FINAL DRAFT

EUROPEAN TELECOMMUNICATION STANDARD

pr **ETS 300 790**

July 1997

Source: ETSI TC-NA

Reference: DE/NA-064006

ICS: 33.020

Key words: UPT, security, card

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

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

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

Contents

Foreword

This final draft European Telecommunication Standard (ETS) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI), and is now submitted for the Voting phase of the ETSI standards approval procedure.

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

Proposed transposition dates	
Date of latest announcement of this ETS (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Introduction

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

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

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

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

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

Blank page

1 Scope

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

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

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

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

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

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

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

2 Normative references

This ETS incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references, the latest edition of the publication referred to applies.

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

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

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

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

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

3 Definition and abbreviations

3.1 Definition

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

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

3.2 Abbreviations

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

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

4 Security requirements and security features

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

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

4.1 UPT Phase 2 security requirements

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

4.1.1 Requirements from the threat analysis

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

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

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

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

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

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

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

Called party specified secure answering of incoming calls:

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

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

Network specified secure answer:

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

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

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

Call pick-up:

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

Multiple registration:

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

Calling party identity presentation and calling party identity restriction:

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

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

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

Connected user identity presentation:

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

Connected user identity restriction:

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

Personal addressing:

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

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

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

Reset of a UPT registration:

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

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

4.1.2 Personal data integrity issues

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

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

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

Services like:

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

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

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

4.1.3 Additional requirements on UPT interworking with GSM

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

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

The following list gives some examples:

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

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

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

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

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

- using a UPT card, following GSM card specifications, but dedicated for UPT use.

The first three methods are not different from what has been described for UPT with PSTN terminals in the security architecture for UPT Phase 1. No additional security requirements have been identified.

The last three methods, using cards, have not been technically specified and need further study as to their feasibility. Possible additional security requirements have to be treated in context with eventual future descriptions of one or more of these options.

4.1.4 Additional requirements on UPT interworking with ISDN

The following extra threats and requirements to UPT are identified in case UPT is used on an ISDN:

- a registration on an ISDN phone implies a registration on all other terminals connected to the same ISDN S-bus. The UPT user is threatened by the possibility of not being aware of having made a registration at more than one terminal (maybe placed in other rooms);

  the UPT user who is going to make a UPT registration at aN ISDN number, shall be warned that the registration will be active at all terminals connected to that ISDN number. It is more user friendly to steer calls to specific terminals;

- service interaction between UPT and ISDN supplementary services may cause serious security problems, as a core UPT feature might override a (security) supplementary service of an ISDN. E.g. imagine an ISDN Closed User Group (CUG) and a third party who makes a (remote) UPT registration or a call forwarding to a number into the ISDN CUG. The ISDN CUG subscriber will not be aware of this registration. Also ISDN CLIR and various ISDN call barring features may not be affected by UPT;

  UPT as a new service shall not damage the security services and features in existing networks, such as CUG, CLIR and various call barring services. It shall never result in a lower security level. Vice versa ISDN supplementary services may not damage existing UPT supplementary services.

4.1.5 Additional requirements on UPT interworking with data services

No additional requirements have been identified.

4.1.6 UPT Security requirements associated with the use of UPT cards

This subclause deals with security requirements, based on identified threats, for management and use of UPT cards.

4.1.6.1 Management requirements

Manufacturing:

- the data and coding in the card's memory is exposed to unauthorized persons or tampered with during the manufacturing of the card. Therefore, the data and the coding shall be physically and logically protected to maintain the integrity of the data and coding (e.g. the program code for the authentication algorithm).

Personalization:

- someone can make copies of a UPT card. Therefore the personalization process has to be designed in such a way that authentication keys are not exposed to anyone else than trusted personnel;

- if Card Holder Verification (CHV) is shared between UPT and another application in a multi application card the CHV may be disabled by the user for the other application (e.g. a GSM SIM), and hence also for the UPT application. Therefore, the UPT CHV shall never be shared with an application where the CHV can be disabled;

- if there is another application in the same card as the UPT application, then the other application may violate the security of the UPT application. Therefore the UPT application shall not be put in the same card as other applications, if this security violation cannot be avoided.

Initial Card Holder Verification:

- if all UPT cards from a UPT SP contain the same initial CHV value some UPT users may keep it without changing it. Unauthorized users may then try this initial CHV if they find or steal a UPT card. Therefore all UPT cards shall not have the same initial CHV information.

Distribution:

- the card can be stolen or distributed to wrong person. Therefore CHV information shall be distributed separately from the card.

Stolen or lost cards:

- a stolen UPT card may be used by someone unauthorized, who has either guessed the CHV information or stolen that as well. Therefore the SP shall keep a black list of PUIs, and the users shall be instructed to report stolen or lost cards to the SP.

Termination:

- a UPT user may keep his card even though his subscription has been terminated. Therefore, the UPT SP shall invalidate the PUI and delete the corresponding authentication key in the AE. Care shall be taken so that a reused PUI does not get the same key again.

4.1.6.2 Operational requirements

Card Holder Verification:

- the card can be lost or stolen. Therefore, the UPT card shall be protected against unauthorized use, by means of a CHV;

- the CHV may be found by exhaustive search. Therefore, the card shall be blocked in case of three consecutive wrong CHV presentations;

- someone unauthorized can use the UPT card after the authorized UPT user has performed the CHV, if the UPT user forgets it in the terminal. Therefore, the duration of the access rights granted by the CHV shall be limited, to protect both the UPT user and the UPT SP;

- the CHV data can be disclosed if a line is eavesdropped, if the UPT card is remotely controlled by the UPT SP. Therefore, the CHV data shall never be transferred over the line, or it shall be protected against eavesdropping;

- the UPT user may forget his CHV information, and unintentionally block his UPT card. He cannot then use the UPT service. Therefore, a procedure to handle this situation is required;

- someone can get hold of the CHV information (e.g. by looking over the UPT user's shoulder). Therefore, it shall be possible for the user to change his CHV information.

Data protection:

- if the UPT card is lost or stolen the data stored in the card can be accessed. Therefore, access control to the data in the card is required. The authentication algorithm and the key(s) shall never be possible to read out from the card;

- additional program code can be added to the card. Therefore, it is required that program code can be added only under control of the card issuer or the card or chip manufacturer.

Manipulated lines, (in case of transparent terminals):

- if a UPT card is controlled by the UPT SP over the network, (i.e. the UPT card is introduced in a "transparent" terminal controlled from the network) then also a line intruder can gain control of the UPT card. If this happens after a successful CHV the access control to the UPT card cannot prevent access to data and the authentication algorithm from the line. Therefore, it is required that the authentication mechanism is not vulnerable for this attack.

Manipulated terminals:

- if a terminal is manipulated it can read out or modify data in the UPT card in an unauthorized manner. Therefore, it is required that the authentication mechanism is not vulnerable for this attack.

4.2 UPT security features

Enhanced security features are necessary for a well functioning UPT Phase 2. In ETS 300 391-1 [2] many security features are already described, both features for the interaction with the UPT user and features integrated in the service management. Security features already specified in Phase 1 are e.g. weak and strong user authentication and access control to the service profile. Examples of security management features are the security profiles, bill limitation, itemized bills and activity monitoring.

This subclause specifies security features for UPT Phase 2, which are new or modified compared to Phase 1.

4.2.1 Authentication features

A new user authentication feature is required for UPT Phase 2 and becomes possible with the support of UPT cards and card reading terminals.

In subclause 4.2.1.1 a discussion on possible features is described, followed by the evaluation in the next subclause.

4.2.1.1 Discussion on possible features to meet the authentication requirements

The one pass strong authentication specified for UPT Phase 1 is not sufficient to meet the requirements when the UPT Phase 2 feature OCR is introduced. The security can be improved by any of the following alternatives:

- two pass strong authentication;

- message authentication, i.e. data integrity protection of critical information between UPT user and SP.

Moreover, security management features to limit the use of this service are strongly demanded (see subclause 4.2.2).

The one pass strong authentication specified for Phase 1 does not meet the requirements of the Phase 2 service Secure Answer (SA). This service can make use of any of the following alternatives:

- two pass strong authentication;

- mutual authentication;

plus a special authentication code to be used only for SA service in case two pass strong authentication can not be used.

Protection against active line manipulation can not be achieved by an authentication feature only. It can only be achieved by a data integrity feature (such as Message Authentication Codes, MAC). A MAC protection can be designed to provide protection to meet also the security requirements for OCR.

4.2.1.2 Evaluation and choice of security features for authentication

Summarizing, the following features can be used to offer the required protection:

- two pass strong authentication or data Integrity protection (e.g. MAC) for increased security especially when OCR is allowed;

- two pass strong authentication, mutual authentication or special PIN for secure answer;

- data integrity protection (e.g. MAC) for the protection against active line attacks.

Two pass strong authentication is chosen as a new UPT Phase 2 security feature. It solves the most important needs. Two pass strong authentication also has the advantage to be closely related to GSM authentication and evolution from UPT Phase 1 cards used as a security module of the advanced DTMF device to UPT Phase 2 cards will be straight forward. It is to be noted that two pass strong authentication can be easily implemented in cards. Mutual authentication is not needed in case two pass strong authentication is chosen, as this covers the threat with SA.

The need for a separate feature called "extra authentication for OCR" has been identified (service requirement). This feature shall be implemented in UPT. The feature is optional for the UPT user as a simple protection against unauthorized use of his OCR.

Two pass strong authentication is chosen for calling UPT user specified secure answering of incoming calls.

Two pass strong authentication is chosen for called party specified secure answering of incoming calls service. However, in order to allow these users to use this service from terminals not equipped with a card reader, a separate feature called "special authentication for secure answering" is needed. This feature shall be implemented in UPT.

Data Integrity protection (e.g. MAC) implemented for UPT Phase 2 cards is considered too complicated and gives little extra value in this situation as the active line manipulation threat has been evaluated as not significant. This feature is therefore not part of this Phase 2 ETS.

4.2.2 Security management

UPT Service Features providing security are bill limitation, itemized bills, activity monitoring, announcements, blocking of registration, reset of registration and contractual agreements. For UPT Phase 2 the same text as in ETS 300 391-1 [2], subclauses 4.3.1, 4.3.2, 4.3.4 and 4.3.5, is valid. For UPT Phase 2 the following additions are relevant.

As the requirements related to the active line attack threats are not fully covered by the authentication features, the service feature OCR shall be strongly limited in its use by restrictions set in security profiles (see subclause 5.7).

The UPT SP shall implement means to warn a UPT user for the situation that a registration made from one terminal connected to an ISDN line access, results in a registration on all other terminals connected to that line access.

4.2.3 Reset and blocking

There are two UPT exceptional procedures defined which are important for UPT security: Reset and Blocking, addressed to be optional. These procedures are intended to protect the privacy and integrity of third parties (e.g. the subscriber of a terminal access). These procedures are intended to be carried out by third parties, i.e. non-UPT users.

The following procedures are described:

- reset of registration for incoming UPT calls;

- blocking of registration for incoming UPT calls;

- deblocking of registration for incoming UPT calls;

- reset of registration for outgoing UPT calls.

Reset and blocking of registration were not generally available in UPT Phase 1. For UPT Phase 2 it is strongly recommended to implement these procedures in all networks. Legal requirements may enforce these procedures as mandatory (see subclause 4.1.2).

4.2.4 Security features related to the use of UPT cards

In this ETS, a UPT Card is presumed to contain two pass strong authentication. The access to UPT by means of a UPT card is a Phase 2 feature. It can be used in UPT card reading terminals. The UPT card is easier to use than the advanced DTMF device, specified in Phase 1. It also makes it possible to speed up the authentication procedure and introduce two pass strong authentication. The UPT card shall support the following security features:

- authentication of the user to the UPT card;

- authentication of the UPT card to the UPT SP.

In combination these two features give authentication of the user to the SP. It can be used to access the UPT service, for authentication required by the secure answer feature and for access to the service profile.

4.2.5 Security features available as UPT supplementary services:

Some of the UPT supplementary services can be used by the UPT user for his own security needs. The security architecture is not based on these services. They are nevertheless important for increasing the security in UPT Phase 2.

The following security related supplementary services may be used by the UPT users:

- calling party identity presentation;
- calling party identity restriction;
- connected user identity presentation;
- connected user identity restriction;
- closed user group;
- advice of charge at UPT call set-up time;
- advice of charge during UPT call;
- advice of charge at UPT call completion;
- all charge acceptance for incoming UPT calls;
- charge refusal for incoming UPT calls;
- password screening of incoming UPT calls;
- priority screening of incoming UPT calls;
- predefined screening of outgoing UPT calls;
- predefined screening of incoming UPT calls;
- barring of all incoming UPT calls;
- barring of all outgoing UPT calls;
- barring of all international incoming UPT calls;
- barring of all international outgoing UPT calls;
- barring of all incoming UPT calls when roaming;
- barring of all outgoing UPT calls when roaming;
- calling UPT user specified secure answering of calls to UPT users;
- called UPT user specified secure answering.

4.3 UPT security limitations

Only a few threats identified have not been covered by security features. UPT features that are new in Phase 2 introduce new threats and sometimes higher risks to existing threats, but the standardized Phase 2 two pass authentication feature offers more protection than the Phase 1 authentication feature. Only threats related to active line manipulation, like taking over the line between a user and SP after fulfilled authentication, are not covered. These threats are not evaluated as significant. They are partly covered by means of security management features. Most of these features do not directly prevent fraud but they detect and limit potential fraud.

Threats not covered also include all those concerned with eavesdropping, e.g. on sensitive personal data. However the threat to eavesdrop authentication codes has no impact when the two pass authentication feature is used.

Feature/service interaction between UPT features/services mutually, and between UPT features/services and PSTN, ISDN or GSM services may result in unwanted interactions. These interactions could have an impact on the security level of UPT if not solved correctly.

5 Security mechanisms

This clause describes how the security requirements and the security features stated in clause 5 can be accomplished by security mechanisms, where different from UPT Phase 1. It comprises mechanisms for access control and authentication, as well as aspects of security management and security profiles. A two pass strong authentication mechanism supported by a card is specified in this clause.

5.1 Access control mechanisms

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

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

- access to the UPT service profile and other management data by users, subscribers, authorized personnel of the UPT SPs, and by enquiries from home or visited network;

- access to the data in the advanced DTMF device;

- access to the data in the UPT card.

5.1.1 Access control to the services

In UPT Phase 2, the check of the service profile data for authorization is recommended to be carried out at the home location. Hence the same text as in ETS 300 391-1 [2], subclause 5.1.1 is valid.

5.1.2 Access control to the service profile data

The same text as in ETS 300 391-1 [2], subclause 5.1.2 is valid.

The following additions and modifications in the structure of the service profile are foreseen:

a) information set by the SP at subscription time:

   - services subscribed to (PSTN, ISDN, GSM);
   - types of authentication subscribed to (weak, one pass, two pass authentication);
   - security options subscribed to (called party specified secure answering of incoming UPT calls, intended recipient identity presentation);

b) information changeable by the subscriber:

   - type of authentication allowed (weak, one pass, two pass authentication);
   - security options allowed (called party specified secure answering of incoming UPT calls, intended recipient identity presentation);

c) information changeable by the user:
   - type of authentication activated (weak, one pass, two pass authentication);
   - security options activated (called party specified secure answering of incoming UPT calls, intended recipient identity presentation).

5.1.3 Access control to the data in the UPT card

The card shall at least contain the following sensitive data:

- PUI (the Personal User Identity);
- K (the authentication key);
- the program code for the authentication algorithm f;
- CHV;
- unblocking CHV.

The card shall also contain a Timer value (T) which indicates how long the access rights granted by the CHV are valid. It may contain (optional to the SP) Maximum value of T (T_{MAX}), indicating the maximum value.

The following requirements on data access are specified:

- it shall never be possible to read K, CHV and the program code for the authentication algorithm;

- it shall not be possible to read PUI, T, T_{MAX} or to perform an authentication before a successful CHV has been performed;

- it shall not be possible for the user to change the PUI, K, T_{MAX} or the algorithm in the UPT card;

- it shall be possible for the user to change CHV and T in the UPT card.

5.2 User authentication mechanism

For UPT Phase 2 two additional authentication mechanisms are specified here, two pass strong authentication, and CHV. The access to the UPT service is established by the use of a UPT card. The authentication process can be split up into two parts: the authentication of the user to the card and the authentication of the card to the UPT SP. It shall not be possible to perform the two pass strong authentication without a previous successful CHV.

The two pass strong authentication mechanism is specified to be used between a UPT card and the AE, when the card is inserted in a UPT card reading terminal. It is not intended to be used in an advanced DTMF device.

The two pass strong authentication mechanism avoids replay attacks. Compared with the one pass strong authentication mechanism specified in ETS 300 391-1 [2] it gives additional protection: It protects against the Secure answer threat described in subclause 4.1.1, because the masquerader is not supposed to be able to foresee the next challenge from the UPT SP.

An AE associated with the Service Data Function (SDF), shall initiate the authentication mechanism. The steps are:

1) the AE requests the PUI from the UPT card;

2) the AE receives the PUI from the UPT card, if it is black listed or invalid the process is aborted and the authentication has failed;

3) the AE performs the two pass strong authentication;

4) if the authentication has succeeded the user can use services according to his service profile, if not, the authentication failure is presented to the user.

The steps above are described in figure 1.

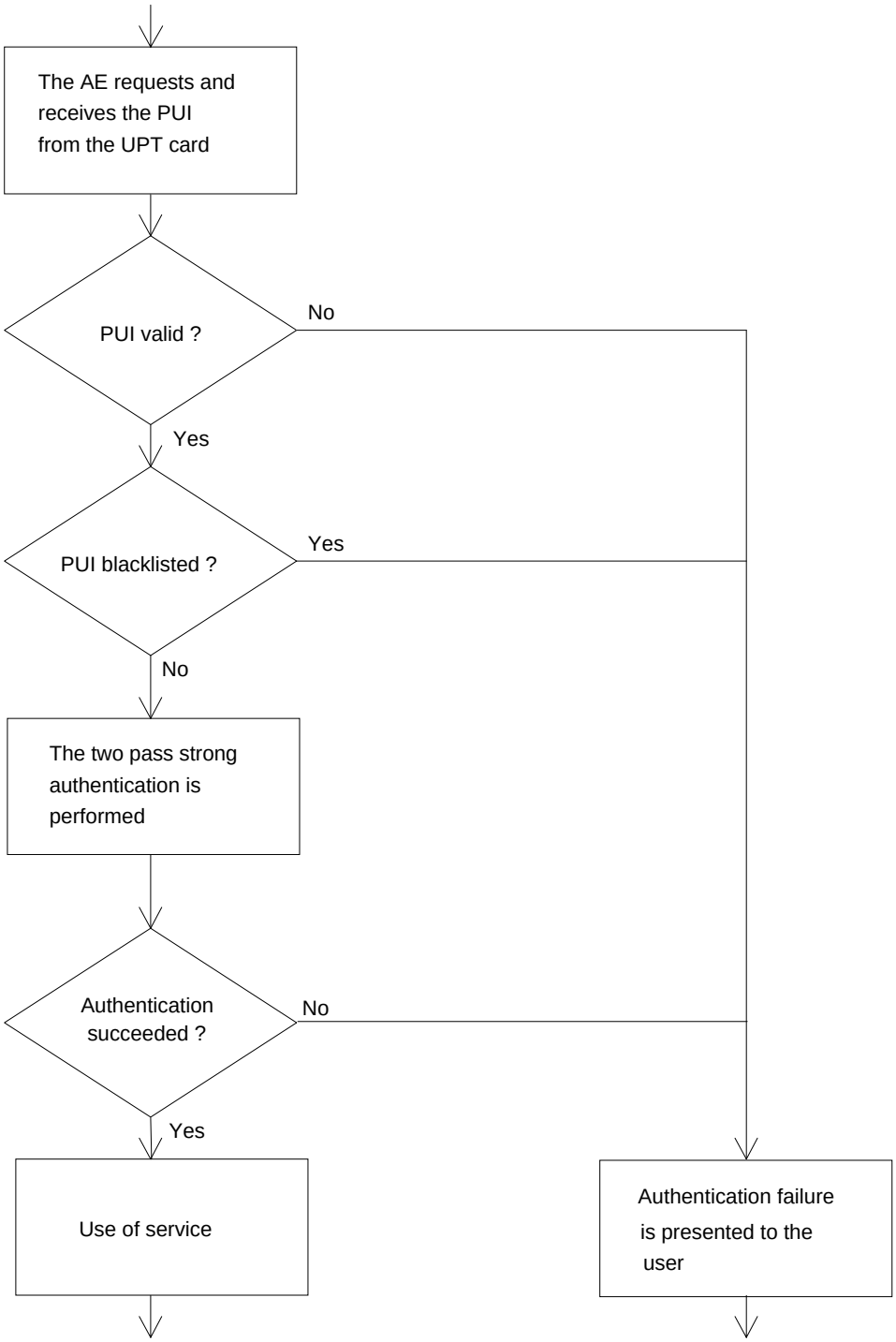

Figure 1: Functional description of the two pass strong authentication feature

5.2.1 Two pass strong authentication

The relevant data required for authentication is as follows:

RAND The RANDom number (challenge) generated by the AE at each authentication attempt. It is used as an input to the authentication algorithm f, to guarantee variation of the Authentication Code (AC).
AC Variable authentication code, calculated in the UPT card.
AC' Variable authentication code calculated in the AE.
f Algorithm for the calculation of the variable AC. f shall be a one-way function. The algorithm is used both in the UPT card and in the AE.
K Individual secret authentication key, stored both in the UPT card and the AE.
PUI The personal user identity is stored in the UPT card and in the network.

The authentication mechanism is performed as follows:

a) the random number (challenge) RAND is generated by the AE and sent to the UPT card;

b) the UPT card receives RAND, calculates AC using the received RAND, K and f and returns the AC to the AE;

c) the AE calculates AC', using RAND, K and f;

d) the AE compares AC' with the received AC. If they are equal the authentication was successful. If they are not equal the authentication has failed.

The steps above are described in figure 2. For a detailed description, see clauses 6 to 10.

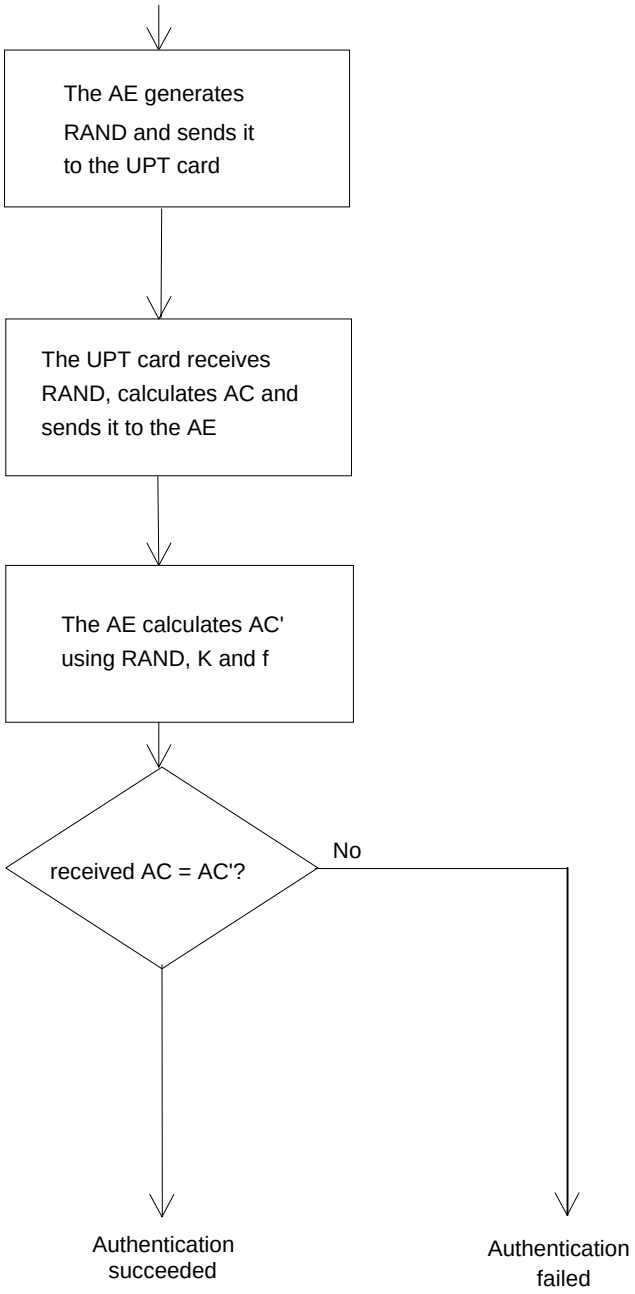

Figure 2: Functional description of the two pass strong authentication mechanism

5.2.2 Authentication of the user to the UPT card

The authentication of the user to the UPT card works as follows:

a) the UPT card is residing in a UPT card reading terminal;

b) the user is prompted by the UPT card reading terminal to give his CHV, if the UPT card is not blocked;

c) the user gives his CHV via the keypad of the UPT card reading terminal;

d) the UPT card reading terminal transfers the CHV to the UPT card. The UPT card reading terminal shall not keep the CHV after it has transferred it to the UPT card;

e) if the received CHV has the correct value, then the UPT card goes to the state "Correct CHV given", else the user is prompted to try again. In case of three consecutive wrong CHV presentations the UPT card is blocked;

f) the UPT card contains a maximum timer value T_{MAX} defined by the SP and another T which can be changed by the user as long as it is shorter than T_{MAX}. T is read out by the terminal and a timer in the terminal using this value is started. T_{MAX} is optional to the SP, T is mandatory to the SP. If the timer reaches time-out, the access rights granted by the CHV are lost. Access rights return by entering the CHV again;

g) only as long as the UPT card is in the state "Correct CHV given" it is possible to read out the PUI and to use the authentication algorithm in the UPT card;

h) the UPT card leaves the state "Correct CHV given" when it is reset or powered off.

If the UPT card is blocked, then the authentication of the user to the UPT card procedure cannot be performed. Authentication becomes possible after an unblocking procedure, using an unblocking CHV, is performed.

5.3 Extra authentication for outgoing calls

In this subclause is specified a simple authentication mechanism, to be used for each call in case of OCR is active, in addition to the normal authentication at registration time. This mechanism is optional to the user and mandatory to the UPT SP.

At subscription time, each user will be attributed a special outgoing call PIN, OCPIN. If the user is allowed to use weak authentication, the OCPIN value shall be different from his PIN value.

If the user is allowed to use weak authentication, it shall not be possible for the user to change his PIN value to the OCPIN value.

The mechanism is performed as follows:

a) the user presents his OCPIN using a DTMF telephone's normal key pad or a DTMF device each time he wants to set up a call from the terminal he is registered on;

b) the OCPIN value is checked. If its value is correct then the user is allowed to proceed.

The OCPIN is a weak security mechanism, meant as an addition to OCR.

- OCPIN can protect against someone unintentionally using someone else’s OCR; it is not safe enough to protect against intentionally using someone else’s OCR;

- there is a risk the user will choose the same code for OCPIN and CHV, which lowers the level of security of CHV;

- some terminals display or store the digits typed in; like for all PIN codes this also applies to OCPIN.

The SP should warn the user for these risks of OCPIN.

NOTE: It is allowed to fix the same values for OCPIN and SAPIN (see subclause 5.4).

5.4 Special authentication for called party specified secure answering of incoming calls

This subclause specifies a simple authentication mechanism, to be used for called party specified secure answering of incoming calls, if the user is unable to use his UPT card. This mechanism is optional to the user and optional to the SP.

At subscription time of this supplementary service, the user may get a secure answer PIN, SAPIN. If the user is allowed to use weak authentication, the SAPIN value shall be different from his PIN value.

If the user is allowed to use weak authentication, it shall not be possible for the user to change his PIN value to the SAPIN value.

The mechanism is performed as follows:

a) the user is asked to authenticate himself each time he receives a call on the terminal he is registered on;

b) the user presents SAPIN using a DTMF telephone's normal key pad or a DTMF device;

c) the SAPIN value is checked. If its value is correct then the call is completed.

The SAPIN is a weak security mechanism, meant as an additional mechanism to the UPT user who normally uses his UPT card, but who also wants to use secure answer in case no card reading device or terminal is available.

- SAPIN can protect against unintentionally answering an incoming call directed to someone else when Called party specified secure answer applies; it is not safe enough to protect against intentionally answering someone else’s incoming call;

- there is a risk the user will choose the same code for SAPIN and CHV, which lowers the level of security of CHV;

- some terminals display or store the digits typed in; like for all PIN codes this also applies to SAPIN.

The SP should warn the user for these risks of SAPIN.

NOTE: It is allowed to fix the same values for SAPIN and OCPIN.

5.5 Security management

The same text as in ETS 300 391-1 [2], subclause 5.3 is valid. The following security management measures are specified in that ETS:

- security audit trail;

- event handling;

- charging control;

- information management.

For UPT Phase 2 the following additions are relevant.

5.5.1 Charging control

The UPT supplementary service "Advice of Charge" shall be implemented in such a secure way that the UPT user can rely on the correctness of the information presented as the user will make a decision based on this information.

The UPT supplementary service "All Charge acceptance" shall give the UPT user sufficient information to make the decision to accept the charge, i.e. he should be informed about the costs he is going to accept. The use of this supplementary service shall be mentioned on an itemized bill on the UPT users request.

The UPT SP shall control charging also during a call, to avoid too high bills which will intentionally not be paid.

5.5.2 Information management

The UPT user shall be informed about the risks of the UPT features and supplementary services and ways to minimize them. The UPT user shall be given the possibility to block or refuse services in order to protect himself from unwanted calls, costs and risks.

The line subscriber shall be informed if a UPT user has registered for outgoing calls on his terminal. It can be done by using a special dial tone or by giving the following information to the users of the terminal:

"UPT REGISTRATION FOR OUTGOING CALLS FOR THIS TELEPHONE".

5.5.3 Service restrictions for OCR and for Remote OCR (ROCR)

The use of the service OCR shall be restricted to prevent fraud. This shall be done by specification in the service profile of the UPT user. The profile shall contain the allowed number of simultaneous OCRs. Furthermore the service profile shall offer the possibility to contain a pre-defined set of Access Registration Addresses (ARAs) or Network Access Points (NAPs) allowed for OCR and ROCR. On request of the UPT subscriber or the UPT user this set will be defined and activated.

5.5.4 Warnings about registration side effects

A UPT registration that takes place at a line access where more than one terminal is connected to (especially ISDN), results in a registration on all terminals connected to that line access. The UPT SP shall give a warning to the UPT subscriber and to the UPT user. The warning shall be given at subscription time and directed to the UPT subscriber and to the UPT user.

Moreover, the UPT user may also be given an announcement at registration time. It is up to the SP to implement these announcements. Examples of announcements are given in ETS 300 391-1 [2], subclause 5.3.4.

5.5.5 Security management of the UPT card

Confidentiality and integrity of the sensitive information (e.g. program code, keys and CHV) in the card shall be ensured throughout all the steps in the card life cycle: manufacturing, card preparation, UPT application preparation, usage and termination. For key management see also ISO/DIS 10202-7 and EN 726-2.

The UPT card and the CHV shall be given to the user or subscriber separately and at least one of them shall be distributed in a highly secure way (e.g. by identification of the UPT user at the post office).

The UPT user and subscriber shall be informed about the use of the UPT card, in respect to the security risks they take when giving the card to other users or potential users. They shall be requested never to give away their CHV.

The UPT user and subscriber shall be asked to report stolen or lost cards to the UPT SP, so that he can black list the corresponding PUI.

When the subscription is terminated the UPT SP shall invalidate the PUI and delete the corresponding authentication key in the AE.

5.6 Service limitations

The same text as in ETS 300 391-1 [2], subclause 5.4 is valid. For UPT Phase 2 the following additions are relevant.

Even for the case that one pass strong or two pass strong authentication is used by SPs, the full set of UPT Phase 2 services provided to users shall be restricted. Access to services which entail high risk to any participant in UPT or the SP shall not be allowed without adequate restrictions. The following restrictions have been identified as possible for the service features introduced in UPT Phase 2.

Predefined sets of Access Registration Address' (ARAs) or NAPs mean that the subscriber and the SP agree in a secure way on which ARAs or NAPs, individual or category, shall be allowed for the service. The SP shall however set the maximum limit for the number of ARAs or NAPs or category allowed. The limits for the predefined sets can be chosen to be zero (meaning the set is empty for all users, i.e. the service is not offered at all for this type of authentication). The procedures to define and to change, if requested by the subscriber, these sets shall be performed with the same level of security as the normal subscription procedure.

The choice of the predefined sets limits have to be continuously tuned by the SP with regard to anticipated and perceived threats to the service.

Predefined sets shall not allow roaming to another UPT service domain unless activity monitoring is active in this other domain

Table 1: Service limitations

Feature class	Feature	Possible restrictions
Core features	Outcall registration (also via all call and linked registrations)	predefined set of ARAs allowed for registrations for outgoing calls; predefined area in which registrations for outgoing calls are allowed; limited number of simultaneous (parallel) registrations.
	remote outcall registration (also via remote all call and remote linked registrations)	remote outcall registrations is not allowed; predefined set of ARAs allowed for registrations for outgoing calls; predefined area in which registrations for outgoing calls are allowed; limited number of simultaneous (parallel) registrations; predefined set of NAPs from which remote outcall registrations are allowed to be performed.
Supplementary features	secure answering of incoming calls, calling UPT user specified	allowed only if the called party is authenticated with two pass strong authentication (see subclause 4.1.1).
	secure answering of incoming calls, called UPT user specified	allowed only if the called party is capable to be authenticated with two pass strong authentication (see subclause 4.1.1).
ARA = Access Registration Address NAP: Network Access Points		

5.7 Security profiles

A chosen set of service limitations and security measures defines a security profile. The SP shall specify one security profile for each type of authentication used. As a general rule restrictions in service provision should be most severe in case of weak authentication and least severe in case the two pass strong authentication is used.

Three security profiles fulfilling minimum security requirements are specified in subclauses 5.7.1 to 5.7.3. A SP 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.

5.7.1 Security profile for weak authentication

The same text as in ETS 300 391-1 [2], subclause 5.5.1 is valid. For UPT Phase 2 the following additions are relevant.

The following limitations on services introduced in Phase 2 are required:

- predefined set of ARAs allowed for outcall registrations (maximum 5 ARAs should be allowed);
- remote outcall registrations are not allowed;
- limited number of simultaneous (parallel) outcall registrations;
- authentication for calling specified secure answer on incoming calls shall never be requested from a user who has not the two pass strong authentication in his service profile;
- authentication for called specified secure answer on incoming calls shall never be requested from a user who has not the two pass strong authentication in his service profile.

5.7.2 Security profile for one pass strong authentication

The same text as in ETS 300 391-1 [2], subclause 5.5.2 is valid. For UPT Phase 2 the following additions are relevant.

The following limitations on services introduced in Phase 2 are required:

- predefined set of ARAs allowed for outcall registrations (only a small number of specified ARAs should be allowed);
- predefined set of ARAs allowed for remote outcall registrations (only a small number of specified ARAs should be allowed);
- limited number of simultaneous (parallel) outcall registrations;
- authentication for calling specified secure answer on incoming calls shall never be requested from a user who has not the two pass strong authentication in his service profile;
- authentication for called specified secure answer on incoming calls shall never be requested from a user who has not the two pass strong authentication in his service profile.

5.7.3 Security profile for two pass strong authentication

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

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

The following service limitations are required:

- predefined set of ARAs allowed for remote incall registrations;
- predefined set of ARAs allowed for outcall registrations;
- predefined set of ARAs allowed for remote outcall registrations;

- limited number of simultaneous (parallel) outcall registrations;

- bill limitation.

6 Parameter sizes and values

Table 2 defines the sizes of all parameters that are used in this ETS. In some cases, the parameter size need not be standardized and then only a recommended value is given.

Table 2: Parameter sizes and values

Parameter	Length [bits]	Length [digits]	Remarks
PUI		≤16	
RAND	64-128		
AC	32-64		
K	128		Recommended value.
OCPIN		4-6	
SAPIN		4-6	
CHV		≥ 4	
Unblocking CHV		≥ 8	
T			Recommended value: default 1 minute, changeable by user.
T_{max}			Recommended value: 8h.

7 Functional specification of the UPT card

A UPT card is used by a UPT user to authenticate himself to the AE. It shall support the two pass strong authentication.

The functions specified in this chapter are valid for the UPT card supporting two pass strong authentication only.

7.1 Storage of data

The UPT card shall at least contain the following security related data:

- PUI;

- K (authentication key for two pass strong authentication);

- the program code for the authentication algorithm f;

- CHV (the data needed for card holder verification);

- unblocking CHV;

- T (timer value);

- Command Type (CT).

The UPT card may also optionally contain T_{MAX} (maximum timer value).

7.2 Processing

Processing means the usage of data inside the UPT card. It has to be pointed out that the intermediate results in the authentication algorithm are security relevant and shall therefore not leave the UPT card.

At least the following processes shall be supported by the UPT card:

- CHV;
- changing of CHV;
- unblocking CHV;
- timer;
- changing T;
- two pass strong authentication.

For two pass strong authentication the following steps are performed by the UPT card:

a) the user gives his CHV to the card via the keypad of the UPT card reading terminal;

b) the card compares the received CHV with the CHV value already stored in the card. If they match, then the CHV was successful and the number of remaining CHV attempts is set to the initial value. If the CHV failed, then the number of remaining CHV attempts is decreased by one. If it reaches zero, then the next CHV attempt will block the card;

c) T is read out from the UPT card and initiate the timer according to this value;

d) the PUI and CT value are read out from the UPT card, and they are sent to the AE in an authentication request;

e) the UPT card receives the RAND from the AE in an authentication request;

f) the UPT card performs the authentication calculation, using the authentication algorithm f as function, the random number RAND and the key K, selected by the terminal, as input. The AC is the output from this process;

g) the AC is read out from the UPT card and the PUI, CT and AC are transferred to the AE;

h) if, at any time, the time-out is reached, then the access rights granted by the CHV are lost.

7.2.1 Time-out

Directly after the CHV, a timer shall start in the terminal. The T is used to initiate the timer. The maximum time is an optional feature, decided by the SP by choosing the value of T_{MAX}. The user is allowed to change the timer value by choosing the value of T. T shall never be greater than T_{MAX}. The authentication procedure can be repeated if needed, e.g. in case of authentication failure, until the time-out is reached. If it has been reached a new CHV has to be performed to make a new try possible.

7.2.2 Calculations by the authentication algorithm

In each authentication attempt AC = f (K, RAND) shall be calculated using the individual authentication key K and the RAND received from the AE. The calculation shall be carried out by the UPT card.

7.3 User interface

Cards and card reading terminals for the UPT application shall support the following actions:

- CHV;
- changing CHV;

- unblocking the UPT card using the unblock CHV;

- changing T.

8 Functional specification of the security protocol

This clause describes the messages of the authentication protocols. The following protocols are specified:

- two pass strong authentication;
- extra authentication for Outgoing Calls PIN (the OCPIN);
- special authentication for Secure Answer PIN (the SAPIN).

8.1 Two pass strong authentication

The following messages shall be sent between the UPT card and the Authenticating Entity (AE) to perform two pass strong authentication:

- set up message (from the UPT card to AE): PUI, CT;
- authentication request (from AE to the UPT card): RAND;
- authentication response (from the UPT card to AE): PUI, CT, AC.

The RAND is the random number. The AC is the response from the algorithm from the UPT card.

CT signifies Command Type. This field is used to distinguish between type of authentication mechanism (one pass strong or two pass strong) and between type of algorithm (see clause 10). ETS 300 391-1 [2] contains the specification for CT = 1, CT = 2 and CT = 3. The following values are reserved for two pass strong authentication:

CT = 4 signifies two pass strong authentication using the USA-4 algorithm;

CT = 5 signifies two pass strong authentication using the TESA-7 algorithm;

CT = 6 (and all CT starting with 6) signifies two pass strong authentication according to the SP's own specification.

NOTE: The values 0, 7, 8 and 9 are reserved for future use.

8.2 Extra authentication for OCPIN

Once the UPT user has made an OCR, he may use the OCPIN as a protection against misuse of his registration. The following messages shall be sent between the user and the AE to perform the extra authentication for outgoing calls:

a) before each outgoing call, the AE asks the user for his OCPIN value;

b) the user sends his OCPIN value;

c) the AE checks the OCPIN value received and returns the result of the authentication to the service logic;

d) if the authentication is successful, the user is allowed to set up an outgoing call.

NOTE: It should be possible for anyone to set up emergency calls from any terminal. Possible conflicts between OCPIN and emergency calls should be avoided.

8.3 Special authentication for SAPIN

SAPIN can be used as a protection against misuse of answering incoming calls, see subclauses 4.1.1 and 5.4. The following messages shall be sent between the user and the AE to perform the special authentication for incoming calls:

a) before each incoming call, the AE asks the user for his SAPIN value;

b) the user sends his SAPIN value;

c) the AE checks the received SAPIN value and returns the result of the authentication to the service logic;

d) if the authentication is successful, the call is completed.

9 Functional specification of the AE

From the security point of view, the main function of the SDF is to authorize and authenticate the user either by a weak authentication procedure or one pass strong authentication procedure, or two pass strong authentication procedure. The SDF needs to make use of a physical entity, called Authenticating Entity (AE), that shall be protected against analysing or changing of its content. The AE may support more than one authentication procedures (weak, one pass strong, two pass strong).

Below, the following procedures are described:

- check of PUI and authentication type used;

- two pass strong authentication;

- SAPIN and OCPIN procedures;

- PIN change check.

The one pass strong authentication and the weak authentication are described in ETS 300 391-1 [2].

9.1 Check of PUI and authentication type used

The AE checks before the authentication procedure if the PUI is invalid or blacklisted. If this is the case, the authentication is refused. Authentication failure is presented to the user (see figure 1).

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

9.2 Two-pass strong authentication

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

- PUI;

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

The AE contains a random number generator in order to send a challenge number RAND at each authentication attempt.

For the two pass strong authentication procedure the following steps are performed by the AE:

a) the PUI and CT values read out from the UPT card, are received by the AE;

b) the AE generates RAND and sends it to the UPT card in an authentication request;

c) the AE performs the authentication calculation, using the authentication algorithm f as function, the random number RAND and the key K as input. The AC' is the output from this process;

d) the PUI and AC values are received from the UPT card in an authentication response;

e) the AE compares AC' to AC. If they are equal then the AE sends the message authentication successful, if not, the AE sends authentication failure.

9.3 SAPIN and OCPIN procedures

The AE contains the following data for those users who have subscribed to the use of extra PINs for OCR or secure answering:

- OCPIN;

- SAPIN.

The overall description of the use of these extra PINs is given in subclauses 5.3. and 5.4. The AE shall be able to perform the following procedures:

- check of OCPIN;

- check of SAPIN.

If the OCPIN value received from the user is not the correct one, outgoing calls from that terminal he is registered on shall be refused.

If the SAPIN value received from the user is not the correct one, the completion of the call shall be refused.

If weak authentication is used it shall not be possible to set SAPIN or OCPIN to the same value as PIN.

9.4 PIN change check

In the case that users are allowed to use weak authentication and SAPIN or OCPIN, the AE shall check during the change PIN procedure that the value given by the user for his new PIN is different from SAPIN and OCPIN values. If it is not the case, the change of PIN value shall be refused.

The change PIN procedure is described in subclause 9.3 of ETS 300 391-1 [2].

10 Authentication algorithms

For the card based two pass strong authentication in UPT Phase 2, an authentication algorithm is used in the SP's AE, and in the users' UPT cards. According to this ETS, freedom is given to SPs in the choice of the algorithm.

10.1 The USA-4 algorithm

The dedicated UPT authentication algorithm, USA-4, is available for UPT SPs and UPT card manufacturers as one option.

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

10.2 The TESA-7 algorithm

In EN 726-3 internal authentication to be performed in IC cards is defined. The authentication algorithm TESA-7 was specially specified by ETSI for inclusion in this ETS. The use of this algorithm is the recommended option for IC cards used for UPT.

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 SP. 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.

10.4 Same algorithm for one pass and two pass strong authentication

If a SP uses the same algorithm for one pass and two pass strong authentication it is required that different keys for the two types of authentication are assigned to the UPT users if they have both types of authentication in their service profile.

Annex A (normative): Implementation Conformance Statement (ICS) proformas

This annex starts with the scope (A.1) and abbreviations (A.2). Next the following proformas are given:

- ICS proforma for UPT cards used for two way strong authentication (A.3);
- ICS proforma for card reading terminals supporting UPT (A.4);
- ICS proforma for the AE (A.5).

A.1 Scope

This annex provides the Implementation Conformance Statement (ICS) proformas for the security mechanisms specified in this ETS. To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented. Such a statement is called an Implementation Conformance Statement (ICS). This ICS is in accordance with the requirements and the guidelines given in ISO/IEC 9646-7 [3] and ETS 300 406 [4].

The completed proformas is a means for the SP of a UPT system to formulate the requirements on UPT implementations or to decide whether an existing implementation meets the requirements. They detail in tabular form the mandatory and optional capabilities for implementations.

Only the capabilities relating to interoperability and overall security requirements of UPT Phase 2 are treated here. The UPT card, the authenticating entity and the card reading terminal supporting UPT are treated as different implementations with their respective proformas.

A supplier of implementations of security components which are claimed to conform to this ETS is required to complete a copy of the relevant ICS proforma provided in this clause and is required to provide the information necessary to identify both the supplier and the implementation.

If it claims to conform to this ETS, the actual ICS proformas to be filled in by a supplier shall be technically equivalent to the text of the ICS proformas given in this annex, and shall preserve the numbering/naming and ordering of the proforma items.

A.2 Abbreviations

Status column

The following notations, defined in ISO/IEC 9646-7 [3], are used for the status column:

m	mandatory - the capability is required to be supported.
o	optional - the capability may be supported or not.
n/a	not applicable - in the given context, it is impossible to use the capability.
x	prohibited (excluded) - there is a requirement not to use this capability in the given context.
o.i	qualified optional - for mutually exclusive or selectable options from a set. "i" is an integer which identifies an unique group of related optional items and the logic of their selection which is defined immediately following the table.
ci	conditional - the requirement on the capability ("m", "o", "x" or "n/a") depends on the support of other optional or conditional items. "i" is an integer identifying a unique conditional status expression which is defined immediately following the table.

A.3 ICS proforma for UPT cards used for two passstrong authentication

A.3.1 Introduction

The purpose of the ICS proforma is to submit suppliers and implementers with a questionnaire or checklist. This should be completed in order to state conformance with the requirements put forward in the relevant ETS.

A.3.2 Identification of the implementation, product supplier and test laboratory client

For administrative purposes the actual ICS shall identify:

- the implementation;
- the supplier or client of the test laboratory that is to test the implementation;
- the person to contact if there are any queries regarding the ICS.

A.3.3 Identification of the ETS

This ICS proforma applies to ETS 300 790.

A.3.4 Global statement of conformance

The implementation described in this ICS meets all the mandatory requirements of the referenced ETS.

( ) Yes

( ) No

NOTE: Answering "No" to this question indicates non-conformance to the UPT security architecture. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming.

A.3.5 Main features

Table A.1: UPT card

A1					
Item	**Features**	**Ref.**	**Status**	**Support**	**Value(s) supported**
1	Sensitive information is physically and logically protected in the card	5.1.3	m		---
2	CHV is implemented	5.2.2	m		---
3	An individual authentication key is stored in each card	7.1	m		
4	A PUI is stored in each card	7.1	m		
5	A CT value is stored in each card	7.1	m		---
6	A two pass strong authentication mechanism is implemented in the card	7.2	m		---
7	A timer value, T, can be set in the card by the user	7.1 5.2.2	m		
8	A maximum limit for the timer value, T_{MAX}, can be set in the card by the user	7.1 5.2.2	o		---
m = mandatory o = optional					

Table A.2: CHV

A11					
Item	**Features**	**Ref.**	**Status**	**Support**	**Value(s) supported**
1	Authentication can not be performed before a successful CHV is performed	5.2.2	m		---
2	CHV is implemented by a Personal Identification Number	5.2.2	m		
3	After time-out the authentication process in the card can no longer be activated without a new CHV	5.2.2	m		---
4	The card shall be blocked after 3 unsuccessful CHV attempts	7.2 5.2.2	m		---
5	The user shall be able to unblock the card with an unblocking CHV	5.2.2	m		
6	The CHV value can be changed by the user	5.2.2	m		---

Table A.3: Authentication algorithms

A12				
Item	**Features**	**Ref.**	**Status**	**Support**
1	Authentication output using the USA-4 algorithm	10.1	o1	
2	Authentication output using the TESA-7 algorithm	10.2	o1	
3	Authentication output using a proprietary algorithm	10.3	o1	
o1 = one of the options shall be supported.				

A.4 ICS proforma for card reading terminals supporting UPT

A.4.1 Introduction

The purpose of the ICS proforma is to submit suppliers and implementors with a questionnaire or checklist. This should be completed in order to state conformance with the requirements put forward in the relevant ETS.

A.4.2 Identification of the implementation, product supplier and test laboratory client

For administrative purposes the actual ICS shall identify:

- the implementation;
- the supplier or client of the test laboratory that is to test the implementation;
- the person to contact if there are any queries regarding the ICS.

A.4.3 Identification of the ETS

This ICS proforma applies to DE/NA-64006.

A.4.4 Global statement of conformance

The implementation described in this ICS meets all the mandatory requirements of the referenced ETS.

( ) Yes

( ) No

NOTE: Answering "No" to this question indicates non-conformance to the UPT security architecture. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming.

A.4.5 Main features

Table A.4: Card reading terminal supporting UPT

B1					
Item	**Features**	**Ref.**	**Status**	**Support**	**Value supported**
1	A timer function shall be implemented in the card reading terminal	5.2.2	m		
2	After time-out the access rights granted by the CHV are lost	5.2.2	m		---
3	The terminal shall not allow T in the card to be set to a higher value than T_{MAX}	7.2.1	c		
c = conditional on A1 item 8					

A.5 ICS proforma for the AE

A.5.1 Introduction

The actual ICS shall identify:

- the implementation;
- the supplier or client of the test laboratory that is to test the implementation;
- the person to contact if there are any queries regarding the ICS.

A.5.2 Identification of the ETS

This ICS proforma applies to the present document.

A.5.3 Global statement of conformance

The implementation described in this ICS meets all the mandatory requirements of the referenced ETS.

( ) Yes

( ) No

NOTE: Answering "No" to this question indicates non-conformance to the UPT security architecture. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming.

A.5.4 Main features

Table A.5: AE

C1					
Item	**Features**	**Ref.**	**Status**	**Support**	**Values supported**
1	AE supports two pass strong authentication	5.2	m		---
2	AE supports the special authentication for called party specified secure answer (use of SAPIN)	5.4	o		
3	AE supports the extra authentication for outgoing calls (use of OCPIN)	5.3	m		

Table A.6: AE support for two pass strong authentication

C11					
Item	**Features**	**Ref.**	**Status**	**Support**	**Values supported**
1	AE supports checking of blacklisted Personal User Identities (PUIs)	5.2	m		---
2	AE produces a new random value, RAND, for each new authentication	9.2	m		
3	AE accepts authentication if calculated AC' equals received AC	9.2	m		
4	AE does not allow the same authentication key to be used for users who have both one pass strong and two pass strong authentication mechanisms	10.4	m		---

Table A.7: AE support for secure answer special authentication (SAPIN)

C12					
Item	**Features**	**Ref.**	**Status**	**Support**	**Values supported**
1	SAPIN has a length between 4 and 6 digits	6	c		
2	The user is asked for SAPIN if he has subscribed to the called specified secure answer service and if there is no UPT card present	9.3	c		---
3	AE checks the SAPIN value before allowing the incoming call to proceed	9.3	c		---
4	AE checks that PIN used for weak authentication is different from the SAPIN	9.4	c		---
c= conditional on C1, Item 2					

Table A.8: AE support for outgoing call special authentication (OCPIN)

C13					
Item	**Features**	**Ref.**	**Status**	**Support**	**Values supported**
1	OCPIN has a length between 4 and 6 digits	6	m		
2	The user is asked for OCPIN if he has subscribed to the extra authentication for outgoing calls	9.3	m		---
3	AE checks the OCPIN value before allowing the outgoing call to proceed	9.3	m		---
4	AE checks that PIN used for weak authentication is different from the OCPIN	9.4	m		---

Annex B (informative): Bibliography

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

- EC DG XIII COM (1994): "128 Final-COD 288".

- EN 726-2: "Requirements for IC cards and terminals for telecommunication use: Part 2: Security Framework; Version 9.I".

- EN 726-3 (1994): "Identification card systems - Telecommunications integrated circuit(s) cards and terminals", Part 3: "Application independent card requirements".

- ISO/DIS 10202-7: "Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 7: Key Management".

- ETR 055: "Universal Personal Telecommunication (UPT); The service concept; Part 1: Principles and objectives".

- drETS 300 823: "UPT Phase 2; Functional specification of the interface of a UPT Integrated Circuit Card (ICC) and Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN) and Global System for Mobile Communications (GSM) terminals".

- DEN/NA-064011: "Functional specification of the interface of a UPT Integrated Circuit Card (ICC) and Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN) and Global System for Mobile Communications (GSM) terminals (one pass and multiple pass authentication)".

History

Document history			
August 1996	Public Enquiry	PE 112:	1996-08-19 to 1996-12-13
July 1997	Vote	V 9737:	1997-07-15 to 1997-09-12