ETSI TECHNICAL REPORT

ETR 220

November 1995

Source: ETSI TC-NA

Reference: DTR/NA-007008

ICS: 33.040

Key words: UPT, security

Universal Personal Telecommunication (UPT); Phase 1 (restricted UPT service scenario); Service requirements on security features

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 ETSI Technical Report (ETR) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI).

ETRs are informative documents resulting from ETSI studies which are not appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status. An ETR may be used to publish material which is either of an informative nature, relating to the use or the application of ETSs or I-ETSs, or which is immature and not yet suitable for formal adoption as an ETS or an I-ETS.

This ETR specifies the service requirements on security features involved with the restricted Universal Personal Telecommunication (UPT) service (phase 1).

Blank page

1 Scope

This ETSI Technical Report (ETR) specifies the service requirements on security features involved with the restricted Universal Personal Telecommunication (UPT) service (phase 1). It gives an overview of the main security features and mechanisms from the UPT user's point of view.

The security architecture for UPT (phase 1) is given in ETS 300 391-1 [1]. A description of the Man-Machine Interface (MMI) for authentication procedures can be found in ETR 218 [2].

2 References

This ETR incorporates by dated and undated reference, provisions from other publications. These 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 ETR only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

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

[2] ETR 218: "Universal Personal Telecommunication (UPT); Phase 1 (restricted UPT service scenario); Man-machine interface".

3 Abbreviations

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

MMI	Man-Machine Interface
PIN	Personal Identification Number
PUI	Personal User Identity
UPT	Universal Personal Telecommunication

4 General security requirements

The freedom given to UPT users to move freely from one terminal to another also implies that attempts to fraudulently use their subscription can be performed from any terminal. UPT subscribers are therefore, more exposed to fraudulent attempts to use their subscriptions than ordinary subscribers. It is necessary that the UPT service provides sufficient security mechanisms, so that the level of risk incurred by UPT subscribers does not appear prohibitive in comparison with ordinary subscribers.

The security mechanisms provided by the UPT service, irrespective of their strength of protection, should however, not appear to the UPT user as complicated procedures. As far as possible, the security mechanisms should not appear to the UPT user as any extra complication at all, but be part of the general UPT procedures.

5 Forms of misuse

The UPT user may be exposed to various forms of misuse. These forms of misuse will concern for example:

- **fraudulent use:** misuse of a user's resources by unauthorized persons who impersonate the user;

- **fraudulent access to subscription data:** access to UPT service profile data by unauthorized means;

- **eavesdropping:** unauthorized listening or recording of information during the communication;

- **malicious behaviour:** malicious use of UPT procedures by third parties in order to interfere with, or degrade, the service offered to a UPT user.

Misuse may also occur between different network operators in a multi-operator environment.

6 Types of security features

From a user's point of view, various security features protecting against such misuse may be considered for phase 1. Possible security features could include:

1) subscription data access control;

2) user action authorization;

3) user event control;

4) user identity confidentiality;

5) user identity authentication.

NOTE: User data confidentiality is the property that the user information carried on traffic channels during communication is not made available or disclosed to unauthorized individuals, entities or processes. User data confidentiality will depend on the terminals, services and networks used, and must be considered outside the scope of UPT; it is not a UPT feature.

6.1 Subscription data access control

Subscription data access control is the property that the UPT user's service profile data is protected against unauthorized access.

Only the UPT user, the UPT subscriber and the UPT service provider should be authorized for operations on a UPT user's service profile. Any unauthorized access attempts should be rejected and possibly recorded.

Subscription data access control should be **mandatory** for UPT service providers, and should be a natural part of the UPT subscription.

6.2 User action authorization

User action authorization is the property that the UPT user's actions are authorized.

The UPT subscriber will, at subscription time, set up a matrix of authorized actions in the UPT service profile (like access parameters for service management procedures, interrogation or modification, a list of services and facilities actually subscribed to, etc.).

User action authorization should be **mandatory** for UPT service providers, and should be a natural part of the UPT subscription.

6.3 User event control

User event control is the property that the UPT user has a certain control over which events the UPT user may be exposed to by the network or by other users.

User event control may comprise various kinds of protection, including:

- protection against unexpected charges (e.g. credit limit);

- protection against disclosure of physical location during normal procedures (e.g. connected with certain number identification supplementary services, if applicable);

- blocking of access to the UPT service for a subscription if the number of consecutive unsuccessful authentication attempts for this account exceeds a predefined limit;

- blocking the use of the UPT service from a terminal access if the number of unsuccessful authentication attempts originating from this terminal access exceeds a threshold (this threshold could be a number of attempts per time period).

Various forms of user event control should be **mandatory** for UPT service providers, but **optional** for UPT users. User event control may, for example, be provided through UPT-specific supplementary services or through features of the UPT service profile.

6.4 User identity confidentiality

User identity confidentiality is the property that the user's identity is not made available or disclosed to unauthorized individuals, entities, or processes.

User identity confidentiality protects the UPT user's general privacy. For example it contributes to protect the UPT user against tracing of his physical location by illegal means.

User identity confidentiality may imply that the UPT user should use an identity (Personal User Identity (PUI)) for identifying the UPT user to the network which is different from that user's UPT number.

The use of a PUI should be **optional** for UPT users and for UPT service providers.

6.5 User identity authentication

User identity authentication is the property that the user's identity is verified to be the one claimed.

User identity authentication protects the user and the network against unauthorized and fraudulent use.

User identity authentication may imply that a UPT user will have to authenticate himself during each of the UPT procedures. The authentication mechanisms used may vary according to the procedures requested by the UPT user and the current user-state. One example is when the UPT user has registered for outgoing calls, requesting that each outgoing call set-up should be authenticated. In this case, the authentication procedure should be simple for the UPT user (e.g. by a Personal Identification Number (PIN) code) as the UPT user has already authenticated himself during the registration procedure.

User identity authentication should be **mandatory** in UPT.

History

Document history	
November 1995	First Edition

ISBN 2-7437-0327-X
Dépôt légal : Novembre 1995