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.

These requirements mean that there is a need for some kind of agreement by third parties in the UPT remote registration situation, and service providers need to take account of the relevant (forthcoming) national laws concerning the protection features that are required.

4.3 UPT specific security features

In the service descriptions of UPT some features are defined that serve as countermeasures to some of the identified threats. These features, as well as some frequently used precautions that are normal practice in telecommunication based services, are described here together with the more specific security features needed to fulfil the security requirements.

4.3.1 UPT service features providing security

These features alone are not always sufficient to counteract a particular threat, but they nevertheless contribute (together with other security measures) to attaining the required security level. Important security features in this category are:

- bill limitation;
- itemized bills;
- activity monitoring;
- announcements;
- blocking of registration;
- reset of registration;
- contractual agreements.

Bill limitation or credit control is the only effective way to limit the consequences of extensive, possibly unauthorized, use by the user or fraudulent use by masquerading intruders. The limit for accumulated charges should be set by the service provider in co-operation with the subscriber. In order to be effective, the control should be performed in connection with the authentication for every outgoing call (in later phases this may even be extended to in-call control). In the case of overrun of the limit, the service provider shall not allow any more calls which increase the charges. The user should be made aware of this situation immediately before the limit is reached and when making attempts for calls after the limit has been reached.

For extra protection, follow-on outgoing calls may be restricted by the service provider.

Itemized bills play an important role for some threats, which are not easily discovered or prevented otherwise. A drawback is that detection of problems is delayed until the receipt of the bill and is dependent on the bill being scrutinized in detail. Knowledge of the fact that itemized billing is used will give a deterrent effect, which may restrain people from some abuse or misuse of the service.

NOTE 1: Itemized bills can cause privacy problems (e.g. by giving information about the whereabouts of the user). Special precautions need to be taken to observe the relevant legal aspects on the protection of personal data when itemized bills are used.

Activity monitoring is the real-time monitoring of activities and events associated with a user's account or with the UPT service itself including some or all of: authentication attempts; call activities; and charging indications. The pattern of a user's activity may indicate that the user's account is subject to abuse. Activity monitoring is the only fast-acting protection against fraudulent use that the UPT service provider (and indirectly, the service providers UPT subscribers and users) have. This is necessary, particularly if weak user authentication is used.

Announcements given can play an important role for the security of the service. They need to be carefully designed to enlighten users and third parties on the different states of their connection or relation with the operator/service provider.

NOTE 2: Announcements can cause privacy problems (e.g. by giving information about the whereabouts of the UPT user). Special precautions need to be taken to observe the relevant legal aspects on the protection of personal data when announcements are chosen.

Blocking of registration can be a way for third parties to permanently avoid UPT registrations. If UPT blocking is the original default state for all line subscribers and only active unblocking from the line subscriber permits UPT registrations, then a substantial third party protection can be achieved. This could be the normal practice for remote registrations for incoming calls. The unblocking could be carried out in different ways: by written consent from the line subscriber allowing either specific UPT number registrations or all UPT registrations, or by on-line procedures. The consent could be subject to different conditions according to what is offered by the UPT service provider in this respect. The third party shall be able to withdraw any previous agreements.

Local registrations, where registration for incoming calls to a specific line terminal is made from the same terminal (e.g. determined by a calling line identification feature), should be excluded from this requirement.

NOTE 3: The detailed solution(s) for third party protection against unwanted registrations will have to await the outcome of the proposed CEC Directive SYN 288 as well as national legislation regarding call forwarding.

Reset of registration is an essential part of the UPT service. However, it does not give full protection against problems with unwanted registrations as third parties cannot, in general, be expected to be familiar with the reset procedures. In phase 1, reset can only be performed as an off line procedure via the local UPT service provider.

Contractual agreements relating to security issues shall be included in the conditions for the subscription. Security related parts of the conditions to be agreed and signed by the subscriber may include:

- to follow the rules (as declared by the UPT service provider and adjoined to the subscription contract) regarding secure handling of Personal User Identities (PUIs) and PINs for weak authentication and the corresponding rules regarding use of the advanced DTMF device;

- to report immediately to the service provider, loss of PIN or device or other conditions which may lead to fraud or misuse;

- to follow the restrictions in the use of service which may be imposed with regard to third party protection;

- to accept limitations of service with regard to agreed levels of credit control/bill limitation;

- to accept limitations of service which the service provider may subsequently find necessary to introduce to protect the UPT service as such against misuse or fraud;

- to accept liability regarding the possible fraud or misuse of the subscriber's account when the subscriber or the subscriber's users have severely broken the rules;

- to impose the corresponding instructions and restrictions on users (if different from the subscriber).

4.3.2 Authentication of UPT user/UPT subscriber

The threats concerning masquerading towards the UPT service provider are the strongest identified and authentication of the UPT user (and UPT subscriber) is the most important security feature for UPT. For this reason, only strong authentication, using an advanced DTMF device, is recommended. Weak authentication is not a sufficient solution in itself and may only be acceptable if accompanied by several other security features and limitations of the service.

A user contacting the operator or service provider in the case of operator assisted service should be authenticated, if necessary, to protect the service provider or the UPT users from abuse.

NOTE: The authentication service is used by the UPT user accessing the system in various aspects (registration, outgoing calls, service profile management, etc.) as well as by the UPT subscriber's access to service profile management.

4.3.3 Access control features for the UPT access device

A strong physical protection is required for implementing the access control to the sensitive information in the advanced DTMF access device.

Use of an advanced DTMF access device shall be controlled by authentication of the user (i.e. DHV).

4.3.4 Access control to service profile information

Users, subscribers and the service provider's staff shall have access to different parts of the service profile. For this reason there shall be an access control system. Part of the access control for users and subscribers will be the authentication described in subclause 4.3.2. Authentication of personnel and access control in the service provider's local environment should have a dedicated state of the art solution, suitable for this hardware and software environment.

4.3.5 Secure management of the subscription process

Sound and stringent procedures for administration of subscriptions, all secret information and devices as well as adequate access control systems for subscription database systems are required.

NOTE: Subscription may (partly) be handled via telecommunication means if there are adequate security measures (authentication, access control). It is more likely that the subscription will be manual (personal presence, mail) with the corresponding security measures taken for this environment.

This service should be designed to cover threats like the following:

- unauthorized modification of subscription data by user or subscriber;
- unauthorized de-subscription;
- denial of service by device malfunction;
- mis-delivery of UPT devices.

The security features to attain the required level of security management may vary substantially depending on the different environments to be found with service providers and should not be standardized. Therefore, these requirements and the solutions to them are not discussed further in this ETS.

4.4 UPT security limitations

Only a few threats identified have not been covered by relevant security features so far, they are all commented upon in this subclause. Some of these threats are considered to be of less importance either because of low likelihood, or because they have only minor consequences, often both. For other threats, no feasible (cost justified) way to protect against them has been identified.

Threats not covered include all those concerned with eavesdropping or active manipulation of the lines used for UPT registrations. The eavesdropping threats have high vulnerability especially if authentication data is recorded. There is, however, a substantial difference in risk if weak authentication is used instead of the recommended strong authentication. This is especially true if the registration data passes over the air (e.g. in a Public Land Mobile Network (PLMN) access) or if it passes some equipment that has inherent recording facilities (e.g. some Private Automatic Branch Exchanges (PABXs)). This is one reason to limit the service of UPT when weak authentication is used.

Protection against nuisance registrations to terminals of unknowing or unwilling third parties also do not yet have a definite solution. The recommended indications, special dial tones, etc. are not sufficient. Reset of registrations is not generally available in phase 1. Default blocking conditions and active agreement through pre-registration or on-line agreements are possible, but have not yet been sufficiently evaluated. It is felt that the best recommendation which can be given at present is for every service provider to closely watch and follow the requirements of national and European legal entities.

4.5 Security features for IN and inter-network links in general

The requirements for the safe and trusted relation between all the different IN entities, inter and intra-network, has intentionally been left out of the scope of this ETS. This is not because of the lack of importance, but because the security architecture on this level should be standardized on a generic basis, not as a UPT specific solution.

5 Security mechanisms

This clause describes how the security requirements and the security features stated in clause 4 can be accomplished by security mechanisms. It comprises mechanisms for access control and authentication, as well as some aspects of the security management (audit trail, event handling, charging control, information management). Finally, based on specific service limitations, the concept of security profiles for weak and strong authentication is introduced.

5.1 Access control mechanisms

Access control mechanisms shall be used in the following three fields:

- access to the service based on the user's or subscriber's PUI;

- access to the service profile and other management data by users, subscribers, authorized personnel of the service providers, and by inquiries from home or visited network nodes;

- access to the data in the UPT access device.

5.1.1 Access control to services

Access control to the UPT service or to certain service functions can be seen as a combined process with identification and authentication of the involved parties. The process flow of the combined process is described in subclause 5.2. Access control shall be supported by security management procedures as described in subclause 5.3.

Mechanisms for access control to services shall make use of the following authorization lists:

- whitelists;

- blacklists.

Whitelists are access control lists or capability lists, which specify the services that the individual UPT users and subscribers are allowed to use. They may be realized as part of the corresponding service profile data (see subclause 5.1.2).

Blacklists specify those identities (PUIs) that shall not be accepted to get access to the UPT service, e.g. because the UPT user has exceeded the credit limit. Blacklists shall be updated as often as necessary. They shall be realized in the Authenticating Entity (AE) associated with the SDF.

The UPT service provider may define hot lists, too, for those identities where additional measures should take place, e.g. if detailed activity monitoring should be activated (see annex E).

A PUI is blocked if the access is temporarily denied because of too many consecutive wrong authentication attempts. Blocking shall be realized in the AE. An unblocking procedure is described in subclause 5.2.1.

A PUI is named "invalid" if no corresponding service profile data exists.

In UPT phase 1, the check of the service profile data for authorization will always be carried out at the home location of the UPT user. Therefore, no data related to access control needs to be submitted through the network.

All authorization lists shall be installed in a protected environment.

5.1.2 Access control to service profile data

The access to service profile data should be restricted to the following subjects with different access rights:

- UPT user;

- UPT subscriber;

- UPT service provider.

The information stored in the service profile can be subdivided into fixed information and variable information from the UPT user's point of view. The fixed information is typically fixed at subscription time and can be changed only by the UPT service provider, possibly on request of the UPT subscriber. The variable information can be changed by the UPT user or the UPT user's UPT subscriber, explicitly by using UPT service profile management functions or implicitly by using UPT personal mobility functions.

Table 1 shows examples of the different parts of the UPT service profiles, which are essentially taken from ETR 055-6.

Table 1: Parts of the UPT service profiles

A Information set by the service provider at subscription time:

- UPT number;
- PUI;
- default home location of the UPT user;
- bearer services subscribed to (only ISDN);
- teleservices subscribed to (only ISDN);
- UPT supplementary services subscribed to;
- maximum number of failed authentication attempts, before disabling the UPT service profile access;
- types of authentication procedures subscribed to (weak or strong authentication);
- not allowed Access Registration Addresses (ARAs) for incoming calls.

B Information changeable by the UPT subscriber:

- maximum allowed credit for the user (individual threshold of credit);
- maximum number of terminal accesses for remote registration;
- allowed procedures for the UPT user;
- type of authentication procedure allowed (weak or strong authentication).

C Information changeable by the UPT user:

C1 Service related information:

- activation status for each UPT supplementary service;

C2 Mobility related information modified by UPT service profile management procedures only:

- default terminal accesses for incoming calls;
- list of terminal accesses for remote registration;
- default duration (or number of calls) for registration for incoming calls;
- information related to UPT supplementary services;

C3 Mobility related information modified by UPT personal mobility procedures only:

- current terminal access for incoming calls.

NOTE: According to the requirements made in subclause 5.5, the used type of authentication (weak or strong authentication) shall influence the other information in the service profile.

Access control shall be ensured for the relations between the subjects (i.e. the UPT user, the UPT user's subscriber, and the UPT service provider) and the objects (i.e. the parts of the service profile) as stated in table 2. However, there may be agreements between the involved parties allowing other access conditions.

Table 2: Access control to service profiles

Access type objects	Read	Write
A	all (note 1)	provider
B	all (note 1)	provider (note 2), subscriber (note 3)
C1	all (note 1)	provider (note 2), subscriber (note 3), user (note 3)
C2	all (note 1)	provider (note 2), subscriber (note 3), user (note 3)
C3	all (note 1)	user (note 4)

NOTE 1: i.e. the UPT user, the UPT user's subscriber, and the UPT service provider; restrictions may be necessary to protect personal data.
NOTE 2: According to agreements between the UPT subscriber and the UPT service provider.
NOTE 3: By service profile modification procedures.
NOTE 4: By personal mobility procedures.

It is stated in ETR 055-6 that UPT service providers have access to all the service profile information without any restrictions. However, the service providers should restrict their access to the service profile in accordance to European and national (data protection) laws. Furthermore, they should specify the information to be stored in the service profile and its use in the contracts with the UPT subscribers. After termination of a subscription the data shall be deleted unless, and only as long as, they are required to deal with complaints, to recover charges, or for legal obligations.

The UPT service provider is responsible that only authorized personnel have access to the data. The specification of the mechanisms is in the responsibility of the UPT service provider and need not be standardized. The signalling access (e.g. by signalling system No. 7) shall be protected by authentication of the network nodes and authorization lists containing service providers with roaming contracts, according to contracts between the service providers.

5.1.3 Access control to the data in the UPT access device

The access control requirements to the sensitive data stored in the advanced DTMF device are specified in clause 7. The access control mechanism shall use a strong physical protection against reading.

The access control mechanisms for the use of the advanced DTMF device should be supported by a DHV (see annex A).

5.2 User authentication mechanisms

Authentication is used in the following three situations:

- authentication of the user to the UPT service provider;

- authentication of the subscriber to the UPT service provider;

- authentication of the user to the UPT access device (see annex A).

For authentication of a UPT user to the UPT service provider, weak authentication and strong authentication mechanisms are distinguished. The term "strong authentication" is used for mechanisms using variable authentication data, which changes in each authentication attempt and thus avoids replay attacks, whereas the term "weak authentication" is used for mechanisms where the transmitted authentication code, calculated in the UPT Access Device (AC) is always the same.

To avoid replay and other attacks, strong authentication using an advanced DTMF device is recommended.

The first steps in the authentication mechanisms are common for both weak and strong authentication. An AE, associated with the SDF, shall perform the authentication mechanism. The first steps are:

a) the AE receives authentication data from the user (or the device);

b) the AE checks the received PUI. If it is invalid or blacklisted the authentication has failed;

c) the AE selects and performs weak or strong authentication depending on either the type of authentication associated with the PUI, or the format of the authentication data received;

d) if the authentication has succeeded the user can use services according to the user's service profile, otherwise authentication failure is presented to the user.

The steps above are described in figure 1.

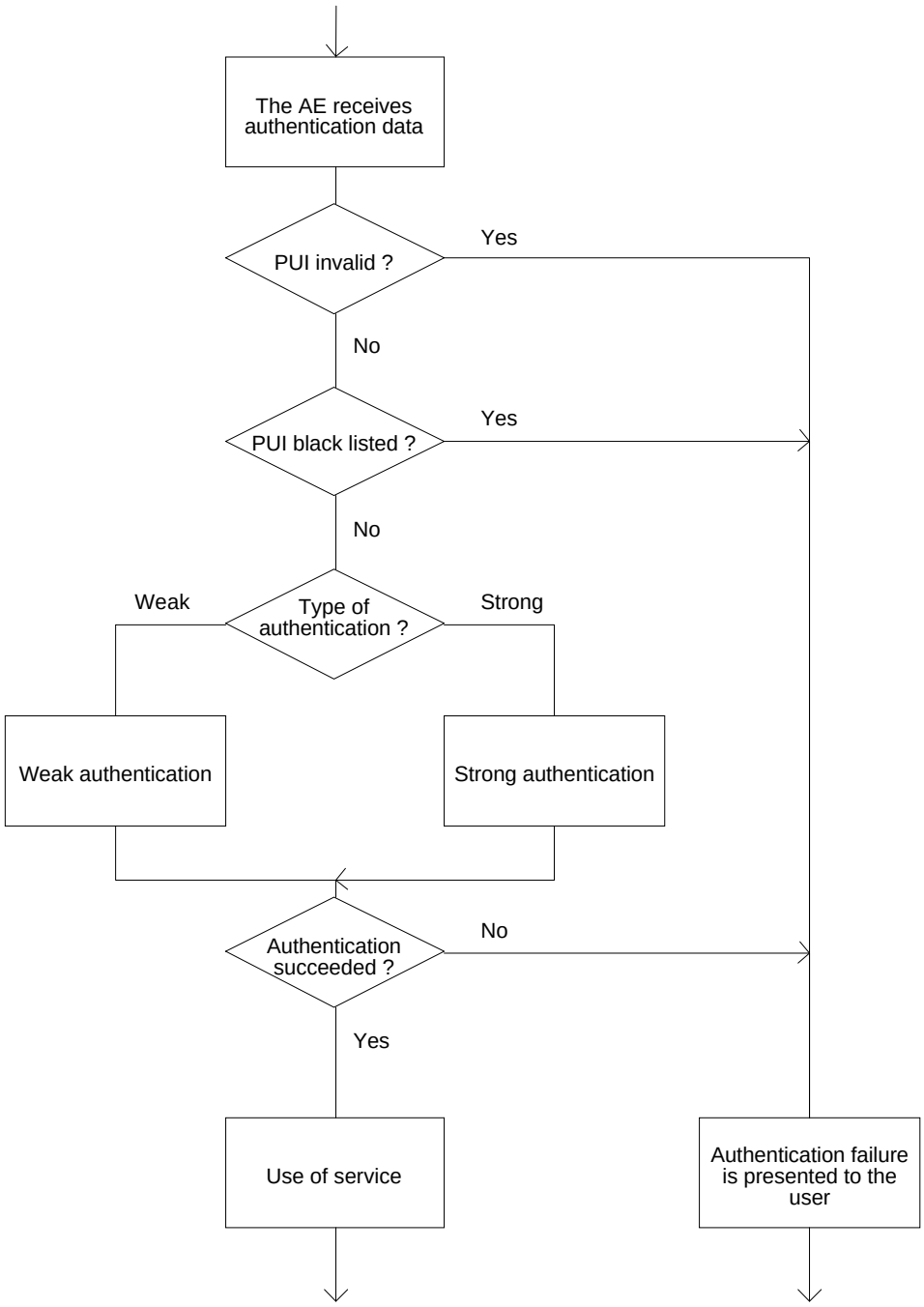

Figure 1: Overview of the authentication mechanisms

5.2.1 Weak authentication

No special access device is necessary for the authentication (from the security point of view), when weak authentication is used.

The relevant data required for weak authentication is as follows:

PUI: the PUI, not the UPT number, shall be used to recognize the UPT user;

PIN: the UPT user's secret PIN, known by the user and the AE only;

RAA: Remaining Authentication Attempts, a counter value used to keep track of remaining PIN entry attempts;

SPIN: Special Personal Identification Number, used for unblocking in case the PUI has been blocked.

Measures have to be taken to limit the possibility for unauthorized persons to guess and use PINs corresponding to certain UPT Numbers (UPTNs) and PUIs:

- knowledge of a PUI or a UPTN shall not make it easier to guess a PIN;
- a minimum length of the PIN is required, to make it difficult to guess and avoid exhaustive search;
- it should be possible for the user to change the PIN on-line, see clause 9;
- the PUI is blocked after a number of consecutive wrong PIN presentations;
- the PUI shall not be publicly known;
- it should be difficult to guess a valid PUI, e.g. by using only a small number of possible non-consecutive PUI values;
- there shall be no obvious correlation between PUI and UPTN;
- the number of consecutive unsuccessful UPT attempts within a single call attempt shall be limited by the visited network.

Blocking of a PUI may occur for the following reasons:

- the UPT user has forgotten the PIN, and made too many attempts with wrong PIN;
- some unauthorized person has made too many false guesses of the PIN;
- some unauthorized person has intentionally blocked the PUI, by presenting wrong PINs several times.

A procedure to unblock a PUI is required. This can be done either on-line or off-line. The on-line unblocking procedure described here is optional.

To avoid exhaustive search of the SPIN, it shall, optionally, be possible to limit the number of unblocking attempts.

The authentication mechanism can be used for both authentication and unblocking, depending on whether or not the PUI is blocked. The user is expected to give the PIN in a normal authentication attempt or the SPIN in an unblocking attempt. The mechanism is performed as follows:

1) the user has presented the PUI and either the PIN or SPIN to the AE, using a DTMF telephone's normal key pad or a simple DTMF device (see clause 7 for definition of simple DTMF device);

2) if the PUI is not blocked, the AE compares the received PIN with the stored PIN. If they are equal, the authentication has succeeded and the RAA counter is set to its initial value. If the PINs are not equal, the authentication has failed and the RAA counter is decremented. If it reaches 0, the PUI is blocked;

3) if the PUI is blocked, the AE compares the received SPIN with the stored SPIN. If they are equal, the authentication has succeeded, the PUI is unblocked and the RAA counter is set to its initial value. If they are not equal, the authentication has failed and the PUI remains blocked;

4) optionally, after the unblocking, the user may be asked if a change to the PIN is wanted. If the user responds that a new PIN is wanted, then the user shall be requested to give the new PIN twice. The new PIN shall be used the next time the AE requires a PIN.

The steps above are described in figure 2. For a detailed description, see clauses 6 to 9.

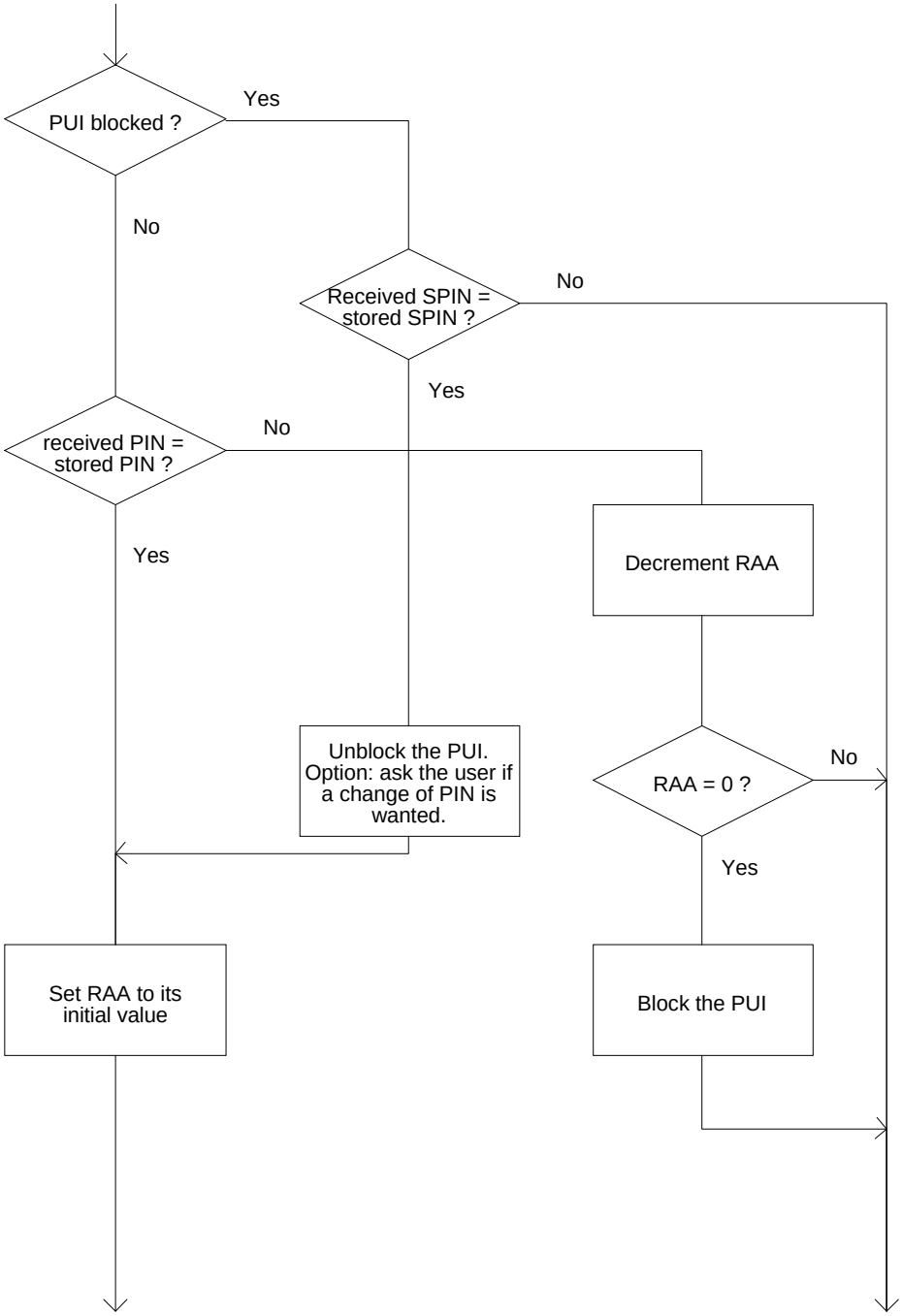

Figure 2: The weak authentication mechanism

5.2.2 Strong authentication

The access to the UPT service is established by the use of a UPT access device. The authentication process can be split up into two parts: the authentication of the user to the device and the authentication of the device to the UPT service provider. For the authentication of the user to the user's device, an example is given in annex A. The authentication to the UPT service provider is done by the device.

The relevant data required for authentication is as follows:

AC: the variable authentication code, calculated in the UPT device;

AC': the variable authentication code calculated in the AE;

f: the algorithm for the calculation of the AC. f shall be a one-way function. The algorithm is used both in the device and in the AE;

K: the individual secret authentication key, stored both in the device and the AE, see annex D;

n: the individual sequence number, generated by the UPT access device and incremented after each authentication attempt. It is used as an input to the authentication algorithm f, to guarantee variation of the authentication code AC;

n_S: the least significant bits of n, which are transmitted from the device to the AE;

n': the next expected sequence number stored in the AE;

PUI: the personal user identity is stored in the UPT access device.

The authentication mechanism is performed as follows:

a) the device has calculated the AC, using n, K and f, incremented its stored n and then sent the PUI, n_S and AC to the AE;

b) the AE checks if n_S is within the acceptable range, by comparing n_S and the least significant bits of n'. If n_S is not accepted, the authentication has failed;

c) the AE expands n_S to n;

d) the AE calculates AC', using n, K and f;

e) the AE compares AC' with the received AC. If they are equal the authentication was successful and the AE replaces n' by n + 1. If they are not equal the authentication has failed.

The steps above are described in figure 3. For a detailed description, see clauses 6 to 9.

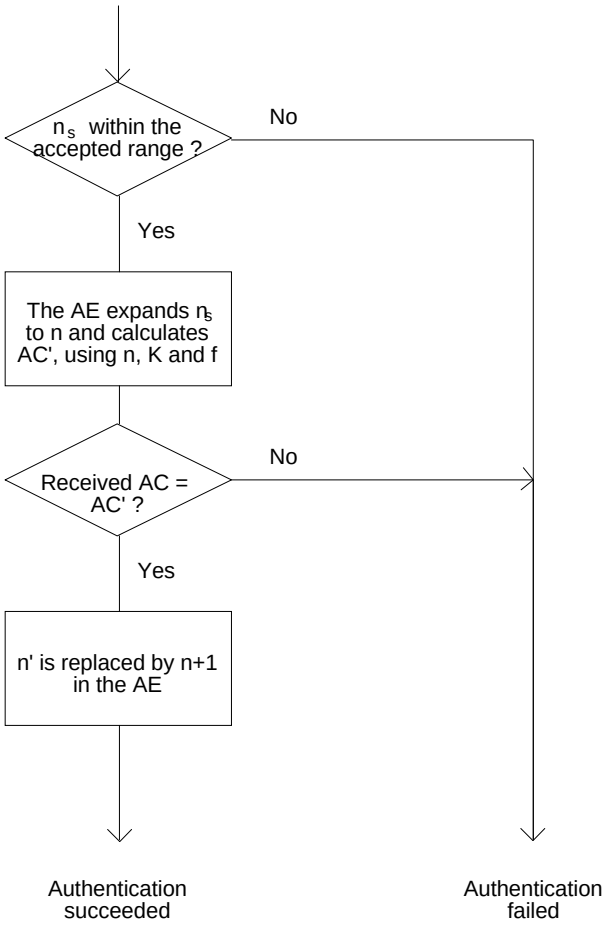

Figure 3: The strong authentication mechanism

5.3 Security management

In order to detect threats against any parties involved with the UPT system as early as possible and to take suitable measures, security audit trails and event handling shall support the above mentioned security mechanisms. Charging control is a measure to limit potential harms to an acceptable amount. Information management gives the user the possibility to be aware of security relevant events.

This subclause specifies the requirements for these aspects of the security management. Additional information regarding bill limitation, subscription process and key management, and activity monitoring is given in annexes C, D and E, respectively.

5.3.1 Security audit trail

The task of security audit trail is to detect actual threats against the UPT system, e.g. unauthorized access to system or user data and unauthorized change of access rights.

The system should contain audit components that are able to log the events with the data, see table 3.

Table 3: Security audit events and data

Event	Data
Use of the identification and authentication mechanism:	- date, time; - user identity; - calling line identity or originating area code; - number dialled; - success or failure of the attempt; - number of synchronization updates.
attempted access to the service profile:	- date, time; - user identity; - name of the object; - type of access attempt; - success or failure of the attempt.

actions by UPT service providers and network operators:	- date, time;
	- user identity;
	- type of action;
	- name of the object to which the action relates, examples are:
	  - introduction;
	  - deletion or suspension of users;
	  - introduction or removal of storage media;
	  - start up or shut down of the system.

It should be possible to restrict the audit to selected parties.

Access to audit data shall only be permitted to authorized persons in accordance with privacy laws. Personal data shall only be stored as long as needed for the investigation of criminal attacks or until the time limit for contesting the bill has been reached. It shall not be possible to use audit data for irregular purposes (see CEC Directive SYN 288).

Tools to examine and to maintain the audit files shall be documented, and the structure of audit records shall be described completely. The mechanisms to obtain, maintain and evaluate an audit trail are out of the scope of UPT. These mechanisms are system specific and may be supported by TMN security mechanisms.

5.3.2 Event handling

Dependent on the evaluation of audit data (on-line or off-line), adequate actions shall be performed in order to enforce the security policy. These actions may include:

- alarms to the security administrator;

- blocking of user access to the system;

- interruption of calls (especially excessively long international calls).

The mechanisms for event handling are out of the scope of UPT. These mechanisms are system specific and may be supported by TMN security mechanisms.

5.3.3 Charging control

The charging administration has to consider security very carefully. Personal data and billing data shall be stored, processed, and transmitted in such a way that user privacy and data integrity are guaranteed.

The following two possibilities to transfer charging data between originating network and home service provider may be considered:

- off-line transfer;

- on-line transfer.

If on-line transfer is used, a separate message is transferred in real time, for each call from the Service Control Function (SCF) to the home SDF.

If off-line transfer is used, the charging information is normally transferred with some delay from the SCF to the home SDF. In this case, credit limits may be considerably exceeded since the home SDF does not always have the latest information.

In order to be able to provide checking of credit limits, charging calculations should be made in real time. At the end of the call, the cost information for that call shall be calculated and sent to the home UPT service provider of the UPT user to be charged for outgoing or incoming (split charging) UPT calls. If the credit limit is exceeded, the corresponding PUI should be blacklisted.

In order to make it possible to check the correctness of billing data, the use of detailed Call Event Records (CERs) is preferable. In this case, each charging record held in the system may contain, in addition to the general data (i.e. destination, origin, chargeable time, date and time of the call) the sequence number of the variable Authentication Code (AC) (if used for authentication, see subclause 5.2.2), which would help to identify doubtful charging records by comparing the sequence numbers.

Itemized bills are a means for the UPT subscriber to view the use of the account and hence to notice fraudulent use. However, to avoid conflicts with privacy requirements, the subscriber should also have the possibility to receive only summarized bills.

The threat analysis has shown that many problems and threats relate to charging and billing. Authentication, supplemented by access control mechanisms and management procedures, can prevent these threats, or at least decrease the possibility of their occurrence.

However, particularly for acceptability purposes, it appears to be necessary to preserve the users from bills of unexpected amounts. Bill limitation is indispensable if only weak authentication is used. Possible mechanisms to realize this requirement are discussed in annex C.

5.3.4 Information management

There should be a facility to inform UPT users, UPT subscribers and other parties about actions that affect their privacy and security or the charging. As far as possible, this information should be given on-line by announcements (speech or display) or by special dial tones. It is up to the service provider to specify the information that is given to the involved parties. This does not need to be standardized. Therefore, the following points are only examples.

The following information may be given to calling parties:

- "EXTRA CHARGING"
  (if the called party is roaming and no charging split is arranged).

The following information may be given to the users of a line subscription:

- "UPT REGISTRATIONS FOR THIS TELEPHONE"
  (the line subscriber should always be aware of UPT registrations on his terminal).

If required, the following information may be given to UPT users after successful authentication:

- "SERVICE LIMITATION";

- "BLOCKING OF REGISTRATION BY LINE SUBSCRIBER";

- "BILL AMOUNT CLOSE TO LIMIT";

- "BILL LIMITATION EXCEEDED";

- "REGISTRATIONS ON OTHER TERMINALS".

The UPT service providers shall be careful not to give too much information. Potential intruders should not be able to misuse such information for their attacks.

Furthermore, information and announcements should not affect the privacy of UPT users and other parties, e.g. a calling user shall not be given information about the location of the called UPT user.

5.4 Service limitations

If weak authentication is used by service providers, the UPT services available to a user shall be restricted. Access to services which entail high risk to any participant in UPT should not be allowed with only weak authentication. It is the decision of the UPT service provider, whether or not to distinguish strictly between UPT subscriptions with weak authentication and service limitations and UPT subscriptions with strong authentication, or the UPT service provider can specify in the service profile, for example, what kind of authentication has to precede the individual services.

Limiting the service offered to users reduces vulnerability to fraud.

The UPT service provider shall specify the service profile data, the services and restrictions dependent on the authentication type.

Examples of possible restrictions for each UPT service feature if weak authentication is used are given in table 4.

These restrictions may of course, to varying degrees be implemented even if strong authentication is used.

It shall not be possible to bypass the restrictions by using operator assisted services.

In the situation of interworking between networks it shall not be possible for a user to bypass service limitations specified in the home network.

It should be possible for the service provider to prevent the use of weak authentication from analogue mobile networks.

Table 4: Service limitations

Feature class	Feature	Possible restrictions
Core features	Local incall registration	Predefined set of ARAs allowed for incall registrations. Predefined area from which registrations are allowed.
	Remote incall registration	Predefined set of ARAs allowed for remote incall registrations. Predefined set of NAPs or area from which registrations are allowed.
	Direct outgoing UPT call	Predefined set of NAPs from which outgoing calls are allowed. Predefined set of NAPs to which outgoing calls are allowed. Only national calls allowed. Only local calls allowed.
	UPT service profile interrogation	Limited set of data. Predefined set of NAPs from which interrogation is allowed.
	UPT service profile modification	Limited set of data. Predefined set of NAPs from which modification is allowed.
	Global follow-on	Predefined set of services. Area from which it may be performed.
	Outcall follow-on	Only national calls allowed. Only local calls allowed. Number of follow-on calls allowed (even to zero). Area from which it may be performed.
Additional features	Access to groups of service profiles	Limited set of data. Predefined set of NAPs for access.
Supplementary features	Call forwarding	Same restrictions as remote incall registration.
	Variable routing	Same restrictions as remote incall registration.
General aspects	Charging	Absolute bill limitation. Bill limitation with respect to time.
	Roaming	Limited set of networks allowed for roaming.

5.5 Security profiles

A chosen set of service limitations and security measures defines a security profile. The service provider shall specify one security profile for each type of authentication used.

Two security profiles fulfilling minimum security requirements are specified in subclauses 5.5.1 and 5.5.2.

A service provider may also specify other security profiles, if they keep at least the same level of security.

The security profile shall be taken into account when the service profile is set. However, also other parts of the UPT system are involved by the chosen security profile.

5.5.1 Security profile for weak authentication

The security profile for weak authentication shall include at least the following security features and measures:

- activity monitoring (especially the authentication attempts should be monitored);
- charging control;
- hard to guess PUI (see subclause 5.2.1);
- security instructions to the user/subscriber (e.g. PIN handling);
- contractual liability of the subscriber (see subclause 4.3.1);
- blocking/blacklisting of PUI;

- the possibility to have itemized bills.

The following service limitations shall be implemented:

- predefined set of ARAs allowed for remote incall registrations;
- predefined set of NAPs from which interrogation of the service profile is allowed;
- predefined set of NAPs from which modification of the service profile is allowed;
- restricted number of follow-on outcalls allowed;
- predefined set of NAPs for access to groups of service profiles;
- bill limitation.

Furthermore, the UPT service provider shall be prepared to use all the restrictions described in table 4. As a result of activity monitoring and experienced fraud and misuse of the UPT service the service provider shall activate the needed service limitations.

5.5.2 Security profile for strong authentication

The security profile for strong authentication shall at least include the following security features and measures:

- activity monitoring;
- security instructions to the user/subscriber (e.g. device handling);
- contractual liability of the subscriber (see subclause 4.3.1);
- blacklisting the PUI;
- possibility to have itemized bills.

The following service limitations are required:

- predefined set of ARAs allowed for remote incall registrations;
- bill limitation.

6 Parameter sizes and values

Table 5 defines the sizes of all parameters that are used in the next clauses. In some cases, the parameter size need not be standardized and hence only a recommendation is given.

Table 5

Parameter	Length (note 1) (bits)	Length (note 1) (digits)	Remarks
AC	32	10 (note 2)	$0 \leq AC \leq 2^{32} - 1$ ($2^{32} - 1 = 4294967295$).
d			Recommended value: $d = 2^8 = 256$.
K	128		
LPIN		≥ 4	Optional parameter, see annexes A and B.
n	64		
n_s	16	5 (note 2)	$0 \leq n_s \leq 2^{16} - 1$ ($2^{16} - 1 = 65535$).
PIN		$\geq 6, \leq 10$	
PUI		≤ 16	
RAA			Recommended value: RAA = 3.
SLPIN		≥ 8	Optional parameter, see annexes A and B.
SPIN		$\geq 8, \leq 12$	Optional parameter.
	LPIN: Local Personal Identification Number SLPIN: Special Local Personal Identification Number		
NOTE 1: The lengths in bits or digits, respectively, are specified only if relevant. NOTE 2: Used for transmission via DTMF (leading zeros need not be transmitted).			

7 Requirements for the UPT access device

A UPT access device is used as an aid for the user when authenticating to the SDF. It is possible to use different types of hand-held devices:

- the simple DTMF device is used to send DTMF signals to the microphone of a telephone. It is necessary if the telephone does not have DTMF signalling. The device need not be personalized and cannot be used for strong authentication;

- the advanced DTMF device has, in addition to DTMF signalling, an internal SM, where data can be protected and the authentication algorithm can be performed. Strong authentication is used with this type of device;

- the card reading DTMF device is an advanced DTMF device with a microprocessor card as the SM. The card may be inserted temporarily in a slot or permanently installed in the device. Strong authentication is used also with this type of device.

The requirements specified in this clause are valid for the advanced DTMF device and the IC card reading device only. No security requirements have been specified for the simple DTMF device. It is regarded as a useful tool to simplify the access to the SDF (the requirements for DTMF signalling and the functional requirements for DTMF devices are given in ETS 300 380 [2]).

DHV is required for the device. The method used, however, is out of the scope of this standard. An example of a method for DHV is given in annex A. In the example a LPIN is used.

The SM interface is not considered here, see annex B.

NOTE: As a special case the device itself can be a SM.

7.1 Storage of data

The device shall at least contain the following data:

- PUI;

- n;

- K;

- the program code for the authentication algorithm f; and

- the data needed for DHV.

At least K and the program code for the authentication algorithm shall be stored in the SM, and it shall never be possible to read them out.

It shall not be possible to read out the PUI or n or to perform a strong authentication before a successful DHV has been performed.

It shall not be possible for the user to write a PUI, n or K into the device.

7.2 Processing

Processing means the usage of data inside the device. One may distinguish between two purposes: either for internal use or as preparation for transmission. The intermediate results in the authentication algorithm are security relevant and, therefore, shall not leave the SM.

For transmission through the network, both n and AC have to be converted into decimal digits inside the device.

At least the following processes shall be carried out in the device:

- incrementation of n;
- conversion of AC and n;
- time-out after DHV;
- key handling;
- calculations by the authentication algorithm;
- DHV.

The last 3 processes shall be carried out in the SM.

For strong authentication the following steps are performed by the device:

1) the user is authenticated to the device, whereby a timer starts;
2) if the DHV was successful and the time-out has not been reached, the user can activate the authentication process;
3) the SM performs the authentication calculation, using the authentication algorithm f as function, the sequence number n and the key K as input. The authentication code AC is the output from this process;
4) the device converts AC and n_S, the least significant part of n, to decimal digits;
5) the stored n is incremented by 1;
6) the device sends the PUI, n_S, and AC to the AE, as DTMF signals.

NOTE 1: Only one AC is produced. If production of another AC is requested, the procedure needs to be repeated from step 2), unless the time-out for the validity of the LPIN has been reached, in which case the procedure needs to be repeated from step 1).

NOTE 2: The user should be informed at subscription time to activate the AC procedure only in combination with a UPT access trial. Otherwise, n may run out of the allowed range d.

7.2.1 Time-out

Directly after the DHV, a timer shall start. The recommended value for the time-out is 1 minute. The authentication procedure can be repeated if needed, e.g. in case of authentication failure, until the time-out is reached. If the time-out is reached, a new DHV needs to be performed, in order to make a new attempt possible.

7.2.2 Calculations by the authentication algorithm

In each authentication attempt AC = f(K,n) needs to be calculated using the individual authentication key K and the stored n. The calculation shall be carried out by the SM.

7.2.3 Sequence number conversion

The stored n is a binary number with a length of 64 bits. Before transmission, the 16 least significant bits of n, denoted n_s, are converted to decimal digits in the following way:

The bits of n = n_{15}, n_{14}, ..., n_1, n_0 are considered as the binary representation of the integer:

$\sum_{i=0}^{15} n_i \ 2^i$,where n_0 is the least significant bit.

The decimal representation of the digits of the resulting integer shall be used for transmission.

7.2.4 Authentication code conversion

The AC is an integer with a length of 32 bits in its binary representation. Before transmission it shall be converted to decimal digits in the following way:

The bits of AC=a_{31}, a_{30}, ..., a_1, a_0 are considered as the binary representation of the integer:

$\sum_{i=0}^{31} a_i \ 2^i$, where a_0 is the least significant bit.

The decimal representation of the integer shall be used for transmission.

7.2.5 Sequence number incrementation

After each time the AC has been calculated, n needs to be incremented by 1 and stored. The storage of this value shall be independent of the power supply of the device.

7.3 User interface

The user interface shall at least make it possible for the user to:

- authenticate to the device (DHV);
- activate the authentication process;
- change LPIN (optional method, see annex A);
- unblock the device with the SLPIN (optional method, see annex A).

NOTE: To make it easier for the user to remember the LPIN, a key pad with mnemonics can be helpful. This may, in many cases, avoid the situation where users write the PIN down and decrease the level of security established by the LPIN procedure.

8 Transmission protocol

This clause defines the protocol elements to be used for authentication and PIN-handling actions from the user (or subscriber) to the UPT system.

Protocols are different for weak and strong authentication because of the specific implementation possibilities when the advanced DTMF device is used. The protocol used for strong authentication should preferably be applicable also for later phases, whereas the weak authentication will not be used in later phases.

It is to be noted that the user may be guided by tones and voice announcements during the transmission of the protocol elements. Sequences as described hereafter may be sent piecewise with interruptions for these guiding announcements. However, the user shall not normally be obliged to wait for these instructions, they may be overridden by the next input from the user or the user's device.

8.1 Transmission coding

Transmission of data from the user to the system shall use DTMF signalling in phase 1. The description of the protocol structure and the protocol elements makes use only of decimal values (0 to 9), the star (*) and the square (#). These shall be sent as DTMF signals in an asynchronous fashion. When conversion from binary information to decimal or vice versa is needed it is described in clauses 7 and 9 respectively.

The star is used as field separator, the square as finalizing indicator.

Transmission of the (sequence of) protocol elements is from left to right. The convention is that the leftmost part of the protocol elements is the most significant.

NOTE: If a user wants to wait for the next announcement after input of a protocol element, then the field separator star (*) cannot be used. After input of each data field, the user may either wait for the time-out given by the system, or enter the square (#).

8.2 Weak authentication

8.2.1 The authentication process

For weak authentication the following information shall be sent by the user.

PUI	*	PIN	#

8.2.2 Changing of PIN

Changing of PIN according to the following procedure can only take place after a successful authentication has been accomplished.

For changing of PIN the following information shall be sent by the user.

FC	*	New PIN	*	New PIN	#

FC signifies Feature Code; definition of its value is outside the scope of this ETS.

8.2.3 Authentication with unblocking

Unblocking can only take place when the user's PUI is blocked by the system because of too many consecutive unsuccessful PIN entries. For unblocking and simultaneous authentication the following information shall be sent by the user.

PUI	*	*	SPIN	#

NOTE 1: Even if the user waits for guiding announcements, the user will send one star (*) together with the SPIN. This preceding star (*) indicates that an SPIN is following instead of the normal PIN.

NOTE 2: If the PUI was already given in the same UPT attempt, repetition of the PUI is optional, it is sufficient to send only the following: * SPIN #

It is recommended that the service provider then instructs the user to change the PIN. This shall be performed as described in subclause 8.2.2.

8.3 Strong authentication

8.3.1 General structure

The following general protocol structure is used for all transmissions from the advanced DTMF devices to the system.

*	PUI	*	CT	*	DF1	*	DF2	#

CT signifies Command Type. This field is used for distinguishing between different types of commands and authentication types (in phase 1, mainly to separate between different algorithms if more than one is used).

DF signifies data fields.

All fields allow variable length of the information in them.

Additional fields of user data may be appended to an authentication transmission as defined above by inserting user fields (star separated) before the final square (#) separator.

8.3.2 The authentication process

For strong authentication the following information is sent by the user via the user's device.

*	PUI	*	CT	*	n_s	*	AC	#

CT = 1 signifies phase 1 authentication using the specific UPT algorithm.

CT = 2 signifies phase 1 authentication using the TE 9 algorithm TESA 7.

CT = 3 (and all CT starting with 3) signify phase 1 authentication according to the service provider's own specifications.

NOTE: Other values of CT are reserved for future use.

9 Requirements for the AE of the SDF

From the security point of view, the main function of the SDF is to authorize and authenticate the user by a weak or strong authentication procedure. The SDF needs to make use of a physical entity, called the AE, which shall be protected against analysing or changing of its content. The AE may support weak authentication, strong authentication, or both weak and strong authentication.

9.1 Check of PUI and authentication type used

The AE shall check whether the PUI is invalid or blacklisted before the authentication procedure. If the PUI is invalid or blacklisted, then the authentication shall be refused. Authentication failure shall be presented to the user.

The AE shall check which kind of authentication is used by analysing the type of data received or by consulting the service profile.

9.2 Weak authentication

The AE contains the following data for all users and subscribers authenticated by the weak authentication procedure:

- PUI;
- PIN;
- SPIN (optional);
- RAA;
- SPIN counter (optional).

The overall description of the weak authentication procedure is given in subclause 5.2.1. The AE shall be able to perform the following procedures:

- check of PIN (see subclause 5.2.1);
- blocking/unblocking (see subclause 5.2.1);
- change of PIN.

9.3 Change of PIN

After a successful authentication, the user should be allowed to change the PIN. This change is carried out according to the following steps:

1) the AE receives a new PIN twice;

2) the AE checks if the two new PINs are equal. If this is the case, the old PIN is replaced by this new PIN. If the two new PINs are not equal, then the change shall be refused. The result shall be presented to the user.

9.4 Strong authentication

The AE contains the authentication algorithm and the following data for all users and subscribers authenticated by strong authentication procedure:

- PUI;
- n';
- K (or a master key from which the authentication keys are derived).

The overall description of the strong authentication procedure is given in subclause 5.2.2.

The conversion of n_S and AC and the checking and expanding of n_S are described below.

9.4.1 Conversions

The number n_S is received in its decimal representation. It shall be converted to its binary representation in the following way:

- the AE computes the binary representation of the integer n_s:

  $n_s = \sum_{i=0}^{15} n_i \, 2^i$, where n_0 has the least significance and n_{15} the most significance.

The variable authentication code AC is received in its decimal representation. It shall be converted to its binary representation in the following way:

- the AE computes the binary representation of the integer AC:

  $AC = \sum_{i=0}^{31} a_i \, 2^i$, where a_0 has the least significance and a_{31} the most significance.

9.4.2 Checking and expanding of n_s

The AE shall compute $X = n_s - n'_s$ where n'_s is the 16 least significant bits of n'.

If $0 \leq X \leq d$, then the AE shall compute $n = n' + X$.

If $X \leq d - 2^{16}$, then the AE shall compute $n = n' + 2^{16} + X$.

In any other case, n_s shall not be accepted and the authentication shall fail.

10 Authentication algorithms

For the strong authentication in UPT, an authentication algorithm is used in the service provider's AE and in the advanced DTMF devices.

According to this ETS, freedom is given to service providers in the choice of the algorithm.

10.1 The specific UPT algorithm

A dedicated authentication algorithm will be available for UPT service providers and device manufacturers as one option. This is the recommended choice if a UPT access device without IC card is used.

The algorithm will not be published. It is distributed on request by a custodian appointed by ETSI.

10.2 The TE 9 algorithm

EN 726 defines commands for internal and external authentication to be performed in IC cards. One option for the used authentication algorithm, which has special support in the proposed standard, is the ETSI algorithm TESA 7. The use of this algorithm is the recommended option if IC cards are used in UPT access devices.

The algorithm will not be published. It is distributed on request by a custodian appointed by ETSI.

10.3 Other algorithms

This ETS allows for the use of other algorithms chosen by the service provider. These may be in the public domain or proprietary. For security reasons and in respect of the overall security of UPT, the algorithm shall fulfil the following requirement:

- for any set of inputs it shall be computationally unfeasible to use the knowledge of the corresponding outputs under an unknown key to deduce the key, or to deduce the output corresponding to any additional input value.

Annex A (informative): Device holder verification

A.1 Introduction

This annex gives one example of a method for DHV.

The aim of the DHV is to protect the UPT user against fraudulent use of a stolen device, by identifying the device holder (normally the UPT user) before it is used.

The DHV can be based on the knowledge of a short code by the user, the LPIN, which is presented to the device by the user. Different mechanisms for linking the device holder to the device may be used, but are not described here.

A.2 DHV in the UPT access device

At the time of personalization, the following data related to the management of the LPIN is loaded into the UPT access device:

- an initial LPIN value; and optionally

- a SLPIN for device unblocking.

After the UPT access device is turned on, the user needs to give the LPIN. The given LPIN is then compared with the LPIN stored in the device.

The UPT access device should not perform any other security related function before the correct LPIN value has been entered by the user. In particular, no authentication data can be obtained before a successful LPIN verification. After a successful DHV a timer is started. When the time-out is reached the DHV is no longer valid. A new card holder verification needs to be performed in order to use the device for authentication.

It should be possible for a UPT user to change the LPIN value. This change can be made in two different ways depending on whether or not the user remembers the old LPIN. If the old LPIN is known, the change LPIN procedure can be used, otherwise the unblocking procedure can be used.

In the change LPIN procedure it should only be possible to change the LPIN after a presentation of the old LPIN. Then the new LPIN needs to be presented twice consecutively. The LPIN is changed only if the old LPIN is correct and the two consecutively new LPINs are equal.

After a predefined value of consecutive false LPIN presentations the UPT access device should be blocked. i.e. all UPT access device functions, except the unblocking capability, are disabled until a successful unblocking has been performed.

If the UPT access device is blocked it should be possible to re-establish the normal operation of the device by entering the correct value of the SLPIN and the LPIN twice (either the old one or a new one). If the SLPIN is correct and the two LPINs given are equal, then the device will be unblocked and the LPIN given will be used for future DHVs.

A limit of the number of unblocking attempts may be possible as described in EN 726.

Annex B (informative): Interface between General Part and SM in the DTMF device

B.1 Introduction

DTMF devices are recommended as UPT access devices (see clause 7). They will include a SM if strong authentication is used. The interface between the UPT user (or subscriber) and the device, and the interface between the device and the UPT system are described in the main part of this ETS.

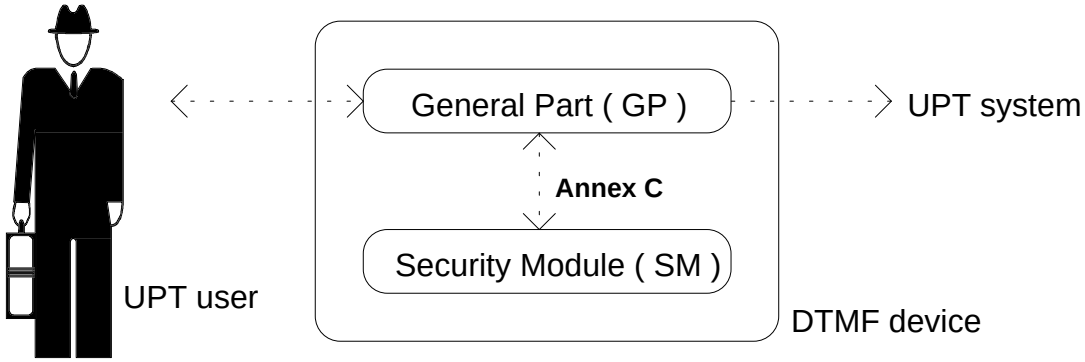

Figure B.1: Interfaces of the DTMF device

The interface between the General Part of the DTMF device (GP) and the SM need not be standardized. The aim of this annex is to give the manufacturers of such DTMF devices some recommendations on how this interface could be implemented. The following proposal takes especially two points into consideration:

- security requirements;

- upwards compatibility with UPT phase 2 (use of IC cards).

The device needs to store UPT user (or subscriber, respectively) related data, especially secret parameters (secret key, LPIN, SPIN); it checks the user's LPIN; it manages the sequence number; and it computes the variable AC. All of this data should be implemented in the SM, even if the data is not secret, to facilitate the personalization process.

NOTE 1: In this annex, it is assumed that the DHV is performed by checking an LPIN in the device, see annex A.

NOTE 2: A fraudster could still manipulate a GP, e.g. in order to eavesdrop the LPIN or to eliminate the time-out. However, this is not seen as a relevant threat since the fraudster would first of all have to steal the device for doing the manipulation (without being noticed by the device holder) and then to steal it a second time for the illegal use itself.

The SM may also be a (multi-application) IC card. This solution will be standardized for UPT phase 2.

The requirements stated in EN 726 should be applied as soon as IC cards are used for UPT. It is possible to apply these requirements to a SM inside a DTMF device already, in UPT phase 1. This is one way to fulfil the security requirements on that SM, and it will facilitate the transformation to later UPT phases, when standardized IC cards will be used for UPT.

In the following, the GP-SM interface is described at a general level for several security relevant procedures. A more detailed description can be found in ETS 300 477.

B.2 Verification of the device holder by an LPIN

The user will enter the LPIN into the UPT access device for authentication to the device. This DHV is done within the SM of the device, by matching the LPIN entered by the user with the securely stored value.

Figure B.2 shows the information flow when the user enters the LPIN.

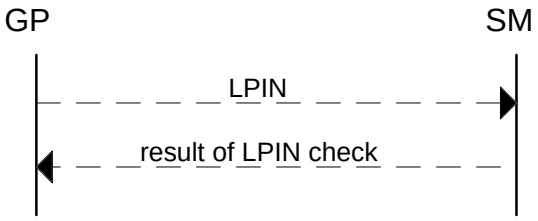

Figure B.2: Information flow for LPIN check

The result of the LPIN check can be one of the following:

- positive: LPIN is accepted;
- negative: another try is possible;
- negative: SM is blocked.

B.3 Time-out

To avoid misuse or malfunction if the user enters the LPIN without performing any subsequent action, a time-out is recommended. The timer may be implemented in the GP. In this case, the procedure given in figure B.3 should take place at time-out.

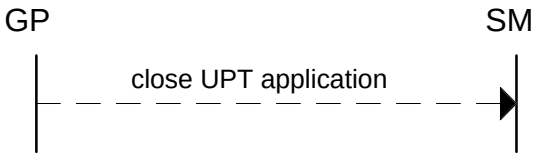

Figure B.3: Information flow for time-out

The command "close UPT application" means that the SM is reset to a status where the access condition DHV is no longer valid.

The time-out action may also be realized by reset or power-off of the SM.

B.4 Unblocking of the device

It should be possible to unblock the device by unblocking the SM. This can be done by input of a SLPIN. Additionally, a new LPIN should be given. The GP checks if the values for the new LPIN (which needs to be entered twice by the user) are equal, before it sends the SLPIN and the new LPIN to the SM.

NOTE: The SLPIN is called UNBLOCK CHV in the terminology of EN 726.

Figure B.4 describes the information flow for the unblocking procedure.

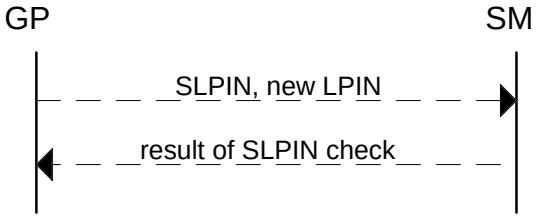

Figure B.4: Information flow for the unblocking procedure

The result of the SLPIN check can be one of the following:

- positive: SLPIN is accepted, SM is unblocked;
- negative: SM is still blocked, another try is possible;
- negative: SM is irreversibly blocked (no possibility to unblock).

B.5 Change of LPIN

The user shall have the possibility to change the LPIN. The GP checks if the values for the new LPIN (which needs to be entered twice by the user) are equal, before it sends the new LPIN to the SM (see figure B.5).

Figure B.5: Information flow for LPIN change

B.6 One pass authentication by use of a sequence number

The one pass authentication mechanism (strong authentication) as described in subclause 5.2.2 can be implemented in the interface between GP and SM as described in figure B.6. It is possible to use the architecture defined in EN 726-3, especially the commands: SELECT; READ RECORD; INCREASE; and INTERNAL AUTHENTICATION.

The prerequisite for this process is a DHV. After this check, the timer within the GP starts.

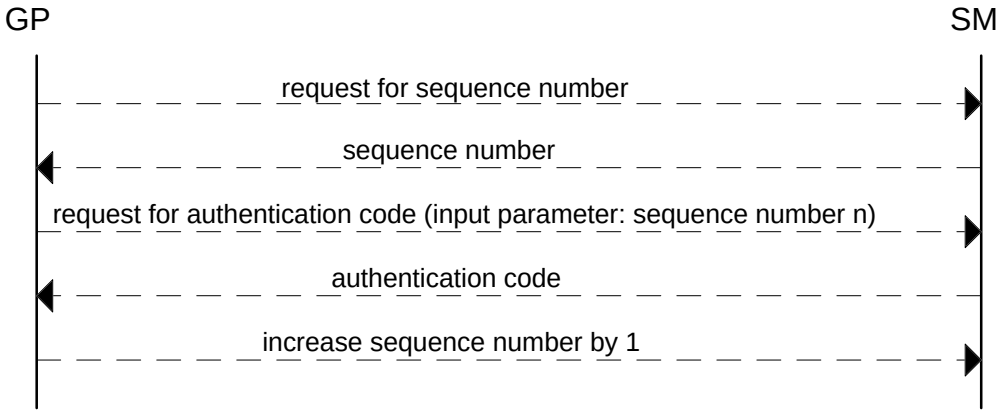

Figure B.6: Information flow for strong authentication

B.7 Key management

No key loading is expected to take place during the usage phase of the device. The key and all personalization data are loaded at subscription time (see annex D).

Annex C (informative): Bill limitation

In this annex, two examples for bill limitation are given. Combinations may also be used.

C.1 Absolute bill limitation

At call set-up, the UPT system checks the total amount of the current bill.

If this is less than a given limit, the call is accepted.

Otherwise, if there are no outstanding bills (i.e. no bills were sent out that are not already paid), the actual bill is sent to the subscriber, but this call is still accepted. Therefore, the service provider sends the bill at the latest when the service provider notices that the limit is exceeded. However, the subscriber gets some time to pay the bill before the PUI is blacklisted.

If the total amount of the current bill exceeds the given limit and there is a bill outstanding (i.e. a bill was sent out that the user has not yet paid, but the user still has time to pay it), this call is still accepted as long as this does not exceed twice the given limit.

Otherwise (i.e. if there is a bill outstanding, and the user has not paid in time or double of the limit is exceeded) the PUI is blacklisted. Subsequent calls should be refused until the bill is paid.

Hence, the UPT service provider is forced to send bills in time and to check payment during each call set-up. The subscriber always gets a bill before the amount exceeds an unacceptable level. Furthermore, the UPT service provider can be sure, in case of fraudulent or bankrupt users, not to lose more money than about double the agreed limit.

C.2 Bill limitation with respect to time

Another possible measure would be to limit the bill with respect to time. This means that if, for example, a limit per week is agreed and this limit is found to be exceeded at call set-up, then the user access would be blacklisted for the rest of the week.

Annex D (informative): Subscription process and key management

D.1 Subscription process

The following activities should be considered:

a) agreement between subscriber and service provider:

- when a subscriber wishes to make a subscription, a contract should be established with the service provider in which the allowed procedures to each user and, especially, the type of authentication procedures allowed should be specified. In case of lost or not received device, the subscriber should be obliged to report it to the service provider;

b) personalization of the advanced DTMF devices (in case of strong authentication):

- each user and optionally the subscriber needs to have an advanced DTMF device. During the personalization, the data as specified in clause 7 should be entered. Unauthorized personalization should be avoided. The manufacturer may implement a secret code (a password or a cryptographic key), which needs to be provided to put the device into personalization mode. This secret has to be given to the concerned service provider in a secure way. The secret code may be a cryptographic key only if a cryptographic algorithm and the mechanism for authentication are already implemented in the SM of the device;

c) installation of all personal data in the AE associated with the relevant SDF:

for each user, the relevant data should be contained in the AE. None of the security relevant data should leave the AE and the service provider should take precautions against possible losses of the data by using backup copies;

d) distribution of devices and LPIN (in case of strong authentication):

- the service provider gives to each user a device with a LPIN and a SPIN. (If this distribution is made by mail it is recommended to use two letters, one for the device and one for the codes, where at least one of the letters should be sent by registered mail);

e) distribution of PIN and PUI (in case of weak authentication):

- the PUI and the PIN shall be given to each user in a secure way (by using two letters, one for the PUI and one for the PIN, i.e. with the second letter sent by registered mail). The user should be advised to change the PIN the first time that the user uses the service;

f) termination of subscription:

- when a user or a subscriber wishes to terminate the subscription, the service provider removes the key and all the subscriber related data in the AE.

D.2 Key management

Key management involves key generation, key loading, key use and how to proceed when a key is lost.

D.2.1 Key generation

To generate authentication keys, the service provider can derive them from a master key and user specific data like PUI or UPTN, or use a random generator. The methods of generating authentication keys is a service provider choice.

D.2.2 Key loading

The installation of the keys in the advanced DTMF devices should be performed during the personalization. EN 726-3 provides some support for key management, this approach is described below.

Two types of keys are specified:

- management keys; and
- operational keys.

The management keys are used to fulfil access conditions required for management actions, like creating files or loading keys into the card.

The operational keys are used in cryptographic processes when the card is in normal operation, like authentication and integrity protection.

A special command has been specified to load keys, "Load Key File". When this command is used, the data (key and related information to be stored in the key file) is encrypted and integrity protected. It can be used to replace a key with a new one. The authentication key to be used in the authentication of a UPT access device is an operational key. It can be loaded into the card, either at personalization or later, but it cannot be entered by the user, due to the access conditions specified for the key file. In the key file in the card it is possible to prevent the use of a specific key for "internal authentication" (authentication of the card).

The "Load Key File" command can be used in the following scheme for key management:

a) the card manufacturer creates a master file, MF, which is the root in the card's tree structure. The card manufacturer creates a key file for management keys needed to create applications in the card. The management key file is loaded with temporary management key(s), K_{TM}, which are also given to the card issuer;

b) the card issuer can use the "Load Key File" command and K_{TM} to replace K_{TM} with the card issuer's own management key(s), K_M, which the card issuer generates. The manufacturer no longer knows any secret key in the card;

c) the card issuer can now create files at the master file level, including a file for operational keys, if needed;

d) the card issuer creates a dedicated file (the root of the file structure of an application) for UPT, DF_{UPT}. The card issuer can also create another management key file to be used under DF_{UPT} only. In this file the card issuer loads a temporary (UPT) management key, K_{TMUPT}, which is also given to the UPT provider;

e) the UPT provider can use the "Load Key File" command and K_{TMUPT} to replace K_{TMUPT} with the UPT provider's own (UPT) management key(s), K_{MUPT}. There will then be a separation between the UPT provider and the card issuer. Subsequently, only the UPT provider can create files under the DF_{UPT};

f) the UPT provider can create an operational key file, and load it with an authentication key.

If the card issuer and the UPT service provider are the same organization, the scheme can be simplified, because no separation between card issuer and UPT provider is needed.

A similar procedure could be used even if the SM is not an IC card.

D.2.3 Key use

In phase 1, the authentication process is always performed in the home network and not in the visited network. Therefore, the authentication key (or the master key) is always readily available for the SDF. The service provider can check the identity of the user by using the authentication algorithm and all data necessary.

D.2.4 Lost key

If a user loses a device, the service provider can provide a new device which contains a new key K. This new key replaces the old one in the AE. A device containing the old key can no longer be used.

Annex E (informative): Activity monitoring

A UPT network requires monitoring facilities to detect fraud, and mechanisms to blacklist a PUI if necessary. Optionally, mechanisms are useful to suspend a UPT service from a particular source or to a particular destination.

Account monitoring requires rapid transport of accounting information. However, current practice is often quite slow, and is usually at least 24 hours in delay.

This annex describes:

- appropriate monitoring points in networks supporting UPT;
- activities and events to be monitored;
- ways of processing these activities and events to provide useful information.

E.1 Monitoring points

A UPT supporting network should have monitoring functions in the centre as well as at the periphery (figure E.1).

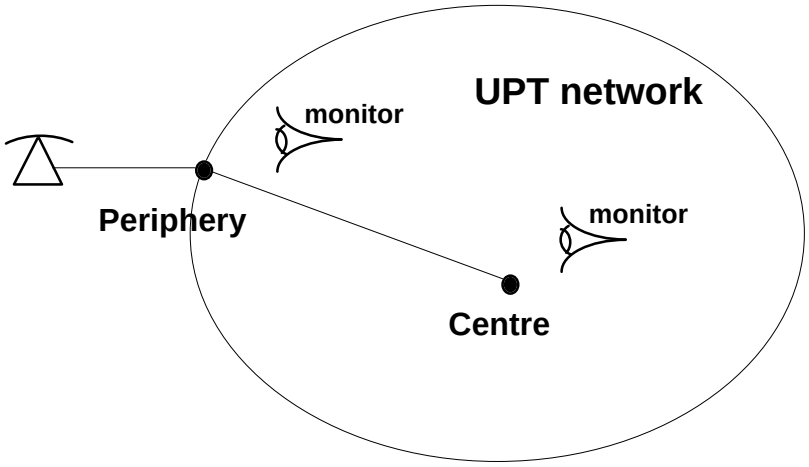

Figure E.1: Monitoring points

E.1.1 Network centre

The centre can observe information relating to the entire network. It will probably rely on being provided with **calling line identity** by the network. The centre will be able to observe rapid switches of registration, or large numbers of calls to an incall registered (apparent) user.

E.1.2 Network periphery

The network periphery can readily **observe** and **collate** information relating to a local area (e.g. a single person checking a number of accounts to find which one fitted a chosen PIN). In some cases, the periphery is in a much better position to monitor than the centre, particularly when authentication is a distributed function.

E.2 Monitored activities

This list of activities is subject to addition. Activities which may be monitored are associated with:

- authentication;
- UPT calls;
- charging.

E.2.1 Authentication

It should be possible to monitor each authentication attempt and to collate according to:

- PUI;
- PIN (if used);
- location (network address, geographic location).

EXAMPLE: The number of all (i.e. not necessarily consecutive) unsuccessful identification and authentication attempts from a specific network access (identified by the calling line identity) could be recorded and limited. After reaching the limit, further UPT access would be inhibited from this access. The line subscriber or other services from this access would not be influenced.

E.2.2 UPT calls

It should be possible to monitor each UPT call and to collate information according to its:

- source;
- destination;
- duration;
- cost (charging information);
- plurality (how many calls are active close in time on the same PUI);
- services.

E.3 Monitoring procedures

E.3.1 Account monitoring

It should be possible to centrally monitor each subscriber's account, for the cumulative spend against a limit associated with a certain period, such as a week. A more sophisticated monitor could look at a number of time periods/limits simultaneously. If the limit is exceeded, then some action is taken which could be:

- automatically to blacklist the PUI;
- to report the credit violation, for manual intervention.

A further feature could be to take into consideration whether the account has been paid since the last bill.

E.3.2 Authentication monitoring

The network should be able to analyse authentication attempts:

- by PUI, to see if an account is under attack (centre);

- by source, to see if attacks have a particular source or locality (periphery or centre);

- by PIN, if weak authentication is used, to detect an attempt to find a matching PUI to a particular PIN (periphery or centre).

E.3.3 Call monitoring

The network should be able to analyse and to collate successful calls, in order to identify patterns of fraud. This analysis should be performed at the centre.

Annex F (informative): Bibliography

The following references are used for informative purposes in this ETS.

prETS 300 391-2: "Universal Personal Telecommunication (UPT); Specification of the Security Architecture for UPT Phase 1; Part 2: Protocol Implementation Conformance Statement (PICS)".

prETS 300 391-3: "Universal Personal Telecommunication (UPT); Specification of the Security Architecture for UPT Phase 1; Part 3: Conformance Test Specification".

prETS 300 477: "Universal Personal Telecommunication (UPT); UPT Phase 2; Functional specification of the interface of a UPT Integrated Circuit Card (ICC) and Card Accepting Devices (CADs); UPT card accepting Dual Tone Multiple Frequency (DTMF) device".

DE/NA-072502: "Universal Personal Telecommunication (UPT); UPT Phase 2; Functional specification of the interface of a UPT Integrated Circuit Card (ICC) and Card Accepting Devices (CADs); UPT card accepting Dual Tone Multiple Frequency (DTMF) device; Conformance Test Specification".

ETR 055-2: "Universal Personal Telecommunication (UPT); The service concept; Part 2: General service description".

ETR 055-6: "Universal Personal Telecommunication (UPT); The service concept; Part 6: Subscriptions and service profiles".

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

ETR 121: "Universal Personal Telecommunication (UPT); Architecture and functionalities for interworking".

prEN 726: "Terminal Equipment; Requirements for IC cards and Terminals for Telecommunication Use".

CEC Directive SYN 287 (1992): "Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data".

CEC Directive SYN 288 (1990): "Proposal for a council directive concerning the protection of personal data and privacy in the context of public digital telecommunication networks, in particular the integrated services digital network (ISDN) and digital mobile networks".

History

Document history			
December 1994	Public Enquiry	PE 75:	1994-12-05 to 1995-03-31
May 1995	Vote	V 80:	1995-05-22 to 1995-07-28
August 1995	First Edition		
January 1996	Converted into Adobe Acrobat Portable Document Format (PDF)		

ISBN 2-7437-0216-8 - Edition complète
ISBN 2-7437-0217-6 - Partie 1
Dépôt légal : Août 1995