SLOVENSKI STANDARD
SIST ETS 300 391-1 E1:2003

01-december-2003

Svetovne osebne telekomunikacije (UPT) – Specifikacija varnostne arhitekture za 1. fazo sistema UPT – 1. del: Specifikacija

Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT phase 1; Part 1: Specification

Ta slovenski standard je istoveten z: ETS 300 391-1 Edition 1

ICS:

33.040.35 Telefonska omrežja Telephone networks

SIST ETS 300 391-1 E1:2003 **en**

EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 391-1

August 1995

Source: ETSI TC-NA

Reference: DE/NA-071401

ICS: 33.040

Key words: UPT, security, authentication

Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT phase 1; Part 1: 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 92 94 42 00 - Fax: +33 93 65 47 16

Contents

Blank page

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 defines the security architecture for Universal Personal Telecommunication (UPT) phase 1.

This ETS consists of 3 parts as follows:

Part 1: "Specification".

Part 2: "Implementation Conformance Statement (ICS) proformas".

Part 3: "Conformance Test Specification (CTS)".

Transposition dates	
Date of adoption of this ETS:	28 July 1995
Date of latest announcement of this ETS (doa):	30 November 1995
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 May 1996
Date of withdrawal of any conflicting National Standard (dow):	31 May 1996

Introduction

UPT is a service which enables improved access to telecommunication services by allowing personal mobility.

The UPT service 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 network provider. Calls to UPT may also be made by non-UPT users.

ETR 055-2 describes three service scenarios for UPT. This specification of the security architecture deals only with the restricted, short term UPT service scenario for UPT phase 1. This scenario has restrictions on networks, services, user friendliness and also on the possibilities to implement security features. The UPT phase 1 scenario is a set of UPT features that can be implemented without major changes to current technology, and is basically restricted to provision in Public Switched Telephone Networks (PSTNs) and Integrated Services Digital Networks (ISDNs). Only the telephone service is provided.

A high level of security is a necessary condition for a telecommunication system like UPT to become a success. Accountability, incontestable charging and privacy are important examples for requirements that need 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 Identification Numbers (PINs). Such data needs strong protection against unauthorized access, e.g. by implementation in logically and physically protected security modules.

Blank page

1 Scope

This European Telecommunication Standard (ETS) provides a description of the mechanisms necessary to provide adequate security within the Universal Personal Telecommunication (UPT) service for phase 1. It is based on the discussion and the conclusions of the general UPT security architecture given in ETR 083 [1].

In ETR 083 [1], the threat analysis leads to security features which are needed to counter the threats detected. Some of the threats are already countered by UPT service features. The security features and mechanisms against the remaining threats are discussed there for all UPT phases. In this ETS, the specific security requirements, features and mechanisms for UPT phase 1 are specified in detail.

Clause 4 summarizes the phase 1 relevant security requirements and security features by means of general descriptions. Clause 5 specifies the security mechanisms, especially for access control, authentication and some security management aspects. Profiles are specified for weak and strong authentication, respectively. Service limitations and other measures are recommended due to the restricted possibilities for the implementation of security features in UPT phase 1, especially if only weak authentication is used.

In clause 6, the sizes and some values of the parameters used in the following clauses are given. clause 7 specifies the requirements for the UPT access device concerning input, output, data storage and the processing of data. Clause 8 contains the standardization of the exchanged data in the protocol for authentication. The security requirements for the Service Data Function (SDF) are specified in clause 9. Finally, the options for the used authentication algorithm are discussed in clause 10.

Only aspects of the UPT security architecture that concern the security of the overall UPT system or data exchanges with network components are standardized.

Some security aspects need not be standardized, e.g. the mechanism used for Device Holder Verification (DHV), bill limitation techniques, the interface between the general part of the Dual Tone Multi Frequency (DTMF) device and its Security Module (SM), the subscription process and key management. They can be specified according to the service providers' needs, provided that the general security requirements are considered. However, examples and recommendations on how to realise these features are given in informative annexes.

Upwards compatibility to later UPT phases is considered as far as useful and possible. This covers especially the use of IC cards as recommended for UPT phase 2.

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 300 380 (1995): "Universal Personal Telecommunications (UPT); Access devices Dual Tone Multi Frequency (DTMF) sender for acoustic coupling to the microphone of a handset telephone".

3 Symbols and abbreviations

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

AC	Authentication Code, calculated in the UPT access device
AC'	Authentication Code, calculated in the AE
AE	Authenticating Entity
ARA	Access Registration Address
CER	Call Event Record
d	tolerance for the difference between the sequence number sent by the UPT access device and the sequence number stored in the SDF
DHV	Device Holder Verification
DTMF	Dual Tone Multi Frequency
f	algorithm for the calculation of the AC
FC	Feature Code
GP	General Part (of the DTMF device)
IN	Intelligent Network
K	Key
LPIN	Local Personal Identification Number
n	sequence number, used by the UPT access device
n'	expected sequence number, stored in the AE
n_s	sent part of the sequence number, i.e. the 16 least significant bits of n
NAP	Network Access Point
PABX	Private Automatic Branch Exchange
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PUI	Personal User Identity
RAA	Remaining Authentication Attempts
SCF	Service Control Function
SDF	Service Data Function
SLPIN	Special Local Personal Identification Number
SM	Security Module
SPIN	Special Personal Identification Number
UPT	Universal Personal Telecommunication
UPTN	UPT Number

4 Security requirements and security features

Security features needed for UPT are specified according to the requirements presented in this ETS and other related documents.

The different aspects which, alone or combined, serve to create a security feature are described in subclause 4.1. The security requirements are summarized in subclause 4.2. The chosen security features for UPT phase 1 are then presented in subclause 4.3, while subclause 4.4 describes some limitations of UPT security in phase 1. Finally subclause 4.5 gives a statement regarding the need for a secure Intelligent Network (IN) platform.

4.1 Security features in general

In UPT, as in all practical systems accessible by the general public, many different security features need to be present and co-operate to give the required level of overall security.

Security services may be distinguished as having one of the following properties:

preventive: intending to make the threat impossible;

reporting: giving the system management or the user information about security problems;

limiting: introducing restrictions into the system in order to limit the consequences of possible security breaches;

restoring: making a quick, safe and orderly return to normal operation after security problems have occurred;

deterrent: having the property that potential mis-users are deterred because they know about this security feature.

All of these properties are necessary and valuable elements in the overall UPT security architecture.

4.2 UPT security requirements

The main sources for assessing the security requirements are the threat analysis performed in ETR 083 [1], ETR 055-11 and the requirements on personal data integrity which have been presented in the legislative arena.

4.2.1 Requirements from the threat analysis

For phase 1, the most important threats are the following:

- masquerading threats, i.e. the threats where intruders masquerade as UPT users for incoming or outgoing calls;
- threats connected with unauthorized modification of subscription data or service profile data;
- incorrectness of billing data;
- unauthorized use of UPT access device;
- unauthorized remote registrations.

NOTE: For more detailed information, see ETR 083 [1].

Threats connected with secure answer, multiple registration and outcall registration are not relevant, because these features are not present in phase 1.

4.2.2 Personal data integrity issues

The security requirements on UPT resulting from the need to protect personal data are not, to a large extent, specific to UPT, but are typical for many telecommunication services, especially those offering personal or terminal mobility. Furthermore, they will depend heavily on European and national legislation enforced for the protection of personal data and the protection of third parties.

Therefore, when offering a specific UPT service or when designing data processing functions and defining the kind of data being generated or stored within the UPT systems, UPT service providers shall consider the relevant national data protection laws. Provisional guidelines are to be found in CEC Directive SYN 287. For UPT, special concern in this respect needs to be paid to the contents of personal data in the UPT service profile. This data and the access conditions to it for the service provider's personnel, the subscriber and the UPT user need to be limited, to be in close accordance with the relevant European guidelines and national laws. As these are, to a large extent, being progressed at present, this ETS only advises service providers to pay close attention to the requirements being formulated in this area.

Concerning the protection of third parties the most imminent requirement is the one proposed by CEC Directive SYN 288 regarding the necessary agreement of the third party in the call forwarding situation. Although this requirement is not yet formally decided it seems likely that this or a similar requirement will be legally enforced for the UPT service. This should primarily have impact on the UPT features which make use of remote registration. Remote registration for incoming calls is, in its effect, very similar to normal call forwarding, whereas local registration (performed at the line subscriber's premises) may be considered as having the (indirect) agreement of the line subscriber.

The threat analysis in ETR 083 [1] and the special document on third party protection, ETR 055-11, have also identified this requirement.