SLOVENSKI STANDARD
SIST ETS 300 790 E1:2003

01-december-2003

Svetovne osebne telekomunikacije (UPT) – Varnostna arhitektura za UPT – Faza 2: Specifikacija

Universal Personal Telecommunication (UPT); Security architecture for UPT phase 2; Specification

Ta slovenski standard je istoveten z: ETS 300 790 Edition 1

ICS:

33.040.35 Telefonska omrežja Telephone networks

SIST ETS 300 790 E1:2003 **en**

EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 790

October 1997

Source: NA

Reference: DE/NA-064006

ICS: 33.020

Key words: UPT, security, card

Universal Personal Telecommunication (UPT); Security architecture for UPT Phase 2; Specification

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 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Foreword

This European Telecommunication Standard (ETS) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI).

This ETS, in association with ETS 300 791 [5], forms the specification of the security architecture for UPT Phase 2.

Transposition dates	
Date of adoption:	19 September 1997
Date of latest announcement of this ETS (doa):	31 December 1997
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	30 June 1998
Date of withdrawal of any conflicting National Standard (dow):	30 June 1998

Introduction

Universal Personal Telecommunication (UPT) is a service that enables improved access to telecommunication services by allowing personal mobility. It enables each UPT user to participate in a user defined set of subscribed services, and to initiate and receive calls on the basis of a unique, personal, network independent UPT number across multiple networks at any terminal, fixed, movable or mobile. Such participation is irrespective of geographic location, limited only by the network capabilities and restrictions imposed by the Service Provider (SP), the subscriber or the user himself. Calls to a UPT user may also be made by non-UPT users.

ETSI TC NA has defined three service scenarios for UPT (ETR 055). This ETS of the security architecture deals with the basic UPT service scenario (UPT Phase 2). This scenario should cover also the Global System for Mobile communications (GSM) network (whereas Phase 1 covered Public Switched Telephone Network (PSTN) and Integrated Services Digital Network (ISDN)), data services (whereas Phase 1 covered the telephony service), Identity Code (IC) cards and IC card reading devices or terminals for authentication (whereas Phase 1 covered only Dual Tone Multi-Frequency (DTMF) signalling for authentication). The UPT Phase 2 also offers a more complete set of service features, including registration for outgoing calls, secure answer, call pick-up and a set of supplementary UPT features.

A high level of security is a necessary condition for a telecommunication service like UPT to become a success. Accountability, incontestable charging, and privacy are important examples on requirements that have to be fulfilled by technical and organizational security measures.

Security mechanisms can only meet their purpose if they are integrated into the system in an appropriate way. Many of these mechanisms depend on the secure handling of secret information like authentication keys and Personal Identity Numbers (PINs).

This ETS in combination with ETS 300 391-1 [2] specifies the complete security architecture for UPT Phase 2. It should be noted that this ETS is meant to be in addition to the Phase 1 ETS ("delta document"). For instance, a new security mechanism using IC cards is described. For security reasons, authentication should be performed by means of UPT cards, when the infrastructure of UPT card reading terminals has been widely established. It is envisaged that the use of strong authentication will increase.

Blank page

1 Scope

This European Telecommunication Standard (ETS) provides a description of the additional requirements, features and mechanisms necessary to provide adequate security within the UPT service for Phase 2. It is based on the specification of the Security Architecture for UPT Phase 1, given in ETS 300 391-1 [2] and it specifies the additions to Phase 1 only. The specific security requirements, features and mechanisms additionally needed for UPT Phase 2 are specified in detail. Where applicable Phase 1 is referred to. Downwards compatibility to UPT Phase 1 is fulfilled. Both this ETS and ETS 300 391-1 [2] are based on the general UPT security architecture given in ETR 083 [1], which describes the threat analysis and security requirements. Only aspects of the UPT security architecture that concern the security of the overall UPT service and information exchange between the user and the network are standardized.

Clause 4 summarizes the Phase 2 relevant security requirements and security features. It also specifies the security requirements to provide UPT on GSM, ISDN and other modern networks. Furthermore, the requirements for cards in UPT (either via card reading terminals or card reading devices) and the requirements for data services are specified.

Clause 5 specifies the security mechanisms for access control, the two pass strong authentication mechanism, security management measures and security profiles.

Clause 6 summarizes the sizes of the parameters used in the mechanisms.

The next three clauses give the functional specifications of respectively the UPT card (see clause 7), the security protocol (see clause 8) and the Authenticating Entity (AE), (see clause 9).

Clause 10 describes the possible authentication algorithms to be used in UPT Phase 2, such as UPT Security Algorithm (USA-4) and TE7 Security Algorithm (TESA-7).

Three relevant Implementation Conformance Statement (ICS) proformas are specified in annexes.

2 Normative references

This ETS incorporates by dated or 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 ETS only when incorporated in it by amendment or revision. For undated references, the latest edition of the publication referred to applies.

[1] ETR 083 (1993): "Universal Personal Telecommunication (UPT); General UPT security architecture".

[2] ETS 300 391-1 (1995): "Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT Phase 1; Part 1: Specification".

[3] ISO/IEC 9646-7 (1995): "Information technology - Open systems interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[4] ETS 300 406 (1995): "Methods for Testing and Specification (MTS); Protocol and profile conformance testing specifications - Standardization methodology".

[5] ETS 300 791: " Universal Personal Telecommunication (UPT); Security architecture for UPT Phase 2 Conformance Test Specification (CTS)".

3 Definition and abbreviations

3.1 Definition

For the purposes of this ETS, the following definition applies:

UPT card: A UPT card is an IC card used for identification and authentication purposes in a UPT service. UPT cards can be used for one pass strong authentication in the advanced DTMFdevices and for two pass strong authentication in card reading terminals. For the purpose of this ETS the latter definition applies.

3.2 Abbreviations

For the purposes of this ETS, the following abbreviations apply:

AC	Authentication Code, calculated in the UPT cardand in the AE
AE	Authenticating Entity
ARA	Access Registration Address
CHV	Card Holder Verification
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
COLP	COnnected Line identity Presentation
CT	Command Type
CUG	Closed User Group
DTMF	Dual Tone Multi-Frequency
f	authentication algorithm
GSM	Global System for Mobile communications
IC	Identity Code
ICS	Implementation Conformance Statement
ISDN	Integrated Services Digital Network
K	Authentication Key
MAC	Message Authentication Code
NAP	Network Access Point
OCPIN	Outgoing Call PIN
OCR	Outgoing Call Registration
PIN	Personal Identity Number
PSTN	Public Switched Telephone Network
PUI	Personal User Identity
RAND	RANdom number
ROCR	Remote Outgoing Call Registration
SA	Secure Answer
SAPIN	Secure Answer PIN
SDF	Service Data Function
SIM	Subscriber Identification Module
SP	Service Provider
T	Timer value in the UPT card
T_{MAX}	Maximum value of T
TESA-7	TE7 Security Algorithm
UPT	Universal Personal Telecommunication
USA-4	UPT Security Algorithm

4 Security requirements and security features

Security features needed for UPT Phase 2 are specified according to the requirements presented in ETR 083 [1] and other ETSI UPT reports. In ETS 300 391-1 [2] are specified the security requirements related to the Phase 1 service.

Subclause 4.1 specifies the additional Phase 2 requirements. Subclause 4.2 specifies the security features and subclause 4.3 describes the limitations of security in UPT Phase 2.

4.1 UPT Phase 2 security requirements

The main sources for assessing the security requirements are the threat analysis performed in ETR 083 [1]. However, properties of Phase 1 security features when combined with Phase 2 services lead to new threats and security requirements as described in this subclause.

4.1.1 Requirements from the threat analysis

The same text as in ETS 300 391-1 [2], subclause 4.2.1 is valid. For UPT Phase 2 the following additions and changes, if any, are relevant.

Hereafter are listed the Phase 2 core and additional features, the new threats related to the use of these new UPT features and the requirements arising from the threat analysis.

Outcall registration, allcall registration, linked registration (features remotely activated or not):

- some people can take a subscription, intensively use it and avoid paying the bill. The impact is emphasized by the possibility to make several outcall registrations at the same time. This implies the need for more efficient security management and services restrictions in order to limit losses;

- masquerading as a UPT user for outcall registration, allcall registration and linked registration. For these UPT features masquerading is a stronger threat tyhan it is for single outgoing calls. Introducing these UPT features increases the economic risks in the case that an intruder acquires valid authentication data. An unauthorized UPT registration for outgoing calls can be exploited in a straight forward way and resulting in very high fraudulent usage. Therefore, the authentication feature shall make it as difficult as possible for an intruder to get valid authentication data. One pass strong authentication codes can sometimes be recorded offline or online in an unauthorized way and be used fraudulently there after. Two pass strong authentication is therefore considered stronger. A sophisticated way to masquerade as a UPT user is to monitor the line between the real user and his SP and when the authentication has been performed to cut the line to the user and act as the real user. This may lead to fake Outgoing Call Registration (OCR) and requires a security feature reducing the risks of this threat;

- a registered user may be unable to supervise the registered terminal(s). It shall be possible for the user to have the option to use an extra authentication feature in order to protect the access of the terminals he is registered on;

- a line subscriber may use his own line without being aware that a UPT user is registered on it for outgoing calls. The UPT user may receive later on the list of calls (itemized bill) made by the line subscriber. It is required that the line subscriber is warned that someone has registered for outgoing calls on his terminal.

Called party specified secure answering of incoming calls:

- if a third party is succeeding to masquerade as a UPT SP he may require an authentication to be performed simply by making a telephone call to the UPT user. The resulting authentication code (if the existing one pass strong authentication is used) or PIN (if the weak authentication is used), can be recorded and used later on for an illegal registration or outgoing call etc. This leads to the security requirement that two pass strong authentication shall be used.

- However, certain network access points do not support the use of two pass strong authentication. In that case a UPT user who is normally authenticated with two pass strong authentication, may be given the possibility to use the called party specified secure answer service with another authentication mechanism. Considering the threat mentioned above, therefore, a special authentication code for secure answer is introduced as a user option. This code shall be different from the one used for weak authentication.

Network specified secure answer:

- network specified secure answer is a UPT Phase 2 supplementary service with the same definition as for called party specified secure answer except this service requires two pass strong authentication. The service cannot be deactivated by the UPT user once subscribed to. It is recognized that this implies that some calls will be prevented.

Calling UPT user specified secure answer of calls to UPT users:

- similar threat and requirement as called party specified secure answering of incoming calls.

Call pick-up:

- to be sure that the right UPT user picks up the call, the use of the call pick-up procedure requires authentication of the user.

Multiple registration:

- in case of multiple terminal access registration, the threats misuse of subscription (no intention to pay the bill) and the masquerading threat will have increased risks and evaluation level. The security management functions (charging control, bill limitation) shall be dimensioned for this situation. The number of simultaneously registered terminals shall be limited.

Calling party identity presentation and calling party identity restriction:

- these supplementary services are similar to the corresponding services defined for PSTN and ISDN and should be subject to the same availability and restrictions as required by laws and rules for personal data integrity protection. If the calling party is a UPT user the terminal access number (line identity) shall never be presented to the called party, only the UPT identity, so that the UPT user location is not given away. This is required even in the case that the corresponding service Calling Line Identification Presentation (CLIP) for PSTN or ISDN is active i.e. UPT requirement in this case shall override the service of the underlying network;

- for emergency reasons certain called parties (e.g. police, fire brigade) may nevertheless be allowed to receive the CLIP even if the caller is a UPT user (override Calling Line Identification Restriction (CLIR));

- similar, even if the originating terminal access has CLIR activated, the UPT identity of a calling UPT user shall be presented to the called party if this is a UPT user with the supplementary service CLIP activated.

Connected user identity presentation:

- the location of a UPT user shall not be disclosed. If the called party is a UPT user, only the UPT identity shall be presented, not the terminal access number, even if the originating network terminal has the corresponding service COnnected Line identification Presentation (COLP) activated.

Connected user identity restriction:

- the terminal access number used by a UPT user shall not be presented. The calling terminal in this case also shall get no presentation of the terminal access number, even if the network service COLP is active.

Personal addressing:

- this service could lead to the misuse of personal data. SPs who offer this service shall avoid conflicts with relevant national laws and rules concerning the protection of personal data integrity.

UPT call forwarding supplementary services, ongoing call redirection, multiparty communication and all charge acceptance for incoming UPT calls:

- these services have in common that they effect charging in a way which may not have been envisaged when the initial call was set up. Charging may be increased substantially or transferred to other parties. Therefore the activation of these calls/services shall be subject to the same restrictions and limitations as are valid for other charged calls and are set in security or service profiles. Authentication shall be performed as during a normal outgoing call.

Reset of a UPT registration:

- this service is designed to protect third parties against unwanted UPT registrations. However it may also cause denial of service for the UPT users. This may be annoying especially if the registration is reset without the UPT user being aware of it.

  NOTE: No special security requirement is set up due to this threat. It is assumed that people, when the UPT service is widely spread, will develop new social habits that solves the problem, e.g. that a UPT user will ask the line subscriber for permission to register on his terminal and that the line subscriber will tell the UPT user, if he resets a registration already in use.

4.1.2 Personal data integrity issues

The same text as in ETS 300 391-1 [2], subclause 4.2.2. is valid. For UPT Phase 2 the following additions and changes are relevant.

UPT Phase 2 introduces new features which may be subject to special restrictions for the reason of personal data protection.

The UPT supplementary service calling party identity presentation can be expected to get the same legal restrictions as the corresponding service in the fixed networks. That means it can only be offered to users with the companion restriction service being made readily available. Care shall be taken that these restrictions do not bypass or are bypassed by supplementary services in the UPT supporting networks. Directives from the European Union in this area have not yet been approved (see document commission's amended proposal for a directive concerning personal data and privacy in the context of digital telecommunication networks (COM (94) 128) so the detailed solutions in this area shall be kept open for future legal requirements. (see also subclause 4.1.1).

Services like:

- connected user identity presentation;
- personal addressing;
- intended recipient identity presentation;
- advice of charge;

may also have implications regarding personal integrity and shall be designed in accordance with national laws and rules on the protection of personal data.

The use of multi application cards for supporting UPT may have effects on the protection of user data in one application against another application in the same card. The requirement is that user data in the UPT card application shall be protected against the unintended use by other applications located inside or outside the IC card.

4.1.3 Additional requirements on UPT interworking with GSM

Some additional security requirements may have to be fulfilled when UPT and GSM are interworking.

The interworking between UPT and GSM can be achieved in different ways which are not mutually exclusive.

The following list gives some examples:

- using the key pad of a GSM mobile station and weak authentication;

- using a simple DTMF device and weak authentication with a GSM mobile station;

- using an advanced DTMF device and strong authentication with a GSM mobile station;

- using a UPT card in a separate card reader connected to the GSM Mobile equipment;

- using a combined UPT/GSM multi application card with a GSM mobile station and the proposed GSM services based on the Subscriber Identification Module (SIM) application tool kit;