ETSI
TECHNICAL
REPORT

ETR 055-4

December 1992

Source: ETSI TC-NA

Reference: DTR/NA-70203

ICS: 33.080

Key words: UPT, service, security

Universal Personal Telecommunication (UPT); The service concept Part 4: Service requirements on security mechanisms

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

ETSI Technical Reports (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 application of ETSs or I-ETSs, or which is immature and not yet suitable for formal adoption as an ETS or I-ETS.

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

This ETR constitutes Part 4 of a multi-part ETR, with the following titles:

ETR 055-1:	"Universal Personal Telecommunication (UPT); The service concept Part 1: Principles and objectives".
ETR 055-2:	"Universal Personal Telecommunication (UPT); The service concept Part 2: General service description".
ETR 055-3:	"Universal Personal Telecommunication (UPT); The service concept Part 3: Service aspects of charging, billing and accounting".
ETR 055-4:	"Universal Personal Telecommunication (UPT); The service concept Part 4: Service requirements on security mechanisms".
ETR 055-5:	"Universal Personal Telecommunication (UPT); The service concept Part 5: UPT terminals and UPT access devices".
ETR 055-6:	"Universal Personal Telecommunication (UPT); The service concept Part 6: UPT subscription and service profile".
ETR 055-7:	"Universal Personal Telecommunication (UPT); The service concept Part 7: User procedures and user states".
ETR 055-8:	"Universal Personal Telecommunication (UPT); The service concept Part 8: Man-machine interface aspects".
ETR 055-9:	"Universal Personal Telecommunication (UPT); The service concept Part 9: Service requirements on numbering, addressing and identification".
ETR 055-10:	"Universal Personal Telecommunication (UPT); The service concept Part 10: Supplementary services".

An additional part (Part 11) which details the requirements on the protection of third parties, is due for publication in 1993.

Blank page

1 Scope

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

The complete general security architecture for UPT is given in DTR/NA-70401 [1]. A description of the man-machine interface for authentication procedures can be found in Part 8 of this ETR.

2 References

The following reference is used from within this ETR.

[1] DTR/NA-70401: "Universal Personal Telecommunication (UPT); General UPT security architechture".

3 Abbreviations

For the purposes of this ETR, the following abbreviations are used.

DTMF	Dual Tone Multi Frequency
PIN	Personal Identification Number
PUI	Personal User Identity
TAN	Transaction Number
UPT	Universal Personal Telecommunication
VAC	Variable Authentication Code

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 not, however, 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 unauthorised persons who impersonate the user;

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

- **eavesdropping**: unauthorised 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. Possible security features could include:

1) subscription data access control;

2) user action authorisation;

3) user event control;

4) user identity confidentiality;

5) user identity authentication;

6) UPT service provider authentication.

NOTE 1: The proposed security features given in this Clause are generally applicable to the long-term UPT scenario.

NOTE 2: User data confidentiality is the property that the user information carried on traffic channels during communication is not made available or disclosed to unauthorised 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 unauthorised access.

Only the UPT user, the UPT subscriber and the UPT service provider should be authorised for operations on a UPT user's service profile. Any unauthorised 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 authorisation

User action authorisation is the property that the UPT user's actions are authorised.

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

User action authorisation 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, negotiation procedures in case of unexpected charges, possibilities for advice of charge, etc.);

- protection against fraudulent outgoing calls: if the terminal where the UPT user has registered is left unattended, the UPT user may want to restrict outgoing calls from this terminal by requesting that authentication should be performed for each call set-up;

- protection against unwanted incoming calls;

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

- blocking of a UPT account 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 unauthorised 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 that UPT user's physical location by illegal means.

User identity confidentiality may imply that the UPT user should use a Personal User Identity (PUI) for self-identification to the network, which is different from the UPT 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 unauthorised 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 he has already authenticated himself during the registration procedure.

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

6.6 UPT service provider authentication

UPT service provider authentication is the property that the UPT user can verify that the UPT service entity is the one claimed.

UPT service provider authentication protects the UPT user against unauthorised and fraudulent use, as well as the UPT user's general privacy.

UPT service provider authentication may imply various actions:

1) a specific authentication procedure is defined for the purpose of UPT service provider authentication;

2) an authentication procedure is used which authenticates both UPT user and service provider simultaneously;

UPT service provider authentication may in the first case be provided in UPT as an option. In the second case, however, it will be provided automatically together with the user identity authentication.

7 Security measures and devices

Various parameters have influence on the security level offered to a UPT user. These parameters include:

- the choice and use of security mechanisms;

- the choice of security equipment for UPT access;

- the security management applied by the UPT service provider.

As a consequence of this range of options, a UPT subscriber may be offered the choice of various levels of security by a UPT service provider at subscription time.

7.1 Security mechanisms

There are many possibilities for the choice of security mechanisms that provide the UPT security features listed above. Security mechanisms especially relevant for UPT include:

- authentication mechanisms;

- access control mechanisms;

- bill limitation mechanisms.

7.1.1 Authentication mechanisms

Authentication of users to the UPT service operator is a necessary condition for the proof of responsibility of the UPT user's actions and for provable charging and billing. Authentication of the service provider to the UPT user is also desirable in order to avoid malicious parties masquerading as the service provider.

There are many possibilities for authentication. The choice depends on technical possibilities on one hand, and on the specified security policy on the other hand. Possible mechanisms range from simple authentication (e.g. PIN) up to biometrical procedures.

The more enhanced mechanisms need the use of advanced technologies like smart-cards and fast encryption chips. Especially for UPT phase 1, it is not possible to use more than an enhanced one-way mechanism. Phases 2 and 3 will allow the implementation of many-way handshake protocols, supplemented, for example, by smart-cards. Mutual authentication will not be possible in UPT phase 1.

The simplest authentication mechanism is the PIN. This PIN could be dialled manually by the UPT user or automatically generated by a simple UPT access device. For convenience, the UPT user should be able to choose and modify his password, either by administrative or automatic procedures. There are, however, some risks associated with the use of a simple PIN:

- replay of authentication data;

- guessing of (PUI, PIN) pairs;

- denial of service by intentional blocking.

These problems can be solved if Variable Authentication Codes (VACs) are used. VACs provide a mechanism similar to having automatically a different PIN value at each authentication. VACs should be verifiable by the UPT service provider, but they have to be non-predictable and non-replayable. authentication data might be time-stamps, sequence numbers or random transaction numbers. This mechanism requires the use of a UPT access device.

If it is possible to use two-way transmission at the access point, challenge and response authentication protocols can be implemented. These protocols need a UPT access device (e.g. smart-card). Authentication is done between the UPT access device and the network.

7.1.2 Access control mechanisms

Access control mechanisms include security mechanisms for subscription data confidentiality, user action authorisation and user event control.

The level of security will depend on the choices made by the UPT service provider, the options decided at subscription time by the UPT subscriber, and the actual use of UPT procedures at a given time by the UPT user.

7.1.3 Bill limitation mechanisms

Many problems and threats arise from billing and charging. Authentication, supplemented by access control mechanisms and management procedures, gives protection against these threats or at least decrease the possibility of their occurrence.

In addition to the security mechanisms mentioned above, bill limitation procedures can be used to guard the UPT subscribers from bills of unexpected amount.

7.2 Security equipment for UPT access

The security equipment used for UPT access concerns both UPT terminals and UPT access devices. Part 5 of this ETR discusses issues related to UPT terminals and UPT access devices in more detail.

UPT facilities must be accessible, both for calls and for registrations, at least from dial pulse and Dual Tone Multi Frequency (DTMF) telephones. Additional UPT access devices may be distributed by UPT service providers in order to facilitate the interactions of the UPT user with the UPT service and to increase the security level.

Some specific physical realisations of UPT access devices are discussed in this subclause. As far as possible a consistent user-interface should be provided, irrespective of the type of the UPT device. A common requirement is that the UPT user should self-authenticate to the device with a simple authentication mechanism, such as a PIN code.

7.2.1 No UPT access device

This case is not very user-friendly. It requires the input of complicated user commands from the UPT user.

There are only restricted possibilities for implementation of security mechanisms. A support by cryptological procedures will not be possible without intelligent UPT access devices. This leaves only the use of PINs as authentication mechanism, possibly supplemented by Transaction Numbers (TANs), taken from a list. Such a solution, with weak authentication, may only be acceptable for a restricted access (e.g. registration for incoming calls).

7.2.2 Magnetic strip card UPT access device

A magnetic strip card UPT access device requires a terminal equipped with a magnetic strip card reader and a signalling interface to communicate with the network. From a security point of view, it appears only as a substitute for a manual input of the PUI and a (possibly long) PIN, and thus does not provide a significant increase in the security level.

7.2.3 One-way tone type UPT access device

Such devices, as for example DTMF devices represent a well-established technique. This is an advantage compared with modems (see subclause 7.2.4). On the other hand, a DTMF device can transmit a maximum of eight numerals per second.

A UPT specific DTMF device would be user-friendly, with the possibility to store user-specific data and by the implementation of special function keys. Security can be increased by the use of enhanced one-way authentication mechanisms, such as VACs.

7.2.4 Modem type UPT access device

Modems are about 10 times faster than DTMF devices. However, without much implementation expense, they do not increment the security compared with DTMF devices. They are also less user-friendly than a smart card.

7.2.5 Smart-card type UPT access device

Smart-cards are the solution at least for UPT phase 3. They make a two-way authentication possible. Furthermore, user authentication can be combined with service provider authentication (mutual authentication). Finally, smart-cards are most user-friendly.

There could be two kinds of use of a smart-card:

- in a terminal equipped with a card reader for enhanced (two-way) features;

- in a one-way tone-type device equipped with a card reader for simple (one-way) features.

7.3 Security management

The security mechanisms have to be supplied with a security management policy. It includes the following topics:

- how to handle cryptological keys and user-related data (key management, personalisation of security devices);

- how to react in case of misuse (security audit trail, event handling);

- what information and announcements have to be transmitted to UPT users and third parties (information policy);

- how to make billing secure by off-line mechanisms (charging administration, black lists).

Security management concerns indirectly the UPT user in the relations with the UPT user's UPT service provider.

7.4 Multiple security levels

Each UPT service provider will have his own security policy, based on a standardised minimum security level and using a choice of security mechanisms, types of UPT access devices, and security management procedures. Various security levels will coexist for the UPT service. When UPT service providers with different security policies are involved, special procedures for inter-domain security are required.

The capabilities of the terminals and networks visited will also influence the security level which can be guaranteed for a UPT user in a given situation. For example, the high level of security provided by the use of a smart card is available only from a terminal with a card reader. A UPT user who has a subscription with a high level of security should not be precluded from using ordinary terminals. In such a case the UPT user could possibly have some limitation on the use of UPT features.

8 Interaction with third parties

The UPT user will use the terminal access of an ordinary subscriber and thus interact with his subscription. This issue is related to the protection of third parties.

History

Document history	
December 1992	First Edition
February 1996	Converted into Adobe Acrobat Portable Document Format (PDF)