ETSI TECHNICAL COMMITTEE REFERENCE TECHNICAL REPORT

TCR-TR 029

May 1995

Source: ETSI TC-NA

Reference: DTR/NA-002504

ICS:

Key words: Security

Security Techniques Advisory Group (STAG); A directory of security features in ETSI standards

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

New presentation - see History box

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Blank page

Foreword

This Technical Committee Reference Technical Report (TCR-TR) has been produced by the Network Aspects Security Techniques Advisory Group (NA/STAG) of the European Telecommunications Standards Institute (ETSI).

This TCR-TR provides an overview of security features which have been specified as part of ETSI standards.

This information could be used by ETSI TCs and STCs as reference and/or background information when drafting new standards which incorporate security features.

Blank page

1 Scope

Security features have been incorporated in a number of European Telecommunication Standards (ETSs), and are likely to become an increasingly important aspect of ETSI work as digital technology comes more and more into use.

This Technical Committee Reference Technical Report (TCR-TR) provides an overview of security features which currently have been integrated, or are in the process of integration, into an ETS.

For each of the activities the scope and status of the work is described.

Also some potential security activities which are identified or planned as future ETSI activities are listed.

This TCR-TR is intended to be a reference document describing the actual status of the security work within ETSI.

For each of the activities described, the corresponding classes from the classification given in ITSTC Memorandum M-IT-06 [1] are indicated. In cases where an activity corresponds to more than one class, the most relevant class is listed first.

It is intended to update this TCR-TR regularly.

2 References

This TCR-TR incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this TCR-TR only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] CEN/CENELEC/ETSI ITSTC Memorandum M-IT-06, issue 1.2: "Taxonomy & Directory of European Standardisation Requirements for Information Systems Security".

[2] TCR-TR 028: "Network Aspects (NA); Security Techniques Advisory Group (STAG); Glossary of security terminology".

3 Definitions

For the purposes of this TCR-TR, the following definitions apply:

A glossary of security definitions and terminology is provided by TCR-TR 028 [2].

4 Abbreviations

For the purposes of this TCR-TR, the following abbreviations apply:

DECT	Digital European Cordless Telecommunications
ERMES	European Radio MEssage System
ETR	ETSI Technical Report
ETS	European Telecommunication Standard
GSM	Global System for Mobile communications
IN	Intelligent Network
ITSEC	Information Technology Security Evaluation Criteria
ISDN	Integrated Services Digital Network
MCU	Multipoint Connection Unit
PNO	Public Network Operator
SAGE	Security Algorithm Group of Experts
STAG	Security Techniques Advisory Group
STC	(ETSI) Sub Technical Committee
TC	(ETSI) Technical Committee
TETRA	Trans European Trunked RAdio system
TMN	Telecommunications Management Network
UMTS	Universal Mobile Telecommunications System
UPT	Universal Personal Telecommunications

5 Overview of ETSI security related standards

Within ETSI the work on security is or has been undertaken in a number of TC's and STC's. This clause provides an overview of these activities.

Where possible, the security activities are classified according to the classification provided by M-IT-06 [1].

I. TC/BTC - Business Telecommunications

Description

STC/BTC4 is preparing an ETSI Technical Report (ETR) which will include information on the security aspects of broadband private networks.

Status of the work

Under preparation, with target date of June 1995 for TC approval.

Documents

DTR/BTC-04002:	"Private Networks; Broadband; Operations and interconnections aspects", draft ETR with target date for TC approval June 1995.

II. STC/NA6 - Intelligent Networks (IN)

Description

ETSI NA6 is responsible for the specification of IN is addressing security for IN. A draft TC-TR is well under way. There is a relation to UPT security (ETSI NA7).

Status of the work

Ongoing.

Documents

DTR/NA-061201:	"Intelligent Network (IN); Security requirements for global IN systems", draft TC-TR with target date for TC approval October 1994.

Corresponding M-IT-06 classification

S0.2.2.8	Architecture and Modelling - Telecommunications Systems.

Possibly others.

III. STC/NA7 - Universal Personal Telecommunication (UPT)

Description

Universal Personal Telecommunication (UPT) is a telecommunication service which provides to the UPT-user personal mobility for incoming and outgoing telecommunication calls, as well as permitting the user to use his personal related supplementary/value added services. UPT shall be independent of the terminals and networks used.

At the end of 1991, a Security Expert Group was installed in ETSI NA7, with the aim to define a security architecture and security standards for the different phases of UPT.

It should be noted that the work on UPT originated in ITU-T SG1. It does not seem however that security issues have been addressed there.

Work has now begun on the security aspects of UPT phase 2, and a number of new work items have been adopted.

Status of the work

The threats analysis has been completed. Work on the security architecture of phase 1 is virtually completed, whilst work on phase 2 is commencing.

Documents

ETR 055-4: "Universal Personal Telecommunications (UPT); The service concept; Part 4: Service requirements on security mechanisms", published February 1993.

ETR 055-11: "Universal Personal Telecommunications (UPT); The service concept; Part 11: Service requirements on protection of third parties", published August 1993.

ETR 083: "Universal Personal Telecommunications (UPT); General UPT security architecture", published July 1993.

NA-TR 010: "Universal Personal Telecommunications (UPT); Phase 1: Service requirements on security features", published May 1993.

ETS 300 391-1: "Universal Personal Telecommunications (UPT); Specification of the security architecture for UPT Phase 1; Part 1: Specification", On Vote 80, ends 28 July 1995.

ETS 300 391-3: "Universal Personal Telecommunications (UPT); Specification of the security architecture for UPT Phase 1; Part 3: Conformance Test Specification (CTS)", On Vote 80, ends 28 July 1995.

NA-TR 014: "Universal Personal Telecommunications (UPT); Authentication algorithm for Phase 1 Requirements specification", published June 1993.

DE/NA-072401: "Universal Personal Telecommunications (UPT); Phase 2; Realisation of the security architecture", draft ETS with target date for STC approval March 1995.

DTR/NA-072402: "Universal Personal Telecommunications (UPT); Phase 2; Security algorithms Requirements specification", draft TC-TR with target date for TC approval May 1995.

DE/NA-072403: "Universal Personal Telecommunications (UPT); Phase 2; Conformance test suite for realization of security architecture", draft ETS with target date for STC approval June 1995.

Corresponding M-IT-06 classification

S0.2.2.8	Architecture and Modelling - Telecommunications Systems.
S1.1.2.2	Secure System Design - Cryptographic Techniques.

IV. STC NA/STAG - Security Techniques Advisory Group

Description

STAG was established to support the security activities within ETSI. It has developed a work programme which has as main goal the development of a Security Standards Policy. Furthermore, STAG is responsible for ETSI's liaison activities in the area of security and will provide advice and technical assistance to ETSI TCs and STCs. STAG will also take technical initiatives in case a need is identified for certain security features which are not currently being addressed by any TC/STC.

Status of the work

Ongoing.

Documents

The following documents will be produced by STAG (all are intended to be TCR-TRs):

TCR-TR 038:	A guide to ETSI security standards policy.
DTR/NA-002501:	Guidelines and methods for identifying, analysing and documenting security requirements for telecommunication systems and services.
DTR/NA-002502:	Guidelines for Security Standardisation.
TCR-TR 028:	A glossary of security terminology.
TCR-TR 029:	A directory of security features in ETSI standards.
DTR/NA-002601:	Baseline security standards.
DTR/NA-002602:	Security management techniques.
DTR/NA-002603:	Guidelines for Integrating Security Mechanisms into ETSI Standards.
TCR-TR 030:	A guide to specifying Requirements for Cryptographic Algorithms.
DTR/NA-002701:	Guidelines on the relevance of security evaluation to ETSI standards.
DTR/NA-002801:	A guide to legislation, recommendations and guidelines governing the provision of security features.

Corresponding M-IT-06 classification

For each of the above documents the corresponding M-IT-06 class is given below.

TCR-TR 038:	S0.4.1	Security policy guidelines.
DTR/NA-002501:	S0.3.1	Risk analysis methods.
DTR/NA-002502:	S1.4.1/ S0.4.2	Guidelines on the use and application of security techniques/architectural guidelines.
TCR-TR 028:	SO.4.4	Definitions and terminology.
TCR-TR 029:	S1.1.6/ S1.1.2.1	Secure system design - system specific/classes of mechanisms.
DTR/NA-002601:	S1.1.2.1	Classes of mechanisms.
DTR/NA-002602:	S1.1.4	Security management techniques.
DTR/NA-002603:	S2.2.1	Integration methods.
TCR-TR 030:	S1.1.3	Security interfaces.
DTR/NA-002701:	S2.5.3	Guidelines on evaluation and certification.
DTR/NA-002801:		No specific class, partly S1.4.2 - Guidelines on secure system design, S0.4.1 - security policy guidelines.

V. STC/RES3 - Digital European Cordless Telecommunications (DECT)

Description

As part of the DECT specification a security architecture was specified with mutual authentication of Portable Part (PP) and Fixed Part (FP) and confidentiality of user and signalling data. The security features of DECT are the following:

a) authentication of a PP by a FP, using a conventional challenge / signed response protocol;

b) authentication of a FP by a PP, using a conventional challenge / signed response protocol;

c) mutual authentication of a PP and a FP in three different options (a) and b), a) and d) and enforced encryption with a fixed key);

d) data confidentiality by means of encryption (over the radio path only);

e) user authentication, by using a personal code in combination with either a), b) or c);

f) security attributes, by providing signalling elements to indicate capabilities.

A standard authentication (optional) algorithm and a standard encryption algorithm (optional) are specified, only for use in DECT and subject to a non-disclosure agreement. The specification also contains a set of recommended security profiles.

Status of the work

Complete, work is proceeding on the test specifications.

Documents

ETS 300 175-7: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT); Common interface; Part 7: Security features", ETS, published October 1992.

prETS 300 331: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT); Common interface; DECT Authentication Module (DAM)", draft ETS on post-Public Enquiry review.

Corresponding M-IT-06 classification

S0.2.2.8	Architecture and modelling - telecommunications systems.
S1.1.2.2	Secure system design - cryptographic techniques.
S1.3.4.8	Profiles - telecommunications systems.

VI. STC/RES6 - Trans European Trunked Radio (TETRA)

Description

Within ETSI RES6 the TETRA system for Trans European Trunked Radio is being specified. RES6 has established an expert group for security. In the first phase (May 1994) confidentiality of traffic on the air interface will be specified; authentication of users, confidentiality on broadcast control channels, hooks for end to end security, as well as other security services, will be worked out in subsequent phases.

Status of the work

Ongoing.

Documents

ETR 086-3: "Trans European Trunked RAdio (TETRA) systems; Technical requirements specification; Part 3: Security aspects", ETR published January 1994.

prI-ETS 300 392-7: "Trans-European Trunked RAdio (TETRA) systems; Voice plus data services; Part 7: Security", draft I-ETS with target date for TC approval 30 June 1994.

prI-ETS 300 393-7: "Trans-European Trunked RAdio (TETRA) systems; Packet Data Optimised (PDO); Part 7: Security", draft I-ETS with target date for TC approval 30 June 1994.

Corresponding M-IT-06 classification

S0.2.2.8 Architecture and modelling - telecommunications systems.

VII. SAGE - Security Algorithms Expert Group

Description

SAGE was established with the objective of designing all cryptographic algorithms for ETSI STCs, and is also available, subject to resources, to design algorithms for parties outside ETSI.

SAGE has completed the specification of an encryption algorithm for the GSM MoU Group. At the moment SAGE is working on an authentication algorithm for TE9 and encryption algorithm for the candidate TE10 standards (audio visual services).

Work is under way on an authentication algorithm for NA7 (UPT).

Status of the work

Ongoing.

Documents

SAGE-TR 001 "Security Algorithms Group of Experts (SAGE); Requirements for an encription algorithm for use in audio visual systems", TC-TR published December 1993.

SAGE-TR 002 "Security Algorithms Group of Experts (SAGE); Report on the specification and evaluation of the GSM cipher algorithm A5/2", TC-TR published December 1993.

Corresponding M-IT-06 classification

S1.1.2.2	Secure system design - cryptographic techniques.

VIII. TC/SMG - Digital mobile communications

Description

For the pan-European GSM system a security architecture has been defined. The main goals are authentication of mobile subscribers and provision of confidentiality over the radio path. The following security features are incorporated:

a) mobile subscriber identity authentication using a conventional challenge / signed response protocol;

b) user data confidentiality on physical connections by means of encryption (over the radio path only);

c) signalling information element confidentiality by means of encryption (over the radio path only);

d) mobile subscriber identity confidentiality by issuing temporary identities;

e) connection less user data confidentiality, not supported by a mechanism;

f) optional control of supplementary services by the subscriber using a password.

The use of an operator defined authentication algorithm and up to seven GSM standard encryption algorithms is specified. At the moment two such algorithms have been defined. These are only for use in GSM.

Status of the work

Phase 1 of the GSM is complete, apart from the necessary updating of the technical specifications and their conversion into formal standards (ETSs and I-ETSs as appropriate). Phase 2, which includes an enhanced range of services such as data-transfer, is now under way.

Documents

ETS 300 506: "European digital cellular telecommunications system (Phase 2); Security aspects (GSM 02.09)", Published September 1994.

ETS 300 509: "European digital cellular telecommunications system (Phase 2); Subscriber Identity Modules (SIM); Functional characteristics (GSM 02.17)", Published September 1994.

GSM TS 04.08: "European digital cellular telecommunications system (Phase 1); Mobile radio interface layer 3 specification; Part 3: Signalling support of the second ciphering algorithm (GSM 04.08)", Latest ETSI edition published January 1995.

I-ETS 300 022-3: "European digital cellular telecommunications system (Phase 1); Mobile radio interface layer 3 specification; Part 3: Signalling support of the second ciphering algorithm (GSM 04.08)" Extension of GSM 04.08 to cover dual ciphering algorithms, I-ETS published February 1994.

GSM TS 08.08: "European digital cellular telecommunications system (Phase 1); BSS-MSC layer 3 specification, part 2", Latest ETSI edition published January 1995.

GSM TS 08.58: "European digital cellular telecommunications system (Phase 1); BSC-BTS layer 3 specification, part 3", latest ETSI edition published January 1995.

GSM 03.05: "European digital cellular telecommunications system (Phase 1); Technical Performance Objectives", latest edition ETSI-GSM Technical Specification published February 1992.

ETS 300 534: "European digital cellular telecommunications system (Phase 2); Security related network functions (GSM 03.20)", Published September 1994.

prETS 300 614: "European digital cellular telecommunications system (Phase 2); Security management (GSM 12.03)",draft ETS, TC approved for Public Enquiry in April 1995.

Corresponding M-IT-06 classification

S0.2.2.8	Architecture and modelling - telecommunications systems.
S1.1.2.2	Secure system design - cryptographic techniques.

IX. STC/SMG5 -Universal Mobile Telecommunications System (UMTS)

Description

Universal Mobile Telecommunication System (UMTS) aims at the provision of mobile services to users, including systems like GSM, DECT, ERMES, etc. UMTS aspires to a functional integration of above mentioned systems and will be universally provided in both public and business environment.

Compared with GSM, for UMTS a more dynamic data storage and retrieval is considered to reduce signalling load. This will have consequences to security of this data, both with respect to access and security during transport.

In UMTS security services can be defined, providing identification and authentication, data integrity, confidentiality of transported data via the radio path and confidentiality of identity and location of a user. Identification and authentication aspects do not differ much from GSM. However, confidentiality within UMTS deals with different network operators and possibly with high bit rates.

Status of the work

Ongoing.

Documents

DTR/SMG-050901:	"Security principles for the Universal Mobile Telecommunication System (UMTS)", draft ETR targetted for TC approval October 1994.

Corresponding M-IT-06 classification

S0.2.2.8 Architecture and modelling - telecommunications systems.

X. STC/TE3 - Message handling systems

Description

In joint work with EWOS, TE3 drafted specifications for message handling including significant security features.

Status of the work

Ongoing.

Documents:

ENV 41 214:	"Message Handling Common Facilities MTS End-User to MTS End-User and MTA (FS A/3311)", ETSI work item T/TE-09-02, published by CENELEC as an ENV, Joint work with EWOS.
ENV 41 218:	"Message Handling Common Facilities User Agent to Message Store (A/MH12)", ETSI work item T/TE-09-03, published by CENELEC as an ENV, Joint work with EWOS (work item MHS002).
ENV 41 219:	"Functional standard A/MH13 Message Transfer Service (MTS) user to Message Transfer Agent (MTA) (P3)", ETSI work item T/TE3-01.3, published by CENELEC as an ENV, Joint work with EWOS (work item MHS007).
ENV 41 220:	"Functional standard A/MH 31 Message handling systems - Electronic Data Interchange Messaging; Interchange Messaging Service (EDIMS): Electronic Data Interchange (EDI) to EDI User Access (EDIUA)", ETSI work item DEN/TE-03041, published by CENELEC as an ENV, Joint work with EWOS (work item MHS004).

Corresponding M-IT-06 classification

S0.2.2.8	Architecture and modelling - telecommunications systems.

XI. STC/TE6 - X500 Directory

Description

In joint work with EWOS, TE6 specified security features for the X500 Directory.

Status of the work

Ongoing.

Documents:

ETR 097:	"Terminal Equipment (TE); Security architecture for the directory", ETR published April 1994, published also as EWOS ETG 027.
MI/TE-06023:	"STRONG authentication Profile ref: ADI41", miscellaneous work item in association with EWOS EG DIR, AOW and OIW.

Corresponding M-IT-06 classification

S0.2.2.8	Architecture and modelling - telecommunications systems.

XII. STC/TE9 - multi application smart cards

Description

ETSI TE9 works on standardisation of intelligent cards and card terminals for telecommunication applications. TE9 specifies a common set of functions which should be sufficient to fulfil the security requirements for most telecommunication applications. At the same time, for specific applications it's still possible to add on some security functions to meet their own specific security requirements.

Status of the work

Ongoing.

Documents:

EN 726-2: "Requirements for Integrated Circuit (IC) cards and terminals for telecommunication use: Part 2: Security framework", draft EN submitted to CEN for public enquiry (ETSI work item DEN/TE-09001-1).

EN 726-7: "Requirements for Integrated Circuit (IC) cards and terminals for telecommunication use: Part 7: Security module", draft EN submitted to CEN for public enquiry (ETSI work item DEN/TE-09001-6).

Corresponding M-IT-06 classification

S0.2.2.8	Architecture and modelling - telecommunications systems.
S1.1.2.2	Secure system design - cryptographic techniques.

XIII. STC/TE10 - Multi media planning and coordination

Description

Within ETSI NA3 some years ago work on security for audiovisual services was started. This work specifically focused on securing video conferencing in a (multiple) MCU environment. At the moment the work is handled by TE10. The original specification has been split up in two specifications, one for data confidentiality and one for key management and authentication. These specifications were forwarded to ITU-T where they now are processed.

The specified features are:

- data confidentiality, realised by link encryption (links terminal-terminal, terminal-MCU and MCU-MCU);
- authentication and key distribution, realised by a modified X.509 scheme;
- key distribution based on Diffie Hellman (extended protocol); and
- key distribution based on ANSI X9.17.

Status of the work

The work on data confidentiality is out for formal approval; the work on key management and authentication is being finalised at the moment.

TE10 is considering to adopt the standards as ETSs.

Documents

SAGE-TR 001: "Security Algorithms Group of Experts (SAGE); Requirements for an encription algorithm for use in audio visual systems".

Corresponding M-IT-06 classification

S1.1.2.2	Secure system design - cryptographic techniques.
S0.2.2.8	Architecture and modelling - telecommunications systems.

6 Future ETSI security activities

This clause lists a number of potential security (standardisation) activities to be dealt with by ETSI, which are not yet clearly allocated and structured within the ETSI work programme.

Where possible, the security activities are classified according to the classification provided by M-IT-06 [1].

P-I. TMN security

The need to study and possibly standardise TMN security was identified by ETSI TC NA. At the moment no concrete actions to actually start work on this issue have been initiated.

Corresponding M-IT-06 classification

S0.2.2.8	Architecture and modelling - telecommunications systems.

Possibly others.

P-II. Requirements for a PNO encryption algorithm

The potential need for a PNO encryption algorithm, which could be used to protect the management of telecommunication systems has been identified. Both Eurescom and ETSI STAG (having the Eurescom work as basis) produced a requirements specification for such an algorithm. The algorithm will be designed by ETSI SAGE.

Corresponding M-IT-06 classification

S1.1.2.2	Secure system design - cryptographic techniques.

P-III. ITSEC for telecommunication systems

In the past few years significant effort has been undertaken to develop harmonised ITSEC evaluation criteria for Europe. The activities and supporting investigation programme (INFOSEC), which are coordinated by the CEC (DGXIII), have sofar only briefly addressed telecommunication systems. STAG might consider to investigate if and in how far ITSEC is (or should be) applicable for the evaluation of telecommunications systems, if in its current for it could be used for this purpose and what additional actions are needed.

Corresponding M-IT-06 classification

S2.3.1.2	Security evaluation criteria, methodologies and manuals - telecommunication systems, products and services.

P-IV. ISDN security

NA STAG is coordinating actions which are aimed to investigate if ETSI should take up work on ISDN security and what the scope of such work will be. It is expected that in the first half of 1993 a strategy for ETSI work on ISDN security will be established.

Corresponding M-IT-06 classification

S1.1.2.2	Secure system design - cryptographic techniques.

Possibly others.

P-V. HIPERLAN

ETSI RES10 is drafting specifications for high performance LANs. It is likely that as part of this work security features will be specified.

Corresponding M-IT-06 classification

S1.1.2.2	Secure system design - cryptographic techniques.

Possibly others.

History

Document history	
May 1995	First Edition
March 1996	Converted into Adobe Acrobat Portable Document Format (PDF)