[147] TR 102 030 SEC ESI; Provision of harmonised Trust Service Provider status information

[148] TR 102 046 Electronic Signatures and Infrastructures (ESI); Maintenance report

Next Generation Networks

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

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

[151] 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

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

[153] TR 102 420 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of activity on security

[154] TR 102 055 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); ENUM scenarios for user and infrastructure ENUM

[155] TS 187 001; TISPAN NGN Security (NGN_SEC) Requirements – NGN Release 1

[156] DTS/TISPAN-07015-NGN; TISPAN NGN Security – Framework and Requirements - Release Independent

[157] TR 187 002; TISPAN NGN Security -Threat and Risk Analysis – NGN Release 1

[158] TS 187 003; TISPAN NGN Security - Security Architecture – NGN Release 1

[159] TS 102 165-1 TISPAN 07 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis

[160] TS 102 165-2 TISPAN 07 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures

Security Algorithms

[161] TCTR 003 Security Algorithms Group of Experts (SAGE); European Encryption Algorithm for the use in audiovisual systems

[162] TCTR 001 Security Algorithms Group of Experts (SAGE); Requirements specification for an encryption algorithm for use in audio visual systems

[163] TCTR 002 Security Algorithms Group of Experts (SAGE); Report on the specification and evaluation of the GSM cipher algorithm A5/2

[164] TCTR 004 Security Algorithms Group of Experts (SAGE); Cryptographic Algorithm for the European Multi-Application IC-Card

[165] TCTR 005 Security Algorithms Group of Experts (SAGE); UPT Authentication Algorithm for the use in DTMF Devices

[166] TCRTR 032 Security Algorithms Group of Experts (SAGE); Rules for the management of the TESA-7 algorithm

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

[168] MI/SAGE-0008 SAGE Cryptographic algorithm for Public Network Operators

[169] TCRTR 035 Security Algorithms Group of Experts (SAGE); Rules for the management of the Baras algorithm

[170] TR 101 053-1 Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 1: TEA1

[171] MI/SAGE-00010-2 Standard Trans European Trunked RAdio (TETRA) air interface encryption algorithm TEA1 and TEA2

[172] TR 101 053-2 Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 2: TEA2

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

[174] MI/SAGE-00011-2 SAGE Trans European Trunked RAdio (TETRA) set of air interface authentication and key management algorithms TAA1

[175] TR 101 054 Security Algorithms Group of Experts (SAGE); Rules for the management of the HIPERLAN Standard Encryption Algorithm (HSEA)

[176] MI/SAGE-00012-2 SAGE Standard air interface encryption algorithm for HIPERLAN

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

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

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

[180] MI/SAGE-00015-2 Security Algorithms Group of Experts (SAGE); GPRS encryption algorithm

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

[182] MI/SAGE-00016-2 Security Algorithms Group of Experts (SAGE); CTS Authentication and Key Generation Algorithm

[183] MI/SAGE-00017-2 Security Algorithms Group of Experts (SAGE); TEA3 and TEA4 Security Algorithms

[184] TR 101 053-3 Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 3: TEA3

[185] TR 101 053-4 Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 4: TEA4

[186] MI/SAGE-00018 SAGE Design of the 3GPP Encryption and Integrity algorithms

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

[188] MI/SAGE-00019-2 SAGE: Design of a Standard GSM GPRS Encryption algorithm 2 (GEA2)

[189] MI/SAGE-00020-2 SAGE: Design of authentication algorithm for UMTS

Emergency Telecommunications

[190] SR 002 180 Requirements for communication of citizens with authorities/organisations in case of distress (Emergency Call Handling).

[191] SR 002 299 The European regulation specific to Communication in Emergency situations during emergencies.

[192] TS 102 181 Emergency Communications (EMTEL); Requirements for communication between authorities/organizations during emergencies between authorities

[193] TS 102 182 Emergency Communications (EMTEL); Requirements for communications from authorities/organisations to the citizens during emergencies authorities to citizens

[194] TS 102 410 Emergency Communications (EMTEL); Requirements for communications between citizens during emergencies between citizens

[195] TR 102 444 Emergency Communications (EMTEL); Suitability of SMS and CBS for Emergency Messaging

[196] TR 102 445 Emergency Communications (EMTEL); Requirements for Emergency Communications Network Resiliency

[197] TS 170 001 Project MESA; Service Specification Group - Services and Applications; Statement of Requirements

[198] TS 170 002 Project MESA; Service Specification Group - Services and Applications; Definitions Symbols and Abbreviations

[199] TS 170 003 Project MESA; Service Specification Group - Services and Applications; Basic Requirements

Smart Cards

[200] ETSI TS 101 220 (V6.0.0): "Smart Cards; ETSI numbering system for telecommunication application providers (Release 6)"

[201] ETSI TS 102 124 "Smart Cards; Transport Protocol for UICC based

Applications; Stage 1 (Release 6)"

[202] ETSI TR 102 151 "Smart Cards; Measurement of Electromagnetic Emission of SIM Cards (Release 6)"

[203] ETSI TS 102 221 "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)".

[204] ETSI TS 102 223 (V4.3.0): "Smart cards; Card Application Toolkit (CAT) (Release 4)"

[205] ETSI TS 102 224 (V6.0.0): "Smart Cards; Security mechanisms for UICC based Applications - Functional requirements (Release 6)".

[206] ETSI TS 102 225 "Smart Cards; Secured packet structure for UICC based applications (Release 6)"

[207] ETSI TS 102 226 "Smart Cards; Remote APDU Structure for UICC based Applications (Release 6)"

[208] ETSI TS 102 230 (V4.1.0): "Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification (Release 4)"

[209] ETSI TS 102 240 (V6.0.0): "Smart Cards; UICC Application Programming Interface and Loader Requirements; Service description (Release 6)"

[210] ETSI TR 122 907 (V3.1.3): "Universal Mobile Telecommunications System (UMTS); Terminal and smart card concepts (3GPP TR 22.907 version 3.1.3 Release 1999)"

[211] ETSI TS 102 222: "Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications (Release 1999)" compliant with ISO/IEC 7816

[212] ETSI TS 102 310 “Smart Cards; Extensible Authentication Protocol support in the UICC (Release 6)”

RFID

[213] 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 Product Standard for 2 W RFID at UHF

[214] EN 302 208-2 ERM 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: Harmonised EN under article 3.2 of the R&TTE Directive Product Standard for 2 W RFID at UHF

Mobile Commerce

[215] TR 102 203 Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements

[216] TS 102 204 Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface Specification

[217] TR 102 206 Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework

[218] TS 102 207 Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature

[219] TR 102 071 Mobile Commerce (M-COMM); Requirements for Payment

Methods for Mobile Commerce

Broadcasting

[220] TS 101 197 BROADCAST Digital Video Broadcasting (DVB); DVB SimulCrypt; Head-end architecture and synchronisation

[221] EN 300 744 BROADCAST Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television; DVB-H PHY addition

[222] EN 301 192 BROADCAST Digital Video Broadcasting (DVB); DVB specification for data broadcasting

[223] TS 102 201 BROADCAST Digital Video Broadcasting (DVB); Interfaces for DVB Integrated Receiver Decoder (DVB-IRD)

[224] TS 103 197 BROADCAST Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt

[225] TS 102 822-7 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

[226] EN 301 790 BROADCAST; Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems

[227] ETR 289 BROADCAST; Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems

[228] ETSI TS 102 812 Digital Video Broadcasting (DVB); Multimedia Home Platform (MHP) Specification 1.1

Satellite

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

[230] TS 102 465 SES BSM; Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); General Security Architecture

[231] TS 102 466 SES BSM; Details and Download Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Multicast Security Architecture

[232] 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

[233] 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

[234] 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

[235] TS 101 442-6 Satellite Earth Stations and Systems (SES); Satellite Component of UMTS/IMT-2000; Multimedia Broadcast/Multicast Services part 6: Security

Terminals

[236] ETSI TS 101 909-11 Access and Terminals (AT); Digital Broadband

Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 11: Security

Generic Security Issues

[237] ETR 232 Network Aspects (NA); Security Techniques Advisory Group (STAG); Glossary of security terminology
[238] TCRTR 037 Network Aspects (NA); Security Techniques Advisory Group (STAG); Requirements specification for an encryption algorithm for operators of European public telecommunications networks
[239] ETR 235 Network Aspects (NA); Security Techniques Advisory Group (STAG); Requirements specification for an encryption algorithm for operators of European public telecommunications networks
[240] 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
[241] TCRTR 038 Network Aspects (NA); Security Techniques Advisory Group (STAG); A guide to the ETSI security standards policy
[242] ETR 236 Network Aspects (NA); Security Techniques Advisory Group (STAG); A guide to the ETSI security standards policy
[243] TCRTR 049 Network Aspects (NA); Security Techniques Advisory Group (STAG); Security requirements capture
[244] TCRTR 028 Network Aspects (NA); Security Techniques Advisory Group (STAG); Glossary of Security Terminology
[245] TCRTR 029 Network Aspects (NA); Security Techniques Advisory Group (STAG); A directory of security features in ETSI standards
[246] ETR 232 Network Aspects (NA); Security Techniques Advisory Group (STAG); Glossary of security terminology
[247] ETR 332 Network Aspects (NA); Security Techniques Advisory Group (STAG); Security requirements capture
[248] TCRTR 042 Network Aspects (NA); Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms
[249] TCRTR 030 Network Aspects (NA); Security Techniques Advisory Group (STAG); A guide to specifying requirements for cryptographic algorithms
[250] ETR Network Aspects (NA); Security Techniques Advisory Group (STAG); A guide to specifying requirements for cryptographic algorithms
[251] ETR 237 Network Aspects (NA); Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms
[252] ETR 330 Network Aspects (NA); Security Techniques Advisory Group (STAG); A guide to legislative and regulatory environment
[253] 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"

GLOSSARY

3GPP	Third Generation Partnership Project
CA	Certification Authority
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CEPT	European Conference of Posts and Telecommunications Administrations
CSP	Certificate Service Provider
DECT	Digital Enhanced Cordless Telecommunications
EC	European Commission
EDGE	Enhanced Data Rates for GSM Evolution
EMTEL	Emergency Telecommunications
EP	ETSI Project
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communication
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISO	International Organisation for Standardisation
ISO-OSI	International Organisation for Standardisation-Open System Interconnection
IT	Information Technology
LI	Lawful Interception
MNO	Mobile Network Operator
NGN	Next Generation Networks
PAMR	Public Access Mobile Radio
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMR	Private Mobile Radio
RFC	Request for Comment
RFID	Radio Frequency Identification
RP	Relying Party
SIM	Subscriber Identity Module
TC	Technical Committee of ETSI
TDMA/TDD	Time Division Multiple Access/Time Division Duplex
TETRA	TErrestrial Trunked RAdio
TR	ETSI Technical Report
TS	ETSI Technical Specification
TSA	Time Stamping Authority
UICC	Universal Integrated Circuit Card
UHF	Ultra High Frequency
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
WLAN	Wireless Local Area Network
XAdES	XML Advanced Electronic Signature
XML	eXtended Mark up Language