ETSI TECHNICAL REPORT

ETR 083

July 1993

Source: ETSI TC-NA

Reference: DTR/NA-070401

ICS: 33.080

Key words: UPT, security

Universal Personal Telecommunication (UPT); General UPT security architecture

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

Foreword 7

1 Scope 9
1.1 Document structure 9

2 Introduction 11
2.1 Security 12
2.1.1 Fraud 12
2.1.2 Privacy 12
2.1.3 Service availability 12
2.2 Existing systems and UPT 12
2.2.1 Security of (existing) closed systems 13
2.2.2 Security of (UPT) open systems 13
2.3 Pre-UPT security experience 13
2.3.1 Fraud 14
2.3.2 Privacy 14
2.3.3 Service availability 14
2.3.4 Cellular phones 15
2.3.5 Conclusions 15

3 Security threat analysis 16
3.1 Introduction 16
3.2 Threats associated with UPT features 16
3.2.1 Introduction 16
3.2.2 Subscription process 18
3.2.3 Incoming UPT calls 19
3.2.3.1 Incoming UPT call procedure 20
3.2.3.2 Registration and de-registration for incoming calls 21
3.2.3.3 Secure answering of incoming calls 22
3.2.3.4 Intended recipient identity presentation 22
3.2.3.5 Called line address presentation 22
3.2.3.6 Call pick-up 22
3.2.3.7 Remote answering 22
3.2.3.8 Variable default InCall registration 23
3.2.3.9 UPT supplementary services specific to incoming calls 23
3.2.3.10 Multiple terminal registration 24
3.2.4 Outgoing UPT calls 24
3.2.4.1 Outgoing UPT call set-up and procedure 25
3.2.4.2 Follow-on outgoing call 26
3.2.4.3 Supplementary UPT features for outgoing calls 27
3.2.5 OutCall registration and AllCall registration 27
3.2.5.1 Outgoing call Registration 28
3.2.5.2 Registration for incoming and outgoing calls (linked - unlinked) 29
3.2.5.3 Multiple terminal registration 29
3.2.6 Remote registration 29
3.2.7 Service profile management 30
3.2.7.1 UPT service profile interrogation and modification 32
3.2.7.2 Advanced addressing 33
3.2.7.3 Closed UPT user group 33
3.2.8 Terminal access and UPT access device 33
3.2.9 Exceptional procedures 34
3.3 Overall threats to UPT service 34
3.3.1 Threats to personal data integrity 34
3.3.1.1 Threatened subjects 35
3.3.1.2 Identification of sensitive data within UPT 35
3.3.1.3 Identification of sensitive data processing functions 35

3.3.1.4 Location of sensitive data processing functions.................. 35
3.3.1.5 Identification of threats to personal data integrity................ 36
3.3.2 Threats to the UPT service providers systems.. 36
3.3.3 Threats to inter-network communication 36
3.3.3.1 Identification of UPT inter-network links.............................. 37
3.3.3.2 Identification of UPT inter-network procedures................... 37
3.3.3.3 Identification of threats to inter-network communication..... 38
3.3.4 Threats due to security policies 39
3.4 Classification and evaluation of threats.. 40
3.4.1 Criteria for categorisation, evaluation and classification............................... 40
3.4.1.1 Criteria for categorisation.. 40
3.4.1.2 Criteria for evaluation.. 42
3.4.1.3 Criteria for classification.. 42
3.4.2 Evaluated list of threats to UPT 43

4 Security features for UPT 50
4.1 Security features in general... 50
4.1.1 Definitions and terminology 50
4.1.2 Different aspects of security services 50
4.1.3 Authentication 50
4.1.4 Access control 50
4.1.5 Data confidentiality.. 50
4.1.6 Data integrity... 51
4.1.7 Non-repudiation 51
4.1.8 Privacy, anonymity, untraceability... 51
4.1.9 Reporting security services... 51
4.1.10 Limited service.. 51
4.1.11 Deterrent measures... 51
4.2 UPT security requirements.. 52
4.2.1 Requirements from the threat analysis.. 52
4.2.2 Service requirements on security features 54
4.2.3 Personal data integrity issues and third party protection 54
4.3 UPT specific security features... 56
4.3.1 UPT service features providing security 56
4.3.2 Security features proposed for remaining threats.. 58
4.3.2.1 Authentication of UPT user/UPT subscriber 58
4.3.2.2 Authentication of the UPT service provider to the UPT user/UPT subscriber 59
4.3.2.3 Access control to UPT access device................................ 59
4.3.2.4 Access control system to service profile information 59
4.3.2.5 Secure management of the subscription process............... 59
4.3.3 UPT security limitations 60
4.4 Security features for IN and inter-network links in general.. 61
4.4.1 Secure dialogue.. 61
4.4.2 Secure file transfer... 61
4.5 Conclusions.. 62

5 Realisation of the security architecture for UPT 63
5.1 Introduction.. 63
5.2 Security mechanisms for UPT.. 63
5.2.1 Authentication exchange mechanisms.. 63
5.2.1.1 One pass authentication mechanisms................................ 64
5.2.1.2 Multiple pass authentication mechanisms 69
5.2.1.3 Authentication Using Asymmetric Techniques.................... 72
5.2.1.4 Zero-knowledge authentication techniques 72
5.2.1.5 Biometrical procedures 73
5.2.2 Access control mechanisms.. 73
5.2.3 Service limitations.. 73
5.2.4 Bill limitations... 74
5.2.5 Confidentiality mechanisms... 74
5.2.6 Data integrity mechanisms 74
5.3 Security management aspects... 74
5.3.1 Key management... 74

5.3.1.1 Generation of authentication keys 75
5.3.1.2 Initial distribution and installation of keys 75
5.3.1.3 Use of keys within the system 75
5.3.2 Management of the subscription process 76
5.3.3 Security audit trail 77
5.3.4 Event handling 77
5.3.5 Information management 77
5.3.6 Charging administration 78
5.4 Possible UPT access devices and their use 78
5.4.1 No UPT access device 78
5.4.2 Magnetic strip-card UPT access device 79
5.4.3 One-way tone type UPT access device 79
5.4.4 Modem type UPT access device 79
5.4.5 IC cards 80
5.4.6 Compatibility with standards for IC cards 80
5.5 Summary 82
5.5.1 General remarks 82
5.5.2 Recommendations for the UPT phases 82

Annex A: Bibliography 84

Annex B: Symbols and abbreviations 85

Annex C: Requirements on personal data integrity 87

C.1 General issues 87
C.1.1 Intentions of the directive 87
C.1.2 Definitions 87
C.1.3 Personal data to be protected during collection, processing and storage 87
C.1.4 Locations of relevant data processing functions 88

C.2 Provisions for telecommunication organisations 88

History 91

Blank page

Foreword

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

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

Blank page

1 Scope

This ETSI Technical Report (ETR):

- provides an introduction to security in Universal Personal Telecommunication (UPT) systems;
- presents a threat model for UPT;
- states the assumptions made;
- recommends security levels appropriate to identified threats;
- describes potential security features;
- describes security mechanisms which offer security features;
- proposes a general security architecture for UPT;
- states the practical constraints imposed on the architecture.

User authentication is a key part of the UPT service. All likely user authentication procedures are considered, from a simple, manually input Personal Identification Number (PIN) through to a complex, IC card based procedure.

1.1 Document structure

This ETR is structured as follows:

Clause 1: outlines the scope and structure of this ETR.

Clause 2: introduces the reader to the document. The importance of UPT security is highlighted by outlining the historical fraud-related problems of mobility systems with poor intrinsic security.

The remainder of the document is ordered according to aspects of the security architecture, as outlined in figure 1.

Clause 3: identifies all threats that affect the UPT service and its environment. Some threats to security already exist in present telecommunications services. Some of these threats have no particular relevance for UPT, whilst others have **increased impact** once UPT is introduced. This document recommends counter measures to threats to the security of the UPT service. Existing general threats that remain unaltered by the introduction of the UPT service are ignored.

The relationships between the various entities involved in UPT service are described in subclause 3.1. **Specific threats** to UPT service are identified in subclauses 3.2 and 3.3. These threats are **evaluated** and **classified** in subclause 3.4, which presents a threat matrix ordered by threat class.

Clause 4: gives the **security requirements**, based on the evaluation done in subclause 3.4 and in ETR 055-3 and ETR 055-11. **Security features** appropriate to these requirements are proposed, and the **limitations** of these features are identified.

Clause 5: brings selected security features and mechanisms together into a **security architecture** for the UPT service. It discusses the following topics:

- specific security mechanisms:

  - protocols;

  - requirements;

  - limitations;

- security management aspects:
    - key management;
    - audit and event handling;
    - subscription process;
- UPT access devices:
    - DTMF devices;
    - IC cards.

Specific mechanisms are **evaluated** against the requirements of Clause 4. From this evaluation a **generic architecture** is **recommended** for all phases of UPT. Details will be described in the phase related standards on UPT security architecture and the use of IC cards for UPT.

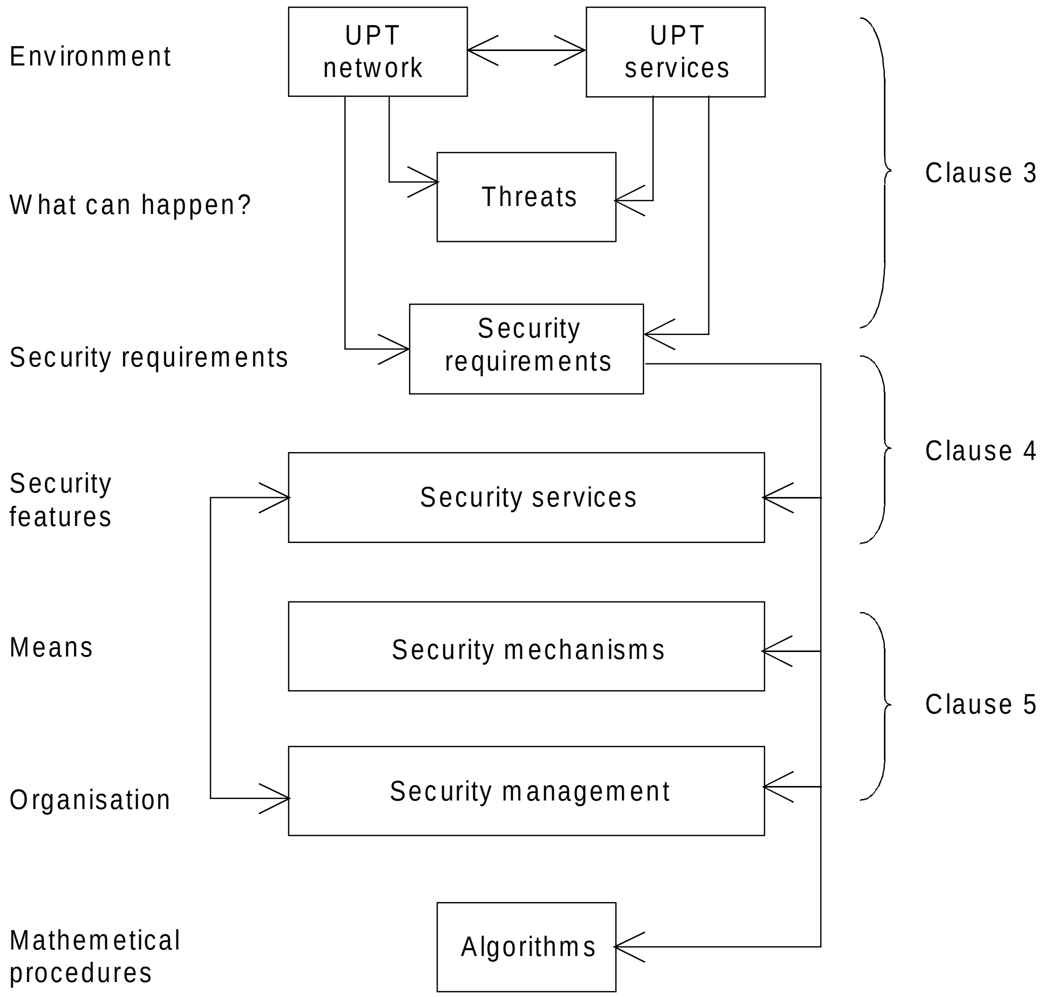


Figure 1: Aspects of UPT Security Architecture

2 Introduction

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 terminal or network capabilities and restrictions imposed by the network provider. Calls to UPT users may also be made by non-UPT users.

ETSI NA7 has defined four service scenarios for UPT which are as follows (see ETR 055-2):

- Phase 1: a restricted service based on existing Intelligent Network (IN) concepts in Public Switched Telephone Network/Integrated Services Digital Network (PSTN/ISDN) networks using Capability Set 1 (CS1) [1)];

- Phase 2: a basic service offering all essential features which should enable personal mobility in different networks, e.g. combined wired network and Global System for Mobile communication (GSM). Registration on any terminal for incoming and, as far as possible, for outgoing calls;

- Phase 3: an advanced scenario with additional and supplementary features and access to data and video networks;

- Phase 4: an evolutionary scenario which should open the service for future extensions.

Due to the flexible nature of the UPT service, UPT subscribers are very exposed to fraudulent use of their subscriptions. UPT users may, in principle, use any terminal in the world for making or receiving calls that will be charged to their account. Equally, a fraudster or malicious person could abuse the UPT subscribers account from **any terminal in the world**. It is prudent for the UPT service specifically to protect:

- subscribers' accounts [2)];

- users' responsibility to their subscribers [3)];

- users' personal details [4)];

- the integrity of the network;

- network operators' revenue streams;

- network operators' reputations;

against fraudulent or malicious attack, by any party.

The purpose of this ETR is to:

- analyse the potential security problems of the UPT service;

- specify the general UPT security architecture.

This general architecture covers all phases of UPT. For each phase there will be, in addition, a separate ETS, which will include a more detailed specification of the phase-specific security mechanisms and references to algorithms.

---

1) CS1 is the Capability Set **1** as defined in CCITT Recommendations of the Q.121x series.
2) In other words, the paying customer or consumer.
3) In the case that the UPT user is separate from the UPT subscriber.
4) Users' personal details are, in general, subject to national and international data protection legislation, agreements and treaties.

2.1 Security

Security in a UPT context refers to issues of:

- fraud;
- privacy;
- service availability.

2.1.1 Fraud

Fraud is the abuse of UPT facilities by unauthorised intruders, in particular to make chargeable use of UPT service, which charge is made against a legitimate UPT user's account. Resulting requirements are for example:

- authentication of users and subscribers;
- incontestable charging;
- auditing.

2.1.2 Privacy

Privacy is the concept that information concerning the UPT user and the UPT subscriber are not revealed to anyone who does not have legal authority to examine that information. This information includes:

- the content of communication;
- account details;
- call details;
- registration details.

2.1.3 Service availability

The ability of UPT users to receive the UPT services at any time that they wish may be limited by:

- service reliability;
- service denial.

2.2 Existing systems and UPT

Many administrations are already operating mobility services that are superficially similar to UPT, such as card calling services. It is important to note that existing services are in general **closed** systems. All of their operation is visible to the single operator. This is in sharp contrast to the **open** system specified for UPT. In such a system a single operator only has visibility of their own operation and interactions. There will be other interactions which are opaque [5)] to any single operator, but which are vital to the provision of UPT service.

[5)] Invisible.

2.2.1 Security of (existing) closed systems

Closed systems are comparatively easy to secure because:

- the extent of the system is finite;
- the trustworthiness of all elements of the system can be controlled;
- security mechanisms can have access to all information in the system;
- the operation of the full system may readily be monitored;
- any fraudulent activity may be monitored in real-time;
- accounts subject to abuse can rapidly be suspended;
- access from the outside world can be easily controlled.

2.2.2 Security of (UPT) open systems

Open systems are comparatively difficult to secure because:

- the extent of the system is unbounded (unknown);
- the trustworthiness of certain elements of the system is unknown;
- security mechanisms can not have access to all information in the system;
- the operation of the full system may not be monitored;
- fraudulent activity may only be monitored in real-time if the system is designed to pass full real-time charging [6] information;
- accounts subject to abuse can only be suspended after all extant authorisations have been revoked.

2.3 Pre-UPT security experience

Valuable lessons for UPT may be drawn from existing operators' experience of mobility services such as card calling, and mobile telephones.

---

6) Charging information includes rate information, and not simply start and stop times.

2.3.1 Fraud

In the past, administrations have operated systems such as calling cards with greater and lesser degrees of security. Fraud on these systems can usefully be characterised by the **percentage of traffic (value)** which is fraudulent:

$$\text{Fraud} = \frac{\text{traffic}_{\text{fraudulent}}}{\text{traffic}_{\text{legitimate}} + \text{traffic}_{\text{fraudulent}}} \cdot 100\%$$

In unprotected services, fraud has had typical [7] values of 50% when little or no fraud prevention has been applied. In these circumstances:

- the service operator can not make a profit;
- customers' accounts are liable to fraud;
- the credibility of the billing system is called into severe question;
- the service falls into disrepute;
- the level of fraud may vary wildly;
- anti-fraud measures have to be installed to ensure the survival of the service.

When adequate anti-fraud measures have been installed, then levels of fraud may be controlled such that fraud falls to about 1% or less. Such a service is:

- profitable;
- free of fraud for most customers' accounts;
- billable, in general, without repudiation;
- reputable [8];
- stable.

NOTE: In spite of this, the disruption caused by fraud always requires a disproportionate amount of operator's (and customers') time, money and effort. The true cost of fraud is always greater than the direct fraud itself.

2.3.2 Privacy

Pre-UPT systems have controlled problems with privacy of personal details by keeping very little personal data available on-line. The mobile systems, however, are especially vulnerable to eavesdropping [9].

2.3.3 Service availability

With the comparatively simple services offered, availability has often been primarily an equipment reliability issue. Service denial **is** an issue where there is service competition (two or more competing operators).

---

7) These figures should not be associated with any specific network or service operator.
8) Though it may have a poor reputation associated with the residual fraud.
9) Intercepting the content of communication.

2.3.4 Cellular phones

The American experience with analogue mobile phones is enlightening. That system did not have strong security designed in. As a result fraud levels were as high as 30% [10)] in the mid 1980s. This was because fraudsters exploited technical weaknesses in the American system. Anti-fraud mechanisms were introduced which reduced the level of fraud to 2%-5%. But then the levels of fraud again increased as fraudsters found new technical holes in a structurally weak security mechanism. This has resulted in yet more expensive redesigns and modifications, and damage to the service provided.

NOTE: At a fraud level of 30% some operators are likely to be bankrupted.

2.3.5 Conclusions

Existing charge card and credit card calling systems, and other mobility services, have only become commercially successful when robust security mechanisms have been applied. The lack of robust security mechanisms in the service definitions has limited the strength of the response to security problems. When security was not addressed at the outset, then the direct cost of modifying equipment and systems has been very high.

The UPT specifications **must** define appropriate security mechanisms to protect:

- UPT users;
- UPT network and service operators;
- the reputation of the UPT service;

because of the circumstances in which UPT is expected to be provided. UPT will be an open system with world-wide access, and the target value for fraud should be less than 0,1%.

---

10) This estimate is taken from "Cellular Fraud" **Cellular Business** March 1991, p32.

3 Security threat analysis

3.1 Introduction

UPT parties or subjects are assumed to be persons or company representatives that can be held responsible for actions within the UPT environment in a legal sense, or that are affected by the introduction of the UPT service.

The parties which could be involved in or related to the UPT service are listed below. Abbreviations used are noted in brackets.

- UPT user (Uus);
- UPT subscriber (Usb);
- UPT service provider (Usp);
- UPT network operator (Uop);
- Network operator (Nop): public network operator, used to pass on UPT communications;
- Line subscriber (Lsb): person who owns the access or terminal to a normal network, which passes UPT communications;
- Other Party (Otp): person who calls a UPT user or a person who is called by a UPT user;
- Intruder (Int): any party who threatens the UPT service or related features.

There is a great variety of relationships between the different UPT parties. All of the relationships have to be controlled by appropriate agreements that take the different legal situations in the various countries into consideration.

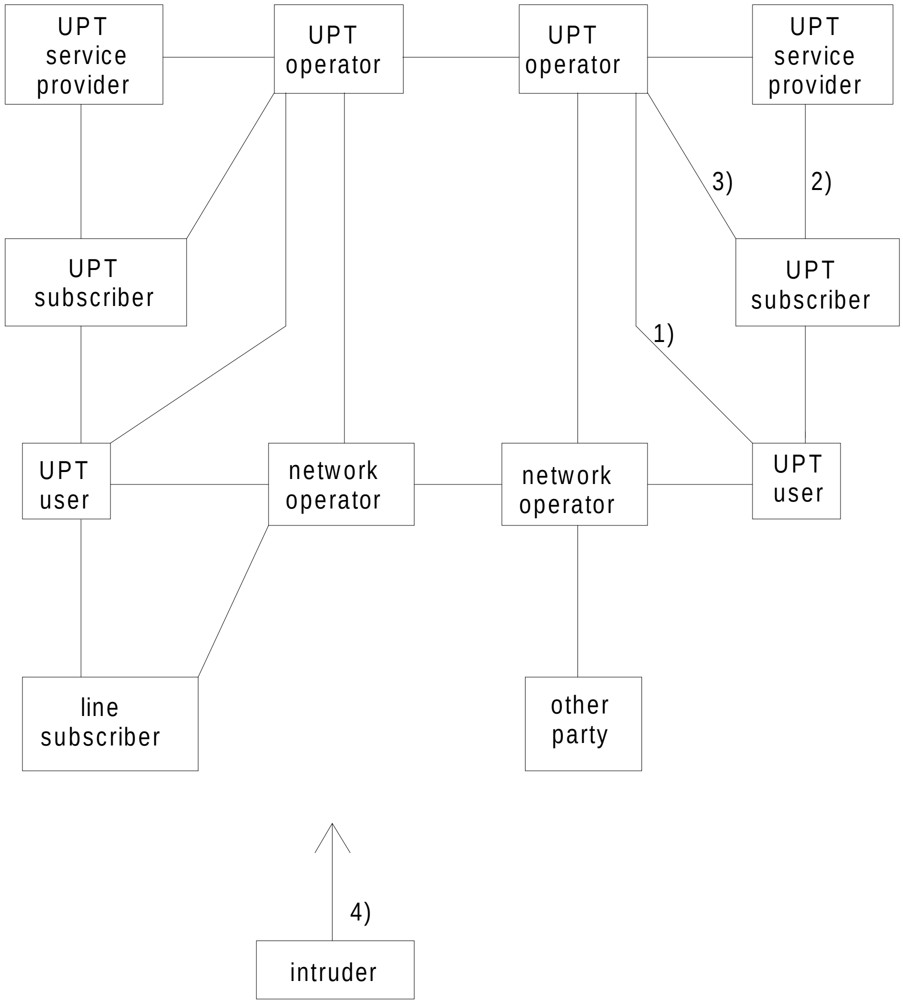
A diagrammatic representation of the relationships of the parties involved in UPT is given in figure 2. The intruder is not specifically placed within the diagram as the relationship depends purely on the type of intrusion perpetrated. Figure 2 shows all the involved parties in a UPT environment as we believe to be the situation. However, for instance, the precise role of the UPT service provider is not clear from the existing documents.

In subclause 3.2 all conceivable threats associated with particular UPT features and procedures are investigated. Subclause 3.3 covers the overall threats to the UPT service, such as the privacy of stored personal data and the subclause 3.4 contains the categorisation and evaluation of the described threats.

3.2 Threats associated with UPT features

3.2.1 Introduction

This subclause describes the threats which are associated with the UPT service and all related features. These features are separated into two groups: core features and additional features of the UPT service (see ETR 055-2 and ETR 055-10). For all features, we analysed the communications between the involved parties and the potential threats which could occur, using the relations and parties as shown in figure 2.



1) e.g. access and service profile management;
2) e.g. charging;
3) e.g. service profile management. In practice this link may be via the service provider;
4) an intruder could attack any party and any link between them.

Figure 2: Model of UPT parties and their relations

These features are implemented using the procedures defined in ETR 055-7. There are also exceptional procedures for use by other parties who may be affected by the UPT service. The threats associated with these are also described here.

We have to introduce an intruder who plays one of two different roles:

- one who actively masquerades as one of the communication parties; and

- one who passively reads information.

For each pair of parties involved and each feature, we should consider the threats posed by such an intruder.

Subclause 3.2 has the following structure. The next section analyses the subscription process (subclause 3.2.2), followed by the normal incoming UPT call (subclause 3.2.3) and outgoing UPT call (subclause 3.2.4). Next, subclause 3.2.5 deals with outgoing calls registration and combined registration and subclause 3.2.6 deals with remote registration. Next, threats to service profile management are described in subclause 3.2.7, threats to terminal access and UPT devices in subclause 3.2.8 and finally, in subclause 3.2.9 threats to the exceptional procedures are described.

3.2.2 Subscription process

The subscription process includes both subscription and de-subscription to the UPT service which, are essential management features. Between subscriber and UPT service provider, a contract will be made. This contract must include agreements about access to the service profile, by the UPT subscriber and by the UPT user, as well as agreements about charging, possible limits on remote registration, etc. Between UPT user and UPT subscriber agreement is also needed on, for instance, parameters changeable by the user and restrictions on remote accesses.

Essential management features which need to be defined (not mentioned in ETR 055-2):

- subscription;

- de-subscription.

For these features we consider the following threats.

sub1 **Unauthorised modification of subscription data by the user.**

A user could modify subscription data in the service profile without agreement with his subscriber (and maybe service provider) because of poor protection of service profile.

Threatened party: UPT service provider, UPT subscriber.

Threatened by: UPT user.

sub2 **Unauthorised modification of subscription data by the subscriber.**

Also the UPT subscriber could modify the subscription data without authorisation.

Threatened party: UPT service provider.

Threatened by: UPT subscriber.

sub3 **Fake subscription.**

An intruder could masquerade as a subscriber to a UPT service provider, probably with charging consequences. This would cover the case where a false name and address is given for billing, for instance.

Threatened party: UPT service provider, UPT subscriber.

Threatened by: intruder.

sub4 **Unauthorised de-subscription.**

A subscription could be terminated by the UPT service provider (or an intruder) without giving notice to UPT subscriber or UPT user. Consequence: denial of service.

Threatened party: UPT user.

Threatened by: intruder.

3.2.3 Incoming UPT calls

This subclause describes the threats associated with UPT features dealing with a normal incoming UPT call.

The following features, related to incoming calls, are defined in ETR 055-2 and ETR 055-10:

- core features (ETR 055-2):
    - registration and de-registration for incoming calls (incoming call procedure NA-70206);
    - secure answering of incoming calls;
    - intended recipient identity presentation;
- additional features (ETR 055-2):
    - multiple terminal registration;
    - call pick-up;
    - remote answering;
    - variable default InCall registration;
- UPT specific supplementary services (ETR 055-10):
    - UPT call forwarding;
    - password screening of incoming UPT calls;
    - call importance indication;
    - priority screening of incoming UPT calls;
    - calling party identification presentation/restriction;
    - call waiting for incoming UPT calls;
    - call hold for incoming UPT calls;
    - pre defined screening of incoming UPT calls;
    - barring of incoming calls;
    - premium charging;
    - personal charging arrangements for incoming UPT calls.

The three core features and the four additional features are analysed in the following subclauses. The UPT specific supplementary services are all in subclause 3.2.3.10.

3.2.3.1 Incoming UPT call procedure

Threats to the incoming UPT call procedure are listed below.

inc1 **Unwanted incoming calls to the UPT user.**

A UPT user could receive calls which the UPT user does not want to receive. In case of charging split, the UPT user or subscriber has to pay for these incoming calls. This problem is not UPT specific, compare with, for instance, GSM.

Threatened party: UPT user, UPT subscriber.

Threatened by: other party.

inc2 **Lack of control over who answers an incoming call.**

An incoming call is accepted at the terminal of the concerned line subscriber. If the person accepting the call is not the UPT user and the UPT user is not present, the UPT user won't get the call. Even in this case, the UPT subscriber has to pay part of the costs for the UPT call.

Threatened party: UPT user, UPT subscriber.

Threatened by: other party.

inc3 **Unknown charging to called party (possibly also to calling party).**

The called party could be charged for more than expected.

Threatened party: UPT subscriber.

Threatened by: UPT service provider.

inc4 **Incorrectness of the billing data.**

A threat to accounting is the potential incorrectness of the billing data, both to the UPT user or subscriber and to the UPT provider and network operator who charge each other for the service and network.

Threatened party: UPT subscriber, service providers.

Threatened by: service providers or operators.

inc5 **Misuse of privileges.**

Especially if the UPT user is not at the home location, the UPT subscriber has to pay the charges for the UPT user's private incoming calls. More generally speaking; incoming calls unauthorised by the UPT user's subscriber.

Threatened party: UPT subscriber.

Threatened by: UPT user.

3.2.3.2 Registration and de-registration for incoming calls

inc6 **Eavesdropping of user identity, authentication information and registration data.**

Registration data, user identity and authentication data could be eavesdropped during registration, for instance, by using a fake terminal, electro-magnetic radiation information, tapping the line, etc. Next threats could be the consequence.

Threatened party: UPT user.

Threatened by: intruder.

inc7 **Modification of user identity, authentication information and registration data.**

Registration data, user identity and authentication data could be modified during registration or by a renewed registration. This threat covers only the modification of the data.

Threatened party: UPT user, subscriber, service provider and operators.

Threatened by: intruder.

inc8 **Masquerading as a UPT user.**

An intruder could use the eavesdropped information to register on someone else's UPT number. As a consequence the UPT user will lose incoming calls, which may be forwarded by the intruder, and the matching UPT subscriber may have to pay the charges for these calls.

Threatened party: UPT user, UPT subscriber.

Threatened by: intruder.

inc9 **Registration unauthorised by the line-subscriber.**

A UPT user can register on a terminal without authorisation of the line-subscriber. The latter gets unwanted and disturbing calls.

Threatened party: line-subscriber.

Threatened by: UPT user, intruder.

inc10 **Chained registration and normal call forwarding.**

Incoming calls by (remote) registration could be forwarded to another terminal access by a non-UPT forwarding feature, activated by the line subscriber or an intruder.

Threatened party: UPT user.

Threatened by: line subscriber, intruder.

3.2.3.3 Secure answering of incoming calls

Secure answer provides the service that only the called party can answer the call, not someone else. Therefore, the incoming calls must be authenticated by the called party.

inc11 **Secure answer is not secure (charging).**

The UPT user could be impersonated by an intruder if the authentication mechanism is not sufficient. If the charging is split the UPT user may, nevertheless, have to pay for the call.

Threatened party: UPT user, UPT subscriber.

Threatened by: intruder.

inc12 **Secure answer is not secure (secrecy).**

There is a threat from an intruder to the calling party that the intruder will answer the call rather than the UPT user. So the secure answer is not secure! As a consequence, the called party is also threatened in this case.

Threatened party: calling party, called party.

Threatened by: intruder.

3.2.3.4 Intended recipient identity presentation

Presentation of the identity of the called UPT user at the alerting terminal.

inc13 **Personal information given in announcement.**

If the announcement gives information about the user's location, UPT number or other personal information, (i.e. destination), then there is a threat to the privacy of the user.

Threatened party: UPT user.

Threatened by: UPT operator.

3.2.3.5 Called line address presentation

inc14 **Loss of called UPT user's privacy.**

The identity of the called terminal address where the UPT user is registered is presented to the calling party. The UPT user may not be aware of this lack of anonymity, or be able to stop it.

Threatened party: called UPT user.

Threatened by: other party, UPT service provider, network operator.

3.2.3.6 Call pick-up

Pick-up a call at another terminal than registered. No additional threats are identified here.

3.2.3.7 Remote answering

Answering and alerting on different terminals. There are the same threats as mentioned above for incoming call.

3.2.3.8 Variable default InCall registration

This additional feature allows a UPT user to register himself at different terminals for different conditions, for instance, at his home number during the weekend and at his office number during the week. This feature is associated with the same threats as the other registration features and will clearly require the same level of authentication.

3.2.3.9 UPT supplementary services specific to incoming calls

Call importance indication

The ability of any person to make a call to a UPT user indicating that the call is important. The called party may specify (using the advanced registration for incoming call feature) that all calls marked with the important indication are to be treated differently.

inc15 **Unauthorised use of call importance indication:**

Using this service too much could lead to the UPT user picking up too many calls, and possibly paying for some of them. No specific threat.

Threatened party: called party.

Threatened by: other party.

Screening of incoming UPT calls

This feature allows a UPT user as a called party to subject all incoming calls to a screening procedure to see if they can be allowed to proceed.

This feature is a countermeasure against unwanted calls!

Premium charging, personal charging arrangements

Charging threats could occur if the calling party does not know how much has to be paid by the calling user for calling, but these threats are not UPT-specific.

Call forwarding UPT to UPT

We have the same threats as mentioned above for incoming call. With UPT call forwarding to other UPT numbers, similar threats as mentioned for registration and remote registration, could arise, but counter measures may be different. A specific threat to UPT call forwarding may be the following.

inc16 **Chained UPT call forwarding.**

A call forwarding is forwarded on another personal number, without the user performing the first forwarding being aware. Typical example: user A forwards calls to UPT user B, who has forwarded his calls to UPT user C.

Threatened party: UPT user.

Threatened by: UPT service provider, other party.

Barring of incoming calls

The UPT user may specify that no incoming UPT-calls may proceed.

inc17 **Unauthorised barring of incoming calls.**

When UPT calls are barred by an unauthorised person, the UPT user gets no UPT calls.

Threatened party: UPT user.

Threatened by: intruder.

3.2.3.10 Multiple terminal registration

Registration or de-registration at several terminals simultaneously.

In general, threats will be the same as for normal registration, but multiple registration offers more opportunities to various threats.

inc18 **Abuse of multiple registration.**

If multiple terminal registration is allowed, then a masquerading intruder may register at another terminal to receive, for instance, some of the calls sent to the UPT user.

Threatened party: UPT user.

Threatened by: intruder.

inc19 **Impersonation of a UPT service provider.**

A registering user may, in fact, be communicating with an intruder masquerading as a UPT service provider. The intruder may then obtain registration or location data from the user, or simply deny the UPT service.

Threatened party: UPT user, UPT subscriber.

Threatened by: intruder.

3.2.4 Outgoing UPT calls

This subclause describes the threats which are associated with the UPT features dealing with outgoing UPT calls. It does not describe the threats to the registration process, these are described in subclause 3.2.5.

The following features, related to outgoing calls, are defined in ETR 055-2 and ETR 055-10:

- core features (from ETR 055-2):
    - outgoing UPT call set-up;
    - follow-on facility for UPT procedures;
- supplementary UPT features (from ETR 055-10):
    - calling-UPT-user-specified secure answering of calls to UPT users;
    - connected user identity presentation;
    - completion of outgoing UPT calls to busy user;
    - screening of outgoing UPT calls.

The two core features are analysed in subclauses 3.2.4.1 and 3.2.4.2. The UPT specific supplementary services are all in subclause 3.2.4.3.

3.2.4.1 Outgoing UPT call set-up and procedure

out1 **Masquerading as a UPT user.**

A UPT user can be impersonated by an intruder. The UPT user's UPT number (and matching authentication data) could be used by someone else and as a consequence the real UPT subscriber would receive the bill for this misuse.

Threatened party: UPT user, UPT subscriber.

Threatened by: intruder.

out2 **Masquerading as a UPT-user with help of the user.**

A UPT user can knowingly provide his registration information, identity and even authentication information to another person who could use it at another place. The real UPT subscriber gets the bill for this misuse but may be able to prove that the user was, for instance, at home and not in another country.

Threatened party: UPT subscriber, UPT service provider.

Threatened by: UPT user.

out3 **Unexpected charging of a UPT subscriber.**

The UPT subscriber of a UPT user as a calling party could be charged for more than expected.

Threatened party: UPT subscriber.

Threatened by: UPT service provider.

out4 **Incorrectness of the billing data.**

A threat to secure accounting is the potential incorrectness of the billing data, both to the user and to the UPT provider and network operator who charge each other for the service and network.

Threatened party: UPT subscriber, UPT service provider, network operator.

Threatened by: UPT service provider, network operator, intruder.

out5 **Eavesdropping of user identity.**

User identity and location information could be eavesdropped during call set-up, for instance, by using a fake terminal or a terminal with memory, electro-magnetic radiation information, tapping the line, etc. If the intruder, which could also possibly be an operator or a service provider, gets information about location, called party, time of the call, etc. then the privacy and the anonymity of the UPT user is at issue (subclause 3.3 describes general aspects of privacy).

Threatened party: UPT user.

Threatened by: intruder.

out6 **Misuse of privileges by a UPT user.**

The UPT subscriber has to pay the charges of the UPT user's private calls. More generally speaking, unauthorised calls by the user.

Threatened party: UPT subscriber.

Threatened by: UPT user.

3.2.4.2 Follow-on outgoing call

A follow-on outgoing call is an outgoing call directly following a previous call and not requiring new call procedures for the next call, such as authentication. Additionally, the following threat is considered.

out7 **Modification of signalling data.**

The indication for a follow-on outgoing call has to be signalled at the end of the previous call. By manipulation of the normal end-of-call signal it may be possible for an intruder to make a call on the bill of the UPT subscriber of the previous caller.

Threatened party: UPT user, UPT subscriber.

Threatened by: intruder.

out8 **Manipulation of terminals.**

By manipulations made within the terminal the line-subscriber or an intruder could make more follow-on calls on the UPT-user's account.

Threatened party: UPT user, UPT subscriber.

Threatened by: line-subscriber, intruder.

3.2.4.3 Supplementary UPT features for outgoing calls

Screening of outgoing UPT calls

The UPT user subjects all outgoing calls to a screening procedure to see if they can be allowed to proceed.

This feature is a countermeasure against unauthorised calls!

out9 **Modification of process data.**

The UPT user or someone else could be interested in changing the result of the screening process in order to authorise inadmissible calls.

Threatened party: UPT subscriber.

Threatened by: UPT user, intruder.

out10 **Impersonation of a UPT service provider.**

A registering user may, in fact, be communicating with an intruder masquerading as a UPT service provider. The intruder may then obtain registration or location data from the user, or simply deny the UPT service.

Threatened party: UPT user, UPT subscriber.

Threatened by: intruder.

3.2.5 OutCall registration and AllCall registration

This subclause describes threats associated with registration for more than one outgoing call. This feature enables the UPT user to carry out UPT-specific procedures only once to make several outgoing calls. According to the service description (ETR 055-2), a UPT user may register to make several outgoing calls from several terminal accesses simultaneously, but only one UPT user may be registered for outgoing calls at the same terminal access.

This subclause also describes the combined registration for incoming and outgoing calls (AllCall registration), which is a combination of InCall and OutCall registration.

The following features are all defined in ETR 055-2:

- core features:
  - OutCall registration (registration for outgoing calls);
  - AllCall registration (combined registration for incoming and outgoing calls - no linkage);
  - linked registration (combined registration for incoming and outgoing calls - linked);
- additional features:
  - multiple terminal registration.

The core and additional features are analysed in separate subclauses.

3.2.5.1 Outgoing call Registration

Many threats for registered outgoing calls are similar as for single outgoing calls. These threats are described in the former subclauses, but the risks/consequences could be different in case of combined registration. Below we describe threats to the registration process for outgoing calls.

all1 **Eavesdropping of user identity and registration data.**

Registration data, user identity and authentication data could be eavesdropped during registration, for instance by using a fake terminal or a terminal with memory, electro-magnetic radiation information, tapping the line, etc. If an intruder, which could also possibly be an operator or a service provider, gets information about location, called party, time of the call, etc. then the privacy and the anonymity of the UPT user is at issue (Subclause 3.3 describes general aspects of privacy). Compare with threats on normal incoming and outgoing calls.

Threatened party: UPT user.

Threatened by: intruder.

all2 **Modification of registration data.**

Registration data, user identity and authentication data could be modified during registration.

Threatened party: UPT user, UPT subscriber.

Threatened by: intruder.

all3 **Masquerading as a UPT user.**

An intruder could use the eavesdropped data of threats mentioned before to register on a UPT number, so the UPT subscriber of this UPT number would have to pay the charges for the intruder's calls.

Threatened party: UPT user, UPT subscriber.

Threatened by: intruder.

all4 **Disclosure of called numbers via bill (privacy).**

If an ordinary line subscriber receives an itemised bill based on calls initiated from his network access, then that subscriber will receive also the numbers called by registered UPT users.

Threatened party: UPT user.

Threatened by: line subscriber.

all5 **Impersonating an already registered UPT user.**

The definition of registered outgoing calls allows the UPT user to make several outgoing calls without authentication being required for each call. The potential consequences are calls being made on other UPT subscribers accounts, or generally speaking, misuse of the UPT registration due to the lack of authentication between calls. This threat is increased, because a UPT user may be registered for outgoing calls from several terminals at the same time.

Threatened party: UPT user, UPT subscriber.

Threatened by: intruder.

all6 **Line-subscriber unaware of OutCall registration.**

A UPT user may register for outgoing calls without the line subscriber's permission. Details of the line subscriber's subsequent calls will appear on the UPT user's next itemised bill, resulting in a threat to the line subscribers privacy.

Threatened party: line-subscriber.

Threatened by: UPT user.

3.2.5.2 Registration for incoming and outgoing calls (linked - unlinked)

Registration for incoming and outgoing calls enables the UPT user to carry out UPT-specific procedures for both incoming and outgoing calls only once for more than one call. Incoming and outgoing calls for the UPT user are registered at the same terminal access.

3.2.5.3 Multiple terminal registration

No totally new threats arise, but the aforementioned threats could have increased risks and evaluation level (especially all4 and all6 linked).

3.2.6 Remote registration

Remote registration and de-registration gives the ability to register and de-register for incoming and/or outgoing calls at any terminal access using a different terminal access.

rrg1 **Unauthorised registration.**

Registration of an arbitrary personal number on a chosen terminal access, without the line-subscriber being aware. The line-subscriber could receive disturbing/unwanted incoming calls.

Threatened party: line subscriber.

Threatened by: UPT user.

rrg2 **Change contents of remote registration message.**

Someone changes the contents of a remote registration message so that communication is routed to a number other than that intended by the user. See inc7, but the impact can be different.

Threatened party: UPT user.

Threatened by: intruder.

rrg3 **Eavesdropping remote registration message.**

Someone eavesdrops the contents of a remote registration message so that he knows where the communication of a user is routed to. See inc6.

Threatened party: UPT user.

Threatened by: intruder.

rrg4 **Unintended reset.**

Someone cancels all registrations on a terminal, without the remotely registered user being aware.

Threatened party: UPT user.

Threatened by: line subscriber, intruder.

rrg5 **Use of other terminal with lower security level.**

If there are different levels of authentication on different types of terminals, which allow different services, an intruder could choose to register on a restricted terminal with lower security level in order to use a complicated terminal with enhanced features.

Threatened party: UPT subscriber, UPT user.

Threatened by: intruder.

3.2.7 Service profile management

These features mostly deal with the access to UPT users' service profiles for reasons other than registration. So to assess the threats associated with these features, we must first consider what information is held in the UPT user's service profile, as defined in ETR 055-6.

This consists of:

Part A set by the service provider at subscription time:

- UPT number;
- Personal User Identity number (PUI);
- default home location;
- service provider services;
- bearer services, tele services and supplementary services subscribed to;
- maximum number of (failed) authentication attempts;
- security options;
- any limits on remote registration;
- disallowed prefixes for incoming calls.

Part B changeable by the UPT subscriber:

- charging options/arrangements;
- credit level;
- access rights for UPT user to service profile;
- roaming restrictions;
- maximum number of terminal accesses for multiple terminal registration;
- maximum number of terminal accesses for remote registration;
- procedures allowed for UPT user.

Part C changeable by the UPT user:

C1 Service-related information:
- request for authentication for incoming calls;
- permitted callers;
- customised announcements;
- charging options;
- security options;
- activation of PSTN/ISDN/PLMN/UPT supplementary services;
- preferred language.

C2 Mobility information altered by service profile management procedures:
- simplified authentication while registered;
- override of registration by other UPT users;
- temporary home location;
- default terminal accesses;
- list of remote accesses;
- default registration duration;
- routing parameters.

C3 Mobility information altered by personal mobility procedures:
- current terminal accesses.

It is stated in ETR 055-6 that UPT service providers have access to all the service profile information without restriction, and can alter the access rights suggested above as they wish.

For each feature and each relevant pair of subjects, we consider the threats involved. In each case both passive threats (such as eavesdropping) and active threats are considered.

The following relevant features are defined in ETR 055-2 and ETR 055-10:

- core features:
  - UPT service profile interrogation;
  - UPT service profile modification;
  - UPT-specific announcements;
- additional features:
  - service personalisation;
  - UPT subscriber access to UPT service profile;
  - operator-assisted services;
- supplementary features:
  - advanced addressing;
  - advice of charge;
  - closed UPT user group;
  - barring of UPT calls;
  - private numbering plans;
  - multiparty communications.

3.2.7.1 UPT service profile interrogation and modification

The following threats refer both to the direct access and to the indirect access via an assistance operator. They include threats to personal data as defined by the CEC personal data protection directive.

spm1 **Eavesdropping information during subscription.**

There may be eavesdropping or interception of the information passing between UPT subscriber and service provider when the subscription is set up. This information will consist of the contents of Part A of the service profile as well as the subscriber's details. Subscription information may be handled electronically or on paper. Compare with threats described in subclause 3.2.2.

Threatened party: UPT user, subscriber, service provider.

Threatened by: intruder.

spm2 **Masquerading as a UPT subscriber.**

The impersonation of a UPT subscriber would allow the attacker to obtain information on the UPT subscriber's users.

Threatened party: UPT subscriber, user.

Threatened by: intruder, acting as a UPT subscriber.

spm3 **Access to user's service profile by the UPT subscriber.**

The UPT subscriber's access to interrogate the UPT user's service profile provides information about the UPT user. It is not clear whether of the UPT subscriber can access Part C of the service profile, containing authentication information and the current location of the user. Given the subservient status of the UPT user to the UPT subscriber, it is not clear that the UPT user needs protection from this access.

Threatened party: UPT user.

Threatened by: UPT subscriber.

spm4 **Manipulation of UPT user's service profile by masquerading as a subscriber.**

The UPT subscriber's access to the service profile (in particular Part B) may be abused by an attacker to manipulate information held there.

Threatened party: UPT user, subscriber.

Threatened by: intruder, acting as a UPT subscriber.

spm5 **Masquerading as a UPT user.**

The impersonation of one UPT user by intruder would allow the reading of all of Part C of the service profile. This would contain potentially valuable information on location, for instance.

Threatened party: UPT user.

Threatened by: intruder, acting as a UPT user.

spm6 **Manipulation of UPT user's service profile by masquerading as a user.**

Similarly, the illegal access as a UPT user to a service profile would allow the manipulation of the UPT user's data. This could allow an attacker to remove authentication options, for instance, or render the service unavailable to the user.

Threatened party: UPT user.

Threatened by: intruder as mentioned in preceding threat.

3.2.7.2 Advanced addressing

This additional feature would allow a UPT user to be addressed by, for instance, name and address rather than UPT number.

There may be data protection implications for a UPT network operator holding personal information such as names, addresses, profession, etc. on UPT users. The UPT network operator would have the names and addresses corresponding to UPT numbers of the UPT users on its database, and this would be valuable information to a service provider wishing to "poach" customers. These threats are generally described in subclause 3.3.

3.2.7.3 Closed UPT user group

No new threats occur. The main threat to this feature is impersonation.

3.2.8 Terminal access and UPT access device

UPT access devices are not strictly speaking UPT features, but they are likely to be an integral part of any UPT service, and the threats associated with them need to be considered. The secure management of these devices is for further study.

It is assumed that the device is used for some form of authentication.

dev1 **Unauthorised use of UPT access device.**

If the device contains authentication information, it may be stolen and used by an impersonator. Similarly, temporary access to the device may enable the authentication information to be extracted.

Threatened party: UPT user, subscriber.

Threatened by: intruder.

dev2 **Denial of service.**

Malfunctioning or difficulty in using the device may result in denial of service to the UPT user followed by loss of credibility for the UPT service.

Threatened party: UPT user.

Threatened by: UPT service provider.

dev3 **Mis-delivery of UPT access devices.**

Theft or delivery of UPT access devices to an intruder at subscription time. This should be covered by management of UPT access devices.

Threatened party: all parties.

Threatened by: intruder (may be passive).

3.2.9 Exceptional procedures

This subclause describes threats associated with the exceptional procedures specified in ETR 055-7.

Reset of registration for incoming and outgoing calls.

Reset is a countermeasure against disturbing calls to the line subscriber. It is not listed in ETR 055-7 or ETR 055-10 as a UPT core or additional feature. The necessity of implementing this feature in UPT is discussed in Clause 4.

ecp1 **Unauthorised or unintended reset.**

Normally only the line subscriber should be able to reset the terminal. Possible threats are that the line subscriber or someone else resets the terminal without the knowledge of the UPT user. It leads to denial of service to the UPT user.

Threatened party: UPT user.

Threatened by: intruder, line-subscriber.

ecp2 **Denial of service.**

There may be many UPT users registered to the same terminal. If one of the concerned users executes a reset, all other users will also be deregistered. Without any information about this deregistration, the other users' service is denied.

Threatened party: UPT users.

Threatened by: UPT user.

Suspension of registration for outgoing calls.

ecp3 **Misuse of the procedure "Suspension of registration for outgoing calls".**

Suspension of registration for outgoing calls is a way for other parties to temporarily override a registration for outgoing UPT calls at specific terminal access without identification or authentication (ETR 055-7). Another party may execute this feature without notification to the line-subscriber.

Threatened party: line-subscriber.

Threatened by: other party who uses this feature.

3.3 Overall threats to UPT service

As the UPT service encompasses a complex environment of different networks, data processing systems, data terminal equipment, users and service providers, threats have to be met that result from the use of data storage and data processing power.

These threats affect the integrity of personal data being processed in the UPT environment and also the UPT data processing systems security.

3.3.1 Threats to personal data integrity

Data that will lead to the identification of an individual or that presents information about a known individual is defined to be personal data in the broadest sense.

The general guidelines on the definition of threats to personal data integrity in this paragraph are taken from the recommendations of the European Commission COM (90) 314 SYN 287 and 288.

3.3.1.1 Threatened subjects

Personal data is related to human beings that take part in the UPT service, as there are:

- UPT subscribers;
- UPT users;
- third parties.

3.3.1.2 Identification of sensitive data within UPT

The identification of personal data to be processed within UPT can be taken from the UPT service profile as defined in ETR 055-6 which is a record containing all information related to the user that is stored permanently or temporarily within UPT systems and terminals (see subclause 3.2.7).

3.3.1.3 Identification of sensitive data processing functions

Within the UPT service the following general data processing functions will be applied:

- data transformation;
- data storing;
- data transmission.

In terms of UPT these general data processing functions will be integrated within:

- subscription procedures;
- registering and deregistering procedures;
- charging procedures;
- submission and delivery of user data.

3.3.1.4 Location of sensitive data processing functions

The locations of sensitive data processing within UPT are:

- all UPT service data bases where personal data is stored;
- all UPT terminal data bases where personal data is stored;
- all UPT links between (see figure 2):
    - UPT subscriber/user and UPT service provider;
    - UPT service provider and UPT service provider;
    - UPT service provider and network provider;
    - UPT operator and the local UPT systems.

3.3.1.5 Identification of threats to personal data integrity

Misuse or unauthorised use of personal data will violate the privacy of human beings taking part in the UPT service. It must be the objective of any countermeasure to protect the UPT user's privacy according to the data protection guidelines given by European or national laws.

Threats to personal data integrity will occur when a profile of one party's personal behaviour concerning:

- the circumstances of his business;
- his personal time management; or
- his temporary location (traceability);

is processed or recorded by either:

- any other UPT subscriber/user;
- third party;
- UPT service provider, operator;
- network operator; or
- any intruder.

The storage time of such data exceeding the minimum required for orderly charging also generates threats to privacy.

The privacy of a party using the UPT service can also be violated when the traffic channels during communication are disclosed to unauthorised individuals, entities or processes.

3.3.2 Threats to the UPT service providers systems

All systems applied or implemented by UPT service providers face a number of threats resulting from any internal systems security violations, like:

- unintended or hidden functionality;
- insufficient reliability;

that are caused by means of:

- local implementation;
- local operation;
- the domain specific security policy.

3.3.3 Threats to inter-network communication

For the exchange of data concerning operation, maintenance and charging between UPT service providers and UPT network operators, a number of procedures have to be defined for the UPT specific inter-network communication.

To define possible threats to the UPT inter-network communication it is necessary to:

- identify the concerned UPT functional entities and communication links between them;
- identify the individual procedures for each communication link against which threats can occur (specific to UPT).

This subclause does not address the communication between subscribers, users and other parties to the network. For the time being, it also does not address the communication between UPT functional entities located in the same network.

3.3.3.1 Identification of UPT inter-network links

Figure 3 illustrates typical UPT inter-network communication links that are concerned with threats and identifies the communicating UPT functional entities. More information can be found in DTR/NA-70303.

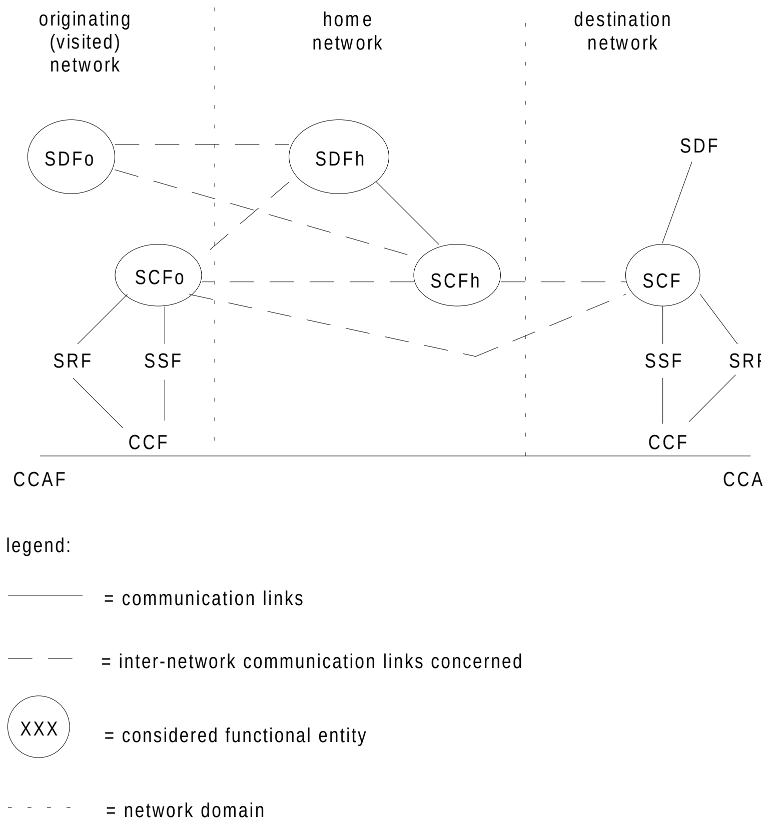


Figure 3: UPT functional entities and communication links concerned with inter-network communication threats

3.3.3.2 Identification of UPT inter-network procedures

For the time being, a detailed list of procedures cannot be deduced from the UPT documentation. Therefore, only an initial list of general procedures is given here:

SCF_o (visited) <-----> SDF_h (home)

- transfer of charging data: via file transfer.

SDF_o (visited)<-----> SDF_h (home)

- transfer of updates to home database: via file transfer.
- transfer of updates to visited database: via file transfer.

SCF_o <-----> SCF

- call handling procedures: via dialogue.
- transfer of updates to database: via file transfer.

3.3.3.3 Identification of threats to inter-network communication

All the threats analysed here are not specific to UPT but are typical for IN inter-network communication.

Each of these threats relates to one of two classes of communication:

- real-time dialogues;
- file transfers and store-and-forward messaging.

As individual procedures cannot be addressed yet, the following "general" threats are defined.

General threats to dialogues

int1 **Network connection to the wrong database.**

An unintentional situation occurs when a control point (SCP) is not connected to the right database (SDP). In this case, information from other persons could be disclosed. For instance, a UPT user has been authenticated by "his" SDP, but next a new retrieval attempt to this SDP results, because of an error, in a connection to another SDP.

Threatened party: UPT service provider, UPT subscriber, UPT user.

Threatened by: UPT service provider, UPT network operator, intruder.

int2 **Masquerading UPT entities.**

An intruder could impersonate a UPT entity (e.g. SCF, SDF, ...) for illegal direction or receipt of calls via a UPT network.

Threatened party: UPT service provider.

Threatened by: intruder.

int3 **Modification, deletion and replay of UPT "signalling data".**

An intruder could change "signalling" information in order to disturb the service or to manipulate the charging information.

Threatened party: UPT service provider, UPT subscriber, UPT user.

Threatened by: intruder.

int4 **Eavesdropping of UPT "signalling" data.**

An intruder could monitor signalling data to get information, e.g. about the location of subscribers or about information internal to the communicating UPT service providers.

Threatened party: UPT service provider, UPT subscriber, UPT user.

Threatened by: intruder.

General threats to file transfers, store and forward messages, respectively

int5 **Masquerading originator, repudiation, modification, deletion and replay of files and messages.**

An intruder could initiate one of the above actions to the intruder's, advantage especially for the manipulation of charging data.

Threatened party: UPT service provider, UPT subscriber.

Threatened by: intruder.

int6 **Eavesdropping of files and messages.**

An intruder could monitor files and messages, e.g. to get information about a subscriber's location or to disclose confidential database information of UPT service providers.

Threatened party: UPT service provider, UPT subscriber.

Threatened by: intruder.

These threats are important, but not specific to UPT and are not treated in the evaluation part of this ETR. They are, however, forwarded to a more general security investigation considering the complete IN architecture.

3.3.4 Threats due to security policies

UPT service providers are likely to have different security policies within their local domains. This may lead to different quality levels for features like the protection of personal data integrity as well as for the security mechanisms supporting authentication and access control.

A threatening situation may, for example, occur when the strong authentication and access procedures of a UPT system or an underlying network are weakened simply by the chaining of this UPT system or this underlying network with another UPT system or underlying network that applies less secure authentication and access control procedures.

Another example of threats resulting from different levels of security between different security domains is the threat to confidential user data that is to be transmitted via the chain of some mobile radio network and some conventional network.

int7 **Difference of security policies.**

Two entities may implement differing security policies, one of which undermines the security of the other.

Threatened party: UPT service provider, UPT subscriber.

Threatened by: intruder.

3.4 Classification and evaluation of threats

In the preceding subclauses a number of threats were identified, that are described very specifically in terms of the UPT features and procedures.

It is the intention of this threat analysis to point out alternative ways to find appropriate countermeasures. Therefore, the threats identified for UPT have to be categorised into more general categories, then to be evaluated according to their importance and finally classified in terms of technical and practical implications.

The distinction between evaluation and classification guarantees an independent verification of the importance of an actual threat from the security point of view, separated from the considerations that will lead to the management decision of a certain security policy whether a countermeasure to a certain threat has to be implemented or not.

3.4.1 Criteria for categorisation, evaluation and classification

3.4.1.1 Criteria for categorisation

The categorisation of threats to the UPT environment is intended to split up the UPT specific threats into more general categories of threats that will simplify the task of finding countermeasures and security mechanisms that might already exist in other environments outside UPT.

Categorisation, however, does not include any evaluation nor any classification, i.e. decision on how or when a threat will have to be met in terms of a specific security policy.

The following criteria for categorisation can be identified for UPT:

- UPT specific categories of threats;

- general categories of threats.

UPT specific categories of threats

UPT specific categories of threats are defined from the point of view of the UPT environment and the various UPT specific procedures.

UPT specific categories of threats are:

- sub: threats associated with the subscription process;

- inc: threats associated with the incoming UPT call procedure;

- out: threats associated with the outgoing UPT call set up procedure;

- all: threats associated with the OutCall and the AllCall registration;

- spm: threats associated with the service profile management;

- dev: threats associated with the terminal access and UPT device;

- ecp: threats associated with the exceptional procedures;

- rrg: threats associated with remote registration;

- int: threats associated with the inter-network communication between different UPT service providers.

General categories of threats

General categories of threats are defined as:

- ACT ACCESS THREATS;
- MNT MANAGEMENT THREATS;
- ECT EXTERNAL (INTER-) COMMUNICATION THREATS;
- ICT INTERNAL (INTRA-) COMMUNICATION THREATS;
- DPT DATA PROTECTION (PRIVACY) THREATS;
- SIT SYSTEM INTEGRITY THREATS;
- DEF UPT SERVICE DEFICIENCIES.

ACCESS THREATS (ACT) are all threats that occur when a UPT subscriber, user or any similar subject tries to get access to UPT resources. Invalid user access to UPT is one of the prime security threats. If invalid accessories can be prevented from using the system, then the subsequent security threat to the system is greatly reduced.

MANAGEMENT THREATS (MNT) are all threats to internal UPT procedures that are used to exchange, e.g. charging or routing information or to provide remote operations between UPT service providers or network providers. Threats resulting from the access of operators to system resources or those resulting from inadequate auditing are also defined to be MNTs.

COMMUNICATION THREATS are threats to the contents of any user communication (e.g. message) or threats to the information accompanying the message end-to-end. As message threats are end-to-end they will not primarily be subject to UPT specific countermeasures. They should rather be met by countermeasures of an additional value-added end-to-end security service and should, therefore, be clearly separate from other threats to UPT. Further, they have to be distinguished as:

- EXTERNAL (INTER-) COMMUNICATION THREATs (ECTs) that arise from attacks of intruders who are external to the communication, e.g. threats caused by wire-tapping, replay and misrouteing of user information or signalling data, traffic analysis; and

- INTERNAL (INTRA-) COMMUNICATION THREATs (ICTs) that arise from attacks between the communicating parties, e.g. end-to-end impersonation or repudiation.

DATA PROTECTION (PRIVACY) THREATs (DPTs) are all threats that might violate the UPT users' privacy, like those threats to the UPT users personal data that is processed and stored within UPT systems for charging, routing or other purposes of the service providers internal data processing.

These threats only have an indirect relationship to a certain call or communication of the UPT service.

SYSTEM INTEGRITY THREATs (SITs) are all threats that result from an intentional internal malfunction or another internal weakness of a UPT system.

UPT SERVICE DEFICIENCIES (DEF) are all problems that result from unintentional side effects of a UPT service.

3.4.1.2 Criteria for evaluation

The evaluation of threats identifies the degree of damage that is caused by an individual threat. Actually the evaluation represents the subjective point of view presented by the evaluator. The evaluation should assign one out of four different levels of importance to each threat:

0 = not existing or not relevant threat;

1 = minor threat;

2 = significant threat;

3 = strong threat.

A security violation will threaten one or more subjects. The threat evaluation levels have to be assigned to a specific subject. In some cases, threats must be assigned to a technical entity that, for example, may represent the "interest" of a service provider.

For the evaluation of threats, also distinctions have to be made according to their:

- IMPACT ON THREATENED SUBJECT;
- LIKELIHOOD OF OCCURRENCE;
- RESULTING EVALUATION LEVEL.

A certain evaluation level is assigned to each of these distinct evaluation criteria.

The RESULTING EVALUATION LEVEL represents a combined evaluation of an individual threat.

3.4.1.3 Criteria for classification

The classification of each individual threat represents the attitude of the implementor's or service provider's security policy towards this threat:

- how complicated it will be in a technical sense to meet a threat;
- when countermeasures will be provided.

Therefore, two criteria for classification can be identified:

- FEASIBILITY;
- IMPLEMENTATION PHASES.

FEASIBILITY criteria are distinguished as:

0 = a countermeasure is already existing;

1 = a countermeasure is easy to provide;

2 = a countermeasure is complicated;

3 = a countermeasure is hardly possible.

IMPLEMENTATION PHASEs are defined in ETR 055-2. For UPT, three implementation phases have been defined. This classification finally indicates whether a threat is intended to be met and in which phase.

3.4.2 Evaluated list of threats to UPT

Tables 1 to 8 give a complete and distinct overview of threats identified for UPT. They have to be reviewed whenever changes are specified for the UPT environment.

The results pointed out in these tables will be used for the design of the security features.

Table 1: Evaluated list of threats to the UPT subscription process

Categorisation				Evaluation 1)				Classification		
Category		Threat Descriptor	Threat-ening Subj. 2)	Impact on Threatened Subject 2)			Likelihood of Occurrence	Resulting Evaluation Level	Feasibility 3)	UPT Phase
UPT Specific	General 4)									
sub1	ACT	unauthorised modification of subscription data by the user	Uus	Usp 2	Usb 2		2	2	1	1
sub2	ACT	unauthorised modification of subscription data by the subscriber	Usb	Usp 2			2	2	1	1
sub3	ACT	fake subscription	Int	Usp 2	Usb 1		1	1	0	1
sub4	ACT	unauthorised de-subscription	Int	Uus 1			1	1	1	1

Explanatory NOTES:

1) Evaluation levels:

0 = not relevant
1 = minor
2 = significant
3 = strong

2) Subjects:

Usp = UPT service provider
Uop = UPT operator
Usb = UPT subscriber
Uus = UPT user
Otp = other party
Nop = network operator
Lsb = line subscriber
Int = intruder

3) Feasibility of countermeasures:

0 = existing
1 = easy to provide
2 = complicated/ expensive
3 = hardly possible

4) Categories of threats:

ACT = access threat
MNT = management threat
ECT = external comm. threat
ICT = internal comm. threat
DPT = data protection threat
SIT = system integrity threat
DEF = UPT service deficiencies

Table 2: Evaluated list of threats to incoming UPT call

Categorisation				Evaluation 1)				Classification		
Category		Threat Descriptor	Threat-ening Subj. 2)	Impact on Threatened Subject 2)			Likelihood of Occurrence	Resulting Evaluation Level	Feasibility 3)	UPT Phase
UPT Specific	General 4)									
inc1	DEF ICT	unwanted incoming calls to the UPT user	Otp	Usb1	Uus1		1	1	1	1
inc2	DEF MNT	Lack of control over who answers an incoming call	Otp	Usb0	Uus0		1	0	3	-
inc3	DEF MNT	unknown charging to called party (possibly also to calling party)	Usp	Usb1			2	1	1	1
inc4	MNT	incorrectness of the billing data	Usp Uop Nop	Usp2	Usb2		2	2	1	1
inc5	ACT	misuse of privileges	Uus	Usb1			2	1	1	1
inc6	DPT	eavesdropping of user identity, authentication information and registration data	Int	Uus1			1	1	2	-
inc7	ECT	modification of user identity, authentication information and registration data	Int	Usp2	Uop2	Usb2 Uus2	1	1	3	-
inc8	ACT	masquerading as a UPT user	Int	Uus3	Usb3		3	3	2	1
inc9	ACT	registration unauthorised by the line-subscriber	Uus Int	Lsb2			1	1	2	2
inc10	DPT	chained registration and normal call forwarding	Lsb Int	Uus2			1	1	2	2
inc11	ACT	secure answer is not secure (charging);	Int	Usb0	Uus0		1	0	2	2
inc12	ECT	secure answer is not secure (secrecy)	Int	Uus2	Otp2		1	1	2	2
inc13	DPT	personal information given in announcement	Uop	Uus1			2	1	1	1
inc14	DPT	loss of called UPT user's privacy	Opt Usp Nop	Uus2			1	1	1	-
inc15	ACT	unauthorised use of call importance indication	Otp	Uus0			1	0	3	-
inc16	DPT	chained UPT call forwarding	Usp Otp	Uus0			1	0	3	-
inc17	ACT	unauthorised barring of incoming calls	Int	Uus1			1	1	2	-
inc 18	ACT	abuse of multiple registration	Int	Uus1			1	1	2	2
inc19	ACT	impersonation of a UPT service provider	Int	Uus2	Usb1		1	1	2	2

Explanatory NOTES:

1) Evaluation levels:

0 = not relevant
1 = minor
2 = significant
3 = strong

2) Subjects:

Usp = UPT service provider
Uop = UPT operator
Usb = UPT subscriber
Uus = UPT user
Otp = other party
Nop = network operator
Lsb = line subscriber
Int = intruder

3) Feasibility of countermeasures:

0 = existing
1 = easy to provide
2 = complicated/ expensive
3 = hardly possible

4) Categories of threats:

ACT = access threat
MNT = management threat
ECT = external comm. threat
ICT = internal comm. threat
DPT = data protection threat
SIT = system integrity threat
DEF = UPT service deficiencies

Table 3: Evaluated list of threats to outgoing UPT calls

Categorisation				Evaluation 1)				Classification		
Category		Threat Descriptor	Threat-ening Subj. 2)	Impact on Threatened Subject 2)			Likelihood of Occurrence	Resulting Evaluation Level	Feasibility 3)	UPT Phase
UPT Specific	General 4)									
out1	ECT ACT	masquerading as a UPT user	Int	Usb3	Uus3		3	3	2	1
out2	ACT	masquerading as a UPT user with help of the user	Uus	Usb2	Usp2		2	2	2	1
out3	DEF	unexpected charging of a UPT subscriber	Usp	Usb1			1	1	1	1
out4	MNT	incorrectness of the billing data	Usp Nop Int	Usb2	Usp2	Nop2	2	2	1	1
out5	DPT	eavesdropping of user identity	Int	Uus1			1	1	2	-
out6	ACT	misuse of privileges by a UPT user	Uus	Usb1			2	1	1	1
out7	ECT ACT	modification of signalling data	Int	Usb2	Uus2		1	1	2	-
out8	SIT	manipulation of terminals	Lsb Int	Uus2	Usb2		1	1	2	-
out9	ECT SIT	modification of process data	Uus Int	Usb2			0	0	3	-
out10	ACT	Impersonation of a UPT service provider	Int	Uus2	Usb1		1	1	2	2

Explanatory NOTES:

1) Evaluation levels:

0 = not relevant
1 = minor
2 = significant
3 = strong

2) Subjects:

Usp = UPT service provider
Uop = UPT operator
Usb = UPT subscriber
Uus = UPT user
Otp = other party
Nop = network operator
Lsb = line subscriber
Int = intruder

3) Feasibility of countermeasures:

0 = existing
1 = easy to provide
2 = complicated/ expensive
3 = hardly possible

4) Categories of threats:

ACT = access threat
MNT = management threat
ECT = external comm. threat
ICT = internal comm. threat
DPT = data protection threat
SIT = system integrity threat
DEF = UPT service deficiencies

Table 4: Evaluated list of threats to OutCall and AllCall registration

Categorisation				Evaluation 1)				Classification		
Category		Threat Descriptor	Threat-ening Subj. 2)	Impact on Threatened Subject 2)			Likelihood of Occurrence	Resulting Evaluation Level	Feasibility 3)	UPT Phase
UPT Specific	General 4)									
all1	DPT	eavesdropping of user identity and registration data	Int	Uus1			1	1	2	-
all2	ACT	modification of registration data	Int	Usb2	Uus2		1	1	3	2
all3	ACT	masquerading as a UPT user	Int	Usb3	Uus3		3	3	2	2
all4	DPT	disclosure of called numbers via bill (privacy)	Lsb	Uus2			1	1	0	2
all5	ACT	impersonating an already registered UPT user	Int	Usb1	Uus1		2	1	3	-
all6	ACT DPT	line subscriber unaware of OutCall registration	Uus	Lsb2			1	1	2	2

Explanatory NOTES:

1) Evaluation levels:

0 = not relevant
1 = minor
2 = significant
3 = strong

2) Subjects:

Usp = UPT service provider
Uop = UPT operator
Usb = UPT subscriber
Uus = UPT user
Otp = other party
Nop = network operator
Lsb = line subscriber
Int = intruder

3) Feasibility of countermeasures:

0 = existing
1 = easy to provide
2 = complicated/ expensive
3 = hardly possible

4) Categories of threats:

ACT = access threat
MNT = management threat
ECT = external comm. threat
ICT = internal comm. threat
DPT = data protection threat
SIT = system integrity threat
DEF = UPT service deficiencies

Table 5: Evaluated list of threats to UPT remote registration

Categorisation				Evaluation 1)				Classification			
Category		Threat Descriptor	Threat-ening Subj. 2)	Impact on Threatened Subject 2)			Likelihood of Occurrence	Resulting Evaluation Level	Feasibility 3)	UPT Phase	
UPT Specific	General 4)										
rrg1	DPT ACT	unauthorised registration	Uus	Lsb2			2	2	2	2	
rrg2	ECT	change contents of remote registration message	Int	Uus2			0	0	2	-	
rrg3	ECT DPT	eavesdropping remote registration message	Int	Uus1			1	1	3	-	
rrg4	ACT	unintended reset	Lsb Int	Uus1			2	1	3	-	
rrg5	ACT	use other terminal with lower security level	Int	Usb3	Uus3		3	3	1	1	

Explanatory NOTES:

1) Evaluation levels:

0 = not relevant
1 = minor
2 = significant
3 = strong

2) Subjects:

Usp = UPT service provider
Uop = UPT operator
Usb = UPT subscriber
Uus = UPT user
Otp = other party
Nop = network operator
Lsb = line subscriber
Int = intruder

3) Feasibility of countermeasures:

0 = existing
1 = easy to provide
2 = complicated/ expensive
3 = hardly possible

4) Categories of threats:

ACT = access threat
MNT = management threat
ECT = external comm. threat
ICT = internal comm. threat
DPT = data protection threat
SIT = system integrity threat
DEF = UPT service deficiencies

Table 6: Evaluated list of threats to UPT service profile management

Categorisation				Evaluation 1)				Classification		
Category		Threat Descriptor	Threat-ening Subj. 2)	Impact on Threatened Subject 2)			Likelihood of Occurrence	Resulting Evaluation Level	Feasibility 3)	UPT Phase
UPT Specific	General 4)									
spm1	DPT MNT ECT	eavesdropping information during subscription	Int	Usp0	Usb1	Uus2	1	1	1	1
spm2	ACT DPT MNT	masquerading as a UPT subscriber	Int	Uus1	Usb1		1	1	1	1
spm3	ACT DPT	access to user's service profile by the UPT subscriber	Usb	Uus1			0	0	1	1
spm4	ACT ECT DPT	manipulation of UPT user's service profile by masquerading as a subscriber	Int	Uus2	Usb2		1	1	1	1
spm5	ACT ECT DPT	masquerading as a UPT user	Int	Uus2			1	1	1	1
spm6	ACT ECT DPT	manipulation of UPT user's service profile by masquerading as a user	Int	Uus2			1	1	1	1

Explanatory NOTES:

1) Evaluation levels:

0 = not relevant
1 = minor
2 = significant
3 = strong

2) Subjects:

Usp = UPT service provider
Uop = UPT operator
Usb = UPT subscriber
Uus = UPT user
Otp = other party
Nop = network operator
Lsb = line subscriber
Int = intruder

3) Feasibility of countermeasures:

0 = existing
1 = easy to provide
2 = complicated/ expensive
3 = hardly possible

4) Categories of threats:

ACT = access threat
MNT = management threat
ECT = external comm. threat
ICT = internal comm. threat
DPT = data protection threat
SIT = system integrity threat
DEF = UPT service deficiencies

Table 7: Evaluated list of threats to terminal access and UPT device

Categorisation				Evaluation 1)				Classification		
Category		**Threat Descriptor**	**Threat-ening Subj. 2)**	**Impact on Threatened Subject 2)**			**Likelihood of Occurrence**	**Resulting Evaluation Level**	**Feasibility 3)**	**UPT Phase**
UPT Specific	**General 4)**									
dev1	SIT ACT	unauthorised use of UPT access device	Int	Usb2	Uus2		2	2	1	1
dev2	SIT	denial of service	Usp	Uus1			1	1	1	1
dev3	MNT	mis-delivery of UPT access devices	Int	Uus2	Usb2	Usp2	1	1	1	1

For explanatory notes, see table 8.

Table 8: Evaluated list of threats to UPT exceptional procedures

Categorisation				Evaluation 1)				Classification		
Category		**Threat Descriptor**	**Threat-ening Subj. 2)**	**Impact on Threatened Subject 2)**			**Likelihood of Occurrence**	**Resulting Evaluation Level**	**Feasibility 3)**	**UPT Phase**
UPT Specific	**General 4)**									
ecp1	ACT	unauthorised or unintended reset	Int Lsb	Uus1			2	1	3	-
ecp2	ACT MNT	denial of service	Uus	Uus1			2	1	3	-
ecp3	ACT	misuse of the procedure 'suspension of registration for outgoing calls'	Otp	Lsb2			1	1	3	-

Explanatory NOTES:

1) Evaluation levels:

0 = not relevant
1 = minor
2 = significant
3 = strong

2) Subjects:

Usp = UPT service provider
Uop = UPT operator
Usb = UPT subscriber
Uus = UPT user
Otp = other party
Nop = network operator
Lsb = line subscriber
Int = intruder

3) Feasibility of countermeasures:

0 = existing
1 = easy to provide
2 = complicated/ expensive
3 = hardly possible

4) Categories of threats:

ACT = access threat
MNT = management threat
ECT = external comm. threat
ICT = internal comm. threat
DPT = data protection threat
SIT = system integrity threat
DEF = UPT service deficiencies

4 Security features for UPT

4.1 Security features in general

4.1.1 Definitions and terminology

Different definitions may be found for security services and security features in standards and literature. Among the more noted and stable references, the OSI Security Architecture ISO 7498-2, the CCITT X.400-series for message handling systems and CCITT Recommendation X.509 directory systems authentication framework are mentioned. The terminology used here will draw upon these references as much as possible.

4.1.2 Different aspects of security services

Security services may be mainly of physical, logical or administrative nature. Most logical security services build upon specific implementations called security mechanisms. Different security mechanisms are usually available for a specific security service. These may have different properties when it comes to implementation and strength. It is also true that one security mechanism often may be used for several security services. It is, therefore, an important step in the choice and design of security mechanisms to first identify the security services needed.

Security services may also be distinguished as to mainly have one of the following properties:

preventive (the security service is intended to make the threat impossible);

reporting (giving system manager or user information about security problems);

limiting (introducing restrictions in the system in order to limit 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 misusers restrain themselves because they know about this security service).

4.1.3 Authentication

This is the basic security service that aims at verifying the identity of a communicating party. Peer-to-peer authentication may be used for different layers in the OSI structure. Data origin authentication corroborates that the data originates from the entity claimed.

Weak or simple authentication makes use of static password technique.

Strong authentication makes use of cryptographic techniques, thereby counteracting replay attacks. In strong authentication the entity is proving that it has access to the correct algorithm and secret key previously issued to this entity. Variation in the cryptographic response, which prevents replay attacks, may be invoked by a random challenge, by time stamps or by following a sequence numbering.

4.1.4 Access control

Access control limits the ability of subjects (e.g. users, subscribers) to access data in host systems (e.g. service profiles). An access control system requires authentication of users. Access may be limited to reading, writing, modifying, deleting, etc. and may be subject to different conditions set by the administrator of the system. Black lists may be part of the access control system.

4.1.5 Data confidentiality

Data confidentiality refers to the protection of data against unauthorised reading, when it is in transit or stored. Data may be user data, signalling data, or user related data like billing or location information.

4.1.6 Data integrity

Data integrity refers to the correctness of data, i.e. the property that it has not been modified or destroyed or replayed in an unauthorised way. The security service will normally aim at detection of loss of data integrity.

4.1.7 Non-repudiation

Non-repudiation provides the receiver (or sender) with a proof that a message was sent (or received respectively) by a certain entity.

4.1.8 Privacy, anonymity, untraceability

This refers to the confidentiality of personal data, which otherwise could conflict with the need for personal data integrity. Anonymity covers the possibility for a user's identity to be unknown towards other parties and in the network. Untraceability covers the aspect not to be located geographically or tracked by other parties.

4.1.9 Reporting security services

Recording and presentation of information about actions performed by users in the system (event reporting) will often function as a supporting security service. (Users' knowledge of this fact may in turn work as a deterrent factor). Examples of reporting security services are:

- itemised billing;
- logging of actions, security audit trail;
- informative announcements, special signalling (tones) to indicate different states in the service.

4.1.10 Limited service

Limiting the service offered to users can reduce otherwise unacceptable risks. The limiting parameters may be according to many different aspects. Examples are:

- geographical area accepted for originating the service;
- roaming restrictions;
- restricted terminal types or networks (e.g. radio access not allowed);
- activity monitoring amounts per call, day, month, etc.;
- limiting the service features offered (e.g. not allowing remote registration or outgoing calls).

The possibility for third parties to reset, block or initiate suspension of (parts of) the service may also be regarded as a way to reduce risks by limiting the possible service.

4.1.11 Deterrent measures

Directly deterrent measures may often be a part of other security services or build on contractual agreements or law. Examples are:

- warning announcements at critical moments in the service;
- spreading knowledge of the existence of reporting mechanisms and audit trails;
- contractual agreements between different parties (e.g. between subscriber and user) with liability clauses;
- common law or data protection acts (e.g. about wire tapping or intrusion in data systems).

4.2 UPT security requirements

4.2.1 Requirements from the threat analysis

According to the analysis made in Clause 3, a number of threats have been evaluated at level 2 or 3 and should be met by adequate security services. These threats are listed below. Minor threats, evaluated at level 1, will, to a considerable extent, be covered by the same security services.

Several threats are connected to the privacy aspect, e.g. the importance of keeping user and subscriber data confidential and under strictly controlled access to those needing the data. Some of these threats lead to requirements primarily associated with the system integrity at the sites of the service provider and network operator. The UPT requirements are, in general, not different from the requirements on the corresponding data for other telecommunication or value added services. The nature of these requirements is as treated in the emerging European Community directives on the protection on personal data as well as in some existing national data protection acts. These requirements are discussed in subclause 4.2.3 only; they are not addressed in Clause 5 on security mechanisms, as they are not considered to be UPT specific.

Many threats will be covered by features already defined in the UPT service concept. These features are described in other UPT documents as part of the general UPT service offer. These threats and the corresponding solutions are listed in subclause 4.3.1. Also, some closely related features or precaution measures, which are normal practice in similar telecommunication services, are considered here.

The required specific security services for the main part of the threats are then proposed in subclause 4.3.2. A few remaining threats, which are hardly possible to counter with security services (in turn supported by corresponding security mechanisms) but are nevertheless judged to be acceptable to the UPT concept, are identified in subclause 4.3.3.

The following threats, as described in the threat analysis in Clause 3, are evaluated as the strongest (level 3):

inc 8 masquerading as a UPT user;

out 1 masquerading as a UPT user;

all 3 masquerading as a UPT user;

rrg 5 use of other terminals with lower security level.

The following threats, as described in the threat analysis in Clause 3, are evaluated as significant (level 2):

sub 1 unauthorised modification of subscription data by the user;

sub 2 unauthorised modification of subscription data by the subscriber;

inc 4 incorrectness of the billing data;

out 2 masquerading as a UPT user with help of the user;

out 4 incorrectness of the billing data;

rrg 1 unauthorised registration;

dev 1 unauthorised use of UPT access device.

The remaining threats were judged to be of minor importance. The following were evaluated at level 1:

sub 3 fake subscription;

sub 4 unauthorised de-subscription;

inc 1 unwanted incoming calls to the UPT user;

inc 3	unknown charging to called party (possibly also to calling party);
inc 5	misuse of privileges;
inc 6	eavesdropping of user identity, authentication information and registration data;
inc 7	modification of user identity, authentication information and registration data;
inc 9	registration unauthorised by the line-subscriber;
inc 10	chained registration and normal call forwarding;
inc 12	secure answer is not secure (secrecy);
inc 13	personal information given in announcement;
inc 14	loss of called UPT user's privacy;
inc 17	denial of service;
inc 18	abuse of multiple registration;
inc 19	impersonation of a UPT service provider;
out 3	unexpected charging of a UPT subscriber;
out 5	eavesdropping of user identity;
out 6	misuse of privileges by a UPT user;
out 7	modification of signalling data;
out 8	manipulation of terminals;
out 10	impersonation of a UPT service provider;
all 1	eavesdropping of user identity and registration data;
all 2	modification of registration data;
all 4	disclosure of called numbers via bill (privacy);
all 5	impersonating an already registered UPT user;
all 6	line-subscriber unaware of OutCall;
rrg 3	eavesdropping remote registration message;
rrg 4	unintended reset;
spm 1	eavesdropping information during subscription;
spm 2	masquerading as a UPT subscriber;
spm 4	manipulation of UPT user's service profile by masquerading as a subscriber;
spm 5	masquerading as a UPT user;
spm 6	manipulation of UPT user's service profile by masquerading as a user;
dev 2	denial of service;

dev 3 mis-delivery of UPT devices;

ecp 1 unauthorised or unintended reset;

ecp 2 denial of service;

ecp 3 misuse of the procedure "'suspension of registration for outgoing calls".

The following threats were considered to be non relevant for UPT or to be of negligible importance (evaluation level = 0):

inc 2 lack of control over who answers an incoming call;

inc 11 secure answer is not secure (charging);

inc 15 unauthorised use of call importance indication;

inc 16 chained UPT call forwarding;

out 9 modification of process data;

rrg 2 change contents of remote registration message;

spm 3 access to user's service profile by the UPT subscriber.

The latter threats may be covered by some security features, existing or introduced for UPT, but will not be explicitly discussed any more in this ETR.

4.2.2 Service requirements on security features

The following documents specifically identify requirements on security features from the service point of view:

ETR 055-4 UPT service requirements on security features;

ETR 055-11 UPT service requirements on protection of third parties.

Other NA 7 documents frequently touch upon security issues.

The requirements identified in all these documents have been considered in the working process of this ETR. The reader is referred to these documents for a more detailed study of the requirements.

4.2.3 Personal data integrity issues and third party protection

This subclause gives guidelines for the design of UPT service profiles, data processing and for the design of the contents of databases within the UPT service providers' systems. It does not contain a description of technical countermeasures against data protection threats, but rather indicates what kind of:

- UPT service;
- data processing functions;
- data stored or generated within a UPT system;
- administrative procedures and management guidelines;

may be restricted or prohibited by some national or European data protection law regulations.

Presently, European data protection laws are not harmonised, but rather, various national data protection regulations apply.

In the worst case, (national) data protection laws or regulations may result in:

- different UPT service profiles;
- different UPT data processing systems and data bases; and
- even different UPT terminals;

in the individual European countries.

Therefore, when offering a specific UPT service profile or when designing data processing functions or when defining the kind of data being generated or stored within the UPT systems, both UPT manufacturers and UPT service providers must consider the individual national data protection law. However, action has been taken on this matter by the Commission of the European Communities.

It is clear from the definitions of personal data that some UPT data and the processing of this are definitely of the nature as covered by the CEC document "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", Brussels, 15 October 1992 (CEC COM(92) 422 final - SYN 287).

The UPT service provider will here play the role of "controller", i.e. the entity or person responsible for the processing of the data and setting the objectives for this.

NOTE: The laws applicable are the national laws, and the place of establishment of the controller decides which country's national law.

The commission's proposed directive aims at removing the obstacles to free movement of personal data between all member states. However, transfer of data to other countries may only take place if the other country can guarantee an adequate level of protection.

The directive is addressed to the member states with the proposal that national laws, regulations and other provisions necessary to comply with the directive shall be brought into force by 1 July 1994.

Basic requirements in the proposed directives concern the subject's informed consent and data quality principles. For UPT it can be considered that the UPT user (the data subject) has consented, and furthermore, the data processing can be seen as necessary for the performance of a contract between the controller (e.g. UPT service provider) and the data subject. More intriguing questions arise when considering the normal (non-UPT) line-subscriber as the data subject and the processing done to this subjects' personal data (e.g. the telephone number) by the UPT service provider. Unintentional or even malicious registrations by UPT users on an unsuspecting line-subscriber's terminal certainly present a problem here. The general requirements as stated in article 23 are that the data subject suffering damage should be entitled to compensation by the controller unless the controller can prove that he has taken suitable steps to satisfy the requirements on secure processing.

It is, of course, too early to say how the requirements on secure processing will be interpreted after their transfer to national law. Subclause 4.3, however, proposes a multitude of security features which, subject to combinations and implementations, are believed to fulfil future European and national requirements.

For a more specific understanding of what possible requirements may in general be laid down on digital telecommunication services, it is clarifying to note the CEC document COM(90) SYN 288 that has been prepared for a European Council Directive concerning "the protection of personal data and privacy in the context of public digital telecommunication networks".

The legal obligations formulated in this document have been converted to a list of requirements formulated in a more technical sense so that they can serve as a guideline for UPT manufacturers and service providers. These requirements are summarised in Annex C.

It is recommended that these requirements are directly applied by manufacturers and service providers when:

- defining a national UPT service profile;

- designing the national UPT data processing functions and the contents of the national data bases; and

- when designing UPT terminal equipment;

in order to establish a common European market for UPT services, systems and terminals. The requirements in Annex C should also be checked against the national data protection law in force before they are applied.

"Personal Data" is defined to be any information relating to an identifiable individual; for UPT the relevant personal data are identified in subclause 3.2.7. The data processing functions and data bases as well as their location are identified in subclauses 3.3.1.3 and 3.3.1.4, respectively.

The most important individual data protection requirements in Annex C can be condensed to the following requirements:

1) call forwarding services are only permitted when the third party has agreed and the calling party is informed during call establishment;

2) call forwarding services can be limited to calling parties identification by request of the third party;

3) the receipt of incoming calls may be limited by the called party to the condition of a calling line identification;

4) it should be possible to block the calling line identification on a case by case basis;

5) the contents of calls may only be made accessible to third parties if all parties concerned have agreed (e.g. conference calls);

6) user information may only be stored during the time of transmission;

7) to guarantee the users, subscribers and third parties self determination concerning their personal data, any collection, processing and storage of personal data;

    - is restricted to be used only directly for the provision of the service;
    - is restricted to the shortest time range possible; and
    - must be given in advance to the knowledge and permission of the individual party concerned;

8) personal data has to be kept confidential and must not be given to other parties (e.g. service providers) without the subscribers' prior consent;

9) the collection or filtering of subscribers electronic profiles about their temporary location, personal and business circumstances etc. is not permitted.

4.3 UPT specific security features

4.3.1 UPT service features providing security

In the service descriptions of UPT some features are defined that serve as countermeasures to several of the threats identified. The threats counteracted by these features, as well as by some frequently used precautions that are normal practice in telecommunication based services, are listed here together with the relevant features. It is to be observed that these features sometimes are not sufficient measures, but that they nevertheless work in the right direction. The shortcomings of the features are at places indicated by having the features in brackets ().

Threat	**Counteracting features**
inc 1	screening of incoming calls;
inc 3	announcements;
inc 4	itemised bills;
inc 5	contractual agreements;
	service profile restrictions;
	itemised bill;
inc 8	(activity monitoring);
inc 9	(reset, blocking of registrations);
inc 10	secure answer;
inc 13	the announcements given in UPT must not contain information which by national data protection acts or EC directives may inflict on the users' personal data integrity;
inc 14	the UPT service shall be designed so that ordinary line based "called lined identity presentation" services in the network is not activated at incoming UPT calls (nor is the UPT identity presented if the UPT user makes use of the UPT supplementary service ”connected user identity restriction”);
out 1	(activity monitoring);
out 2	(service profile restrictions, itemised bill, contractual agreements between user and subscriber);
out 3	announcements on charging;
out 4	itemised bills, contractual agreements;
out 6	itemised bill, service profile restrictions, contractual agreements between user and subscriber;
out 7	(itemised bill);
out 8	(itemised bill);
all 4	itemised billing information to be distributed only to UPT subscriber, contract between subscriber and user;
all 5	(service profile restrictions, activity monitoring, itemised bill), screening of outgoing calls;
all 6	blocking, reset, announcements, special dialling tone;
all 7	secure answer specified;
rrg 1	(announcements, special dialling tone, blocking, reset);
ecp 3	UPT supplementary service "screening of outgoing calls" may be used.

Notes on some of the security features mentioned in this subclause:

Itemised bill: as can be seen, this feature plays an important role for some threats not so easily discovered or prevented otherwise. A drawback is of course that detection of problems is delayed until the receipt of the bill and is dependent on the bill being scrutinised in detail. Knowledge of the fact that itemised billing is used will give a deterrent effect, which may restrain people from some abuse or misuse of the service.

Activity monitoring this is the real-time monitoring of events associated with a user's account including some or all of: authentication, call activity, charging indications. The pattern of a user's activity may indicate that an account is subject to abuse. If strong user authentication is not used, then activity monitoring is the only fast-acting protection that a UPT user and subscriber and their UPT service provider have.

Announcements: recorded announcements play an important role for the security of the service. They must be carefully designed to enlighten users and third parties on the different states of their connection or relation with the operator/service provider. They must, however, not give away information that can infringe on the personal data integrity of users.

Reset, blocking of registration:
essential part of the UPT service. However, it does not give full protection against problems with unwanted registrations as third parties can not in general be expected to be familiar with these procedures. Suitable combinations of announcements, special dialling tones and reset/blocking may be sufficient.

Screening of incoming or outgoing calls as defined in ETR 055-10 (not for phase 1).

Secure answer authentication for the UPT user specified in order to receive a call, as defined in ETR 055-10 (not for phase 1).

Service profile restrictions:
especially different variations of **barring,** as defined in ETR 055-10 (not for phase 1).

4.3.2 Security features proposed for remaining threats

4.3.2.1 Authentication of UPT user/UPT subscriber

This security feature will counteract (or be an important part of counteracting) the following threats:

inc 8 masquerading as a UPT user (evaluated at level 3);

inc 12 secure answer is not secure (privacy) (1);

out 1 masquerading as a UPT user (3);

all 3 masquerading as a UPT user (3);

rrg 5 use of terminals with lower security (3);

spm 2 masquerading as a UPT subscriber (1);

spm 4 manipulation of user's service profile by masquerading as a subscriber (1);

spm 5 masquerading as a UPT user (1);

spm 6 manipulation of user's service profile by a masquerading as a UPT user (1).

For several of these threats weak authentication is not a sufficient solution. The threat **rrg 5** highlights the desire that there should be only one type of authentication. If there are different types, they should at least have equivalent strength.

NOTE 1: 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.

NOTE 2: All the threats evaluated at level 3 are present here and are countered only by the authentication service introduced here. This shows the importance of high strength in the authentication. This can be attained by "strong authentication", which requires the use of a device.

4.3.2.2 Authentication of the UPT service provider to the UPT user/UPT subscriber

This security feature will counteract (or be an important part of counteracting) the following threats:

inc 19 impersonation of a UPT service provider (2);

out 10 impersonation of a UPT service provider (2).

4.3.2.3 Access control to UPT access device

Two features are required for the access control to sensitive information in the UPT access device:

- authentication of user/owner towards the device;
- strong physical protection, e.g. using IC-card type of micro processor.

These features will counter threat:

dev 1 unauthorised use of device (1).

4.3.2.4 Access control system to service profile information

For the controlled access to the service profile data bases there is a need for an access control system (part of the access control will, of course, be the authentication mentioned in subclause 4.3.2.1).

This will cover threats:

spm 2 masquerading as a UPT subscriber (1);

spm 4 manipulation of user's service profile by masquerading as a subscriber (1);

spm 5 masquerading as a UPT user (1);

spm 6 manipulation of user's service profile by a masquerading as a UPT user (1).

4.3.2.5 Secure management of the subscription process

This is primarily a question of having sound and stringent procedures for administration of subscriptions, all secret information and devices as well as adequate access control systems for subscription database systems.

NOTE: Subscription may (partly) be handled via telecommunication means if there are adequate security measures (authentication, access control). More likely 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:

sub 1 unauthorised modification of subscription data by the user (2);

sub 2 unauthorised modification of subscription data by the subscriber (2);

sub 4 unauthorised de-subscription (1);

spm 1 eavesdropping of information during subscription (1);

dev 2 denial of service by device malfunction (1);

dev 3 mis-delivery of UPT devices (1).

4.3.3 UPT security limitations

Some identified threats are not covered so far. These threats may be regarded as constituting security limitations or shortcomings of the UPT service. They may be grouped in the following way.

Threats resulting from eavesdropping

Inc 6, out 5, all 1, rrg 3 are all of this type. They have been considered relevant because of the high vulnerability if authentication data is eavesdropped and can be exploited. This is, however, only true if weak (PIN-based) authentication is used. If strong authentication is used there is no threat on the authentication scheme resulting from the eavesdropping as such. The importance of having strong authentication is of course still more pronounced if cordless/mobile access to the networks is considered (except for systems with encryption on the radio link).

The additional risk of personal data being eavesdropped must be accepted as not being UPT specific or significant.

Threats resulting in nuisance for third parties

Inc 9, rrg 1 are threats associated with unwanted registrations intentional or unintentional. Remote registration may cause similar problems here. Procedures must be designed to minimise the risk of a remote registration being made to an unknowing, unwilling, line-subscriber. If, however, carried out, announcements or special dialling tones are suitable means for notifying the line subscriber. However, the line subscriber can not, in general, be expected to be aware of the procedures for resetting or blocking UPT registrations. Therefore, it should also be made clear in the UPT subscription contract that deliberate UPT registrations on terminals where the line subscriber is not explicitly consenting are not allowed (and if possible liable). If service providers or national laws require it, there could also be introduced a limitation of (especially remote) registrations to predetermined terminals.

These threats are really to be considered as inherent weaknesses of the UPT concept, but are felt to be acceptable with the use of the precautions mentioned here. Many years with normal PSTN call forwarding, which shows equivalent shortcomings, have not brought forward any severe problems of this kind.

Threats resulting in denial of service due to unintentional resets or deregistrations

Inc 17, rrg 4, ecp 1, ecp 2 are all connected with the unknown, unexpected denial of service because reset or the like was executed by someone who probably was not aware of the consequences. These are acceptable as minor threats and must be considered as part of the natural consequences for a service like this. The only "countermeasure" is for the users to be aware of the risks and act accordingly. Similar situations may equally well happen in normal PSTN call forwarding.

Signalling manipulation at follow-on

Out 7 and out 8 regard the threat that an intruder manipulates the follow-on signalling either on the line or in the terminal in order to make free calls thereafter. The threats are considered as minor and countermeasures are difficult/expensive (if problems of this kind should arise, the easiest solution will be to delete the follow-on out-going call procedure). Itemised bills partly cover the threats.

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

This subclause refers to subclause 3.3 of the threat analysis. Security features described here should protect two different classes of communication:

- dialogues;
- file transfers.

The security features discussed here are not UPT specific. They could be used also for the protection of other IN inter-network communications. For efficiency reasons, security functions should be commonly used by all IN services where possible.

Another point is the allocation of security features within the OSI structure. The following requirements were identified:

- security functions should be independent of the underlying network as far as possible;
- security protocols should be independent of the application layer protocols as far as possible.

The security features defined in this subclause are allocated between two IN/UPT entities and are of the type "secure dialogue" or "secure file transfer" The network links are part of the signalling system number 7. It should be noted that secure dialogue and secure file transfer are different security features but that they may be used on the same network link between the same (IN/UPT) entities.

The security features mentioned in the following are shown as examples. The necessary security features and mechanisms are for further study in connection with the development of a general IN security architecture.

4.4.1 Secure dialogue

Secure dialogues should consist of a mutual authentication procedure, a confidentiality service and a data integrity service on the communication link.

- security mechanisms provided:
  - mutual authentication;
  - link encryption;
  - link data integrity;
  - key management to support this.

4.4.2 Secure file transfer

Files should be protected by two security services: file data integrity and file confidentiality:

- security mechanisms provided:
  - Digital signature or MAC for file data integrity;
  - file encryption;
  - key management to support this.

Integrity protection/verification and encryption/decryption are local functions at the respective communicating entities.

4.5 Conclusions

The following security features have been identified as required for UPT:

- authentication of UPT user to service provider;
- authentication of UPT subscriber to service provider;
- authentication of UPT service provider to UPT user;
- authentication of UPT service provider to UPT subscriber;
- access control to UPT device;
- access control system to service profile;
- secure management of the subscription process.

Furthermore, use shall be made of the security features already present in the UPT service description or as considered common practice in telecommunication services:

- reporting security services (especially itemised bills);
- limited service offer (especially limitations of credit through active bill monitoring);
- UPT announcements;
- UPT exceptional procedures "reset" and "blocking";
- UPT "screening";
- UPT "secure answer";
- UPT "service profile" restrictions (resulting in limitation of service).

The threat analysis for UPT has not resulted in specific or urgent requirements for the protection of the internal security between IN entities. It is, however, recognised that with more widespread use of open network policies and more IN services to be launched, the need for a general approach to secure the IN architecture can only increase.

The threats (identified in subclause 3.3.4) to the implemented security of one operator domain due to a less stringent security policy in other co-operating domains have not resulted in requirements on security features per se. It should, however, be pointed out that a co-ordination of security levels must be negotiated between operators/service providers and formally signed by bilateral contracts or as MoU type agreements.

The threat analysis has given strong support for the view that only one - strong - authentication procedure should be standardised and used. The use of weak authentication will put heavy demands on other security services like bill limitation and active bill monitoring. Restrictions in services offered (e.g. outgoing calls not allowed) to users with only weak authentication must be considered by service providers who intend to allow this.

It can be concluded that countermeasures to all threats evaluated at level 2 or 3 have been identified. The few remaining threats are only of level 1 or less and can be accepted as such.

Recommendations on how to implement the chosen security features by security mechanisms are given in the Clause 5.

5 Realisation of the security architecture for UPT

5.1 Introduction

In order to get a security architecture for UPT, we performed in Clause 3 a threat analysis, considering the UPT network as well as the UPT services. We also dealt with political and technical restrictions. In Clause 4, the security requirements are established in order to determine the security features.

This Clause, goes into more detail and shows how the security features can be accomplished. Hence, which mechanisms shall be implemented and which security management features are suitable need to be decided. These choices will depend on the several implementation phases of UPT.

The specification of protocols and algorithms is not part of this ETR. This will be done in other documents, according to the UPT phases.

In subclause 5.2, we discuss those security mechanisms that might supply possible solutions for the UPT security features named in Clause 4. We consider especially authentication mechanisms, access control mechanisms, and on-line mechanisms supporting secure billing. We inspect also mechanisms that prevent against eavesdropping and modification of data (confidentiality mechanisms and data integrity mechanisms).

However, the mechanisms have to be supplied by a security management. In subclause 5.3, we consider how to handle cryptological keys and other user-related data (key management, personalisation of security devices), how to react in case of misuse (security audit trail, event handling), what information and announcements have to be transmitted to UPT users and other parties (information policy), and how billing can be made secure by off-line mechanisms (charging administration, black lists).

In order to evaluate the described mechanisms, we have to consider the UPT access devices that are available in the several phases of UPT. For instance, the use of IC cards (smart cards) gives us more possibilities to introduce authentication mechanisms with multiple pass handshakes, in contrast to e.g. DTMF devices. This subject will be dealt with in subclause 5.4.

Subclause 5.5 will give the result of the preceding considerations. The evaluation criteria for the selection of security mechanisms and management procedures will be summarised, and we will propose deliberate choices for the several UPT phases. Furthermore, the relationship between the required security features and their realisation will be summarised there.

5.2 Security mechanisms for UPT

5.2.1 Authentication exchange mechanisms

There exist many mechanisms for authentication. The choice depends on the technical possibilities on one hand, and on the required security level on the other hand. The possible mechanisms reach from simple authentication (e.g. PIN), via enhanced one pass authentication (e.g. PIN and time stamp with encipherment), up to asymmetrical crypto-mechanisms and zero knowledge proofs. Biometrical procedures may also be considered for some special purposes.

The simple PIN mechanism supplies only weak authentication, whilst the enhanced mechanisms using variable authentication codes supply strong authentication (cf. Clause 4). Multiple pass authentication mechanisms enable also mutual authentication.

The more enhanced mechanisms need the use of advanced technologies like smart cards. Especially for UPT phase 1, we are not able to use more than an enhanced one pass mechanism. Hence we will start with the study of one pass authentication mechanisms. Phase 3 and possibly phase 2 will allow the implementation of multiple pass handshake protocols, supplemented e.g. by smart cards.

It is the task of the security management to exchange authentication data between visited service providers and the home service provider.

5.2.1.1 One pass authentication mechanisms

a) Simple PIN

The simplest authentication mechanism is the PIN. Each user gets a unique identifier (name or number) which might be not secret and a PIN that the user has to keep secret. It is proposed for identification, to use a private Personal User Identity (PUI) instead of the publicly known UPT number. This would render disclosure of UPT user privacy (see subclause 5.2.5) as well as denial of service by intentional blocking (see below) more difficult.

Either the user or the user's UPT access device has to send the PIN to the UPT system (SDF). A positive (negative, respectively) acknowledgement has to be given by the system after the PIN has been verified and accepted (rejected, respectively).

The security policy decides the principal usability and the possible length of PINs. Longer PINs are more secure against guessing than short PINs, however, they are less user-friendly (more difficult to remember), and they extend the transmission time. Depending on the UPT access device, the use of longer PINs might be possible.

Within UPT, the allowed character set for PINs normally consists only of numbers. If a UPT access device is used, alphanumerical signs and the usage of passwords might also be a good solution.

A user-friendly procedure for change of PINs should be offered by the service providers.

If simple PIN is used, the following problems occur:

- **replay:** it may be possible to get the PIN by eavesdropping and thus to replay authentication data;

- **guessing:** a countermeasure against trying all possible PINs belonging to a certain user is blocking of the user's access after a given number of incorrect PIN inputs. However, an attacker could take one arbitrary PIN, and try to find a user identifier (UPT number) belonging to it. Proceeding like this, the attacker would not be blocked after incorrect PIN inputs;

- **denial of service:** if a user's access can be blocked, e.g. after a number of incorrect PIN inputs, an attacker might block one or many user's accesses simply by input of arbitrary PINs. The use of a secret PUI instead of the public known UPT number for identification would help against this threat with regard to a determined person. It protects arbitrary PUIs only if it is very difficult to guess a valid PUI (this can be provided by a sufficient redundancy).

There exist some proposals that suggest how to solve these problems. They are discussed below.

b) Use of a cryptological function without variation

In an attempt to protect the system against eavesdropping, PINs could be enciphered on the communication line by encryption or by a one-way function.

This simple encipherment of a PIN for transfer from the user to the remote UPT service operator does not help against replay, since the transmitted authentication data would always be the same. This needs additional mechanisms that produce unforeseeable authentication data on the transmission line. This can be done by use of time stamps or counters (see below) or by challenge and response procedures (see subclause 5.2.1.2).

However, simple encipherment renders replay more difficult, since the eavesdropper has to enter the enciphered data directly to the transmission line. Simple encipherment does not help prevent guessing and denial of service.

c) blocking and unblocking of user access

- PIN authentication of user to the system.

The above mechanisms do not prevent guessing of PINs. A possible way to prevent guessing is to block a user's access after a given number of incorrect PIN inputs. However, this gives an attacker the possibility to enforce a denial of service. The attacker only has to enter the UPT number of a UPT user and some arbitrary PINs. This threat could be reduced if, for identification, a secret PUI is used instead of the UPT number.

If a user access is blocked, the user has to have the ability to unblock it. An off-line procedure, where the user has to call the UPT service operator, is not very user-friendly. The user or the subscriber should be able to unblock on-line by use of a second Special PIN (SPIN) which may be longer than the normal PIN.

A better solution is in any case, normally not to block user access. If one of the procedures discussed below (time stamp, counter, TAN) is used, together with the possibility of black lists (e.g. for stolen UPT devices), blocking seems indeed not to be necessary. Only in cases of severe misuse should user access be blocked (see subclause 5.3.4 event handling). In the case of such an event, unblocking has to be done by intervention of the UPT service operator.

However, there is another possibility to prevent guessing. After the first PIN input failure, the user's access should be blocked for (e.g.) 1 second, after the second failure for 2 seconds, etc. after the n-th failure for 2^{n-1} seconds. This procedure would render guessing nearly impossible; e.g. after 10 failures, the attacker has to wait 17 minutes, after 20 failures about 12 days, and after 30 failures about 34 years. On the other hand, if an attacker wants to block a user's UPT access (denial of service), he needs a time at least half as long as the access would be blocked.

Hence, the latter procedure would help against guessing the PIN belonging to a particular user as well as against denial of service by blocking. However, it does not prevent guessing of an arbitrary access (fixed PIN, variation of UPT number) if a simple PIN is used for authentication. This problem can only be solved by enhanced authentication procedures (see below) or by enhanced event handling procedures (see subclauses 5.3.3 and 5.3.4).

- Local PIN authentication of user to his UPT access device

If a personalised UPT access device is used, a device holder verification shall be required before any activation of the device. This shall prevent a possible misuse of the device by unauthorised persons. In most standards, this is implemented by a Local Personal Identification Number (LPIN), that is managed within the device (e.g. an IC card). Hence, the user-to-system authentication consists of two steps: user-to-device authentication; and device-to-system authentication. The security of the entire authentication results from the security of each of the two steps.

NOTE 1: Instead of the LPIN, other mechanisms like fingerprints are possible.

NOTE 2: The device holder verification could also be realised within the UPT system. The advantages would be that there would be a direct link between the user and the system and that the operator had the control over the entire authentication. However, the LPIN management inside the device has some major advantages: the user or subscriber can easily change the LPIN (or activate a new LPIN by use of the SPIN), especially if he becomes suspicious that someone got knowledge of it; the LPIN is known only to the user; the LPIN is never sent over the network. See also subclause 5.3.2.

NOTE 3: The LPIN shall be implemented in a physically protected way (see subclause 5.4).

If a LPIN is used in order to authenticate the user to his UPT access device, the device should be blocked after a given number of LPIN input failures. This would protect from misuse of stolen devices.

An unblocking by use of an SPIN should be possible, since LPIN input failures could also be done unintentionally (e.g. by playing children).

d) Variation of the authentication parameters

In order to prevent replay, the one pass authentication protocol might use variable Authentication Codes (ACs). These ACs should be verifiable by the UPT system, but they have to be non-predictable and non-replayable. This procedure requires the use of a UPT access device. A fixed local PIN should authenticate the user to his device.

Since guessing of the AC is very unlikely (depending on the length of the AC) and would enable only one single unauthorised access, blocking after authentication failure is not recommended. Hence, the use of ACs eliminates also the problem of denial of service by intentional blocking.

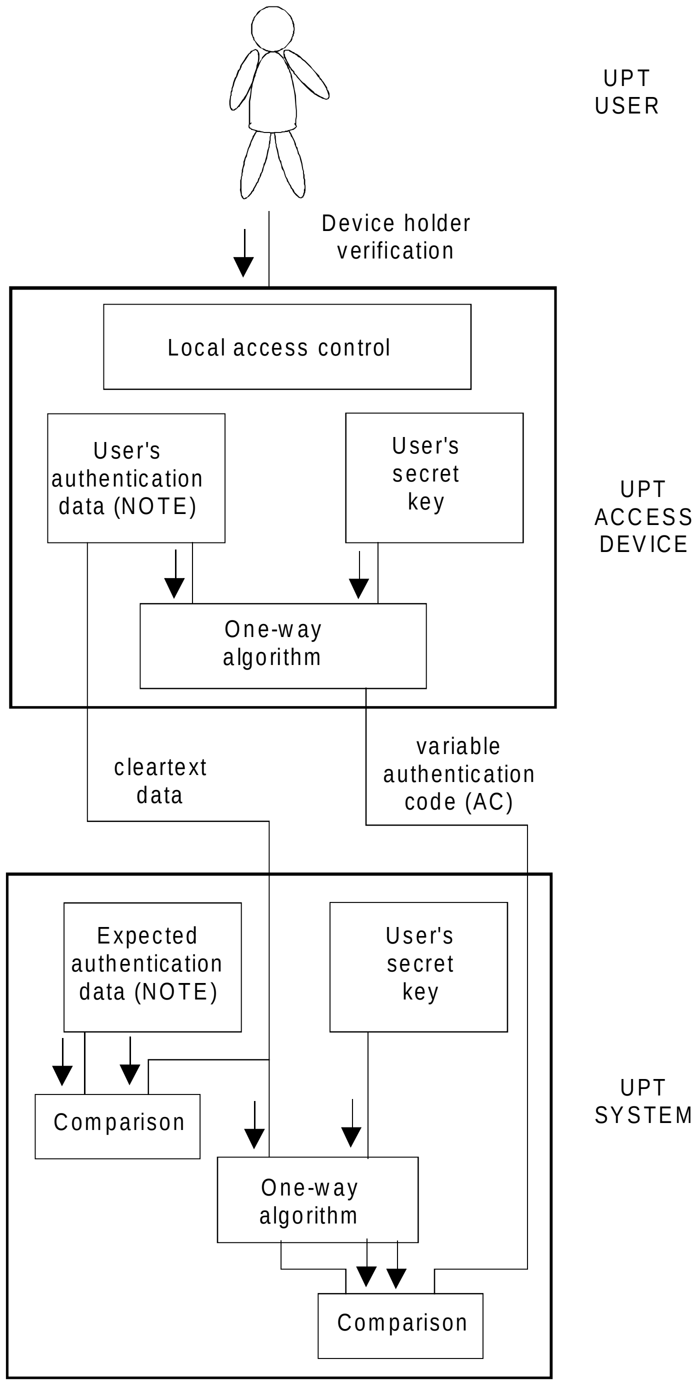
The authentication data might be time stamps, sequence numbers, random numbers, or a combination of these possibilities. For authentication of the user identity, they are (one-way) enciphered, and the result, called variable Authentication Code (AC), is sent together with parts of the cleartext to the UPT system, where verification will be done. The data flow is illustrated in figure 4. Special solutions for ACs are described in the following.

NOTE: The authentication data may be concatenated to information data (e.g. the UPT number or PUI, respectively, the "LPIN" if checked in the system, and user commands) before enciphering, in order to achieve data integrity as well (see subclause 5.2.6).

- Time stamp

If there is a clock in the UPT device or in the UPT terminal, the authentication data could be the actual time stamp. The recommended reference clock is Co-ordinated Universal Time (UTC).

Some problems arise with the use of time stamps: the clocks in the access devices need a reliable power supply with a long life time; they have to be synchronised with the clock in the UPT system (e.g. by manual adjustment by the user). These problems make the integration into smart cards very difficult.



NOTE: e.g. sequence number.

Figure 4: Variable AC

Assuming that 100 % synchronisation of clocks is not possible (especially if the transmission delay is very large), time windows have to be specified. To avoid fast replay attacks within the same window, the additional use of sequence or random numbers may be necessary. This procedure prevents replay since the authentication data changes after each time interval, and prevents guessing. Time stamps offer protection against an attack in which a series of authentications is recorded directly from a UPT access device and then used for masquerade. Additionally, time stamps allow for the detection of forced delays.

- **Counter**

If the UPT device contains a counter, the authentication data could be a sequence number which is increased after each authentication.

It has to be considered how to synchronise the counter of the UPT system with the counter of the UPT device after authentication failures. A possible solution is that the UPT system does not check that the actual sequence number has increased by exactly 1, but rather that it has actually increased. The UPT system should also check, if the sequence number has increased within a reasonable range that might depend on the failure probability. In the following, we propose an authentication procedure in detail.

Let f_K be a one-way encipherment algorithm, where K is a secret cryptological key, agreed between the UPT user and the UPT service provider. Let M = { 0, 1, 2, ..., m } be the set of possible sequence numbers, and n_0 be the initial sequence number (this value might be chosen by the service provider). Let d be the range of tolerance; this value should be very small in comparison to m (e.g. $m = 10^{20}$, $d = 10^{3}$).

The UPT number (or PUI, respectively), the actual sequence number n_a and the authentication code $f_K(n_a)$ are sent to the UPT system. There the function f_K is applied to the received sequence number, and the values are compared. By this procedure, the authentication is done by checking that the device has the correct secret key. Furthermore, it is checked whether n_a is within the range { n'_a, $n'_a + 1$, ..., $n'_a + d$ } where n'_a is the actual (UPT user related) counter value stored in the UPT system.

> NOTE: In order to save transmission time, it is sufficient to send only the least significant digits of n_a instead of the whole number. In this case, the system has to supplement the number before the next steps are executed.

If the result is positive, the system counter n'_a is replaced by $n_a + 1$.

If the sequence number is out of range, the UPT user is given a corresponding message. The user access should not be blocked and the user may try again, since the reason could be e.g. a transmission error. If the user receives this message several times, the user should call the UPT service provider in order to check the reason. The UPT service provider may decide to resynchronise the counter in the system (e.g. if the sequence number is not too much out of range). He may also require the subscriber to send the UPT access device (or the smart card) back to him, and to give him a new device with a new initial sequence number. It should **not** be possible to resynchronise the UPT access device.

If the comparison is negative, the counter n'_a should not be updated (otherwise it would be possible for an intruder to enforce an increment of the counter out of range).

In any case, the counter n_a in the UPT device is increased by 1 after each sending out of the authentication information.

This procedure helps prevent replay since the authentication data change after each authentication. A counter offers weak protection against an attack in which a series of authentications is recorded directly from a UPT access device and then used for masquerade. The masquerade fails as soon as the UPT access device is used directly for authentication. If the AC is large enough (say 32 bits), guessing is in practice a completely unrealistic attack.

- Transaction numbers

Another solution is to give the users a list of pseudo-random Transaction Numbers (TANs). This is implemented e.g. in the German videotex banking. Encipherment of the TANs would not be necessary.

A disadvantage of this procedure is the handling of TAN lists by the users as well as by the UPT system. The computation of the TANs by some procedures (which is somehow a generalisation of the above discussed mechanisms using time stamps or counters) could help against this disadvantage. However, it remains the problem of on-line initialisation and re-synchronisation after failures.

This procedure overcomes replay since the authentication data change after each authentication. Furthermore, it prevents guessing if the TAN values are large enough.

TANs could be useful for unblocking ("second PIN") and for service profile access.

5.2.1.2 Multiple pass authentication mechanisms

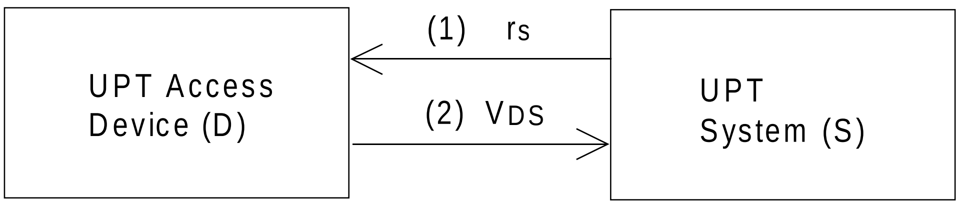
If it is possible to use two-way transmission, challenge and response authentication protocols can be implemented. These protocols run between the UPT access device (e.g. smart card), the UPT system, and possibly a trusted Third Party (TP). Additionally, a local PIN should authenticate the UPT user to his UPT access device.

Multiple pass authentication mechanisms can be used for unilateral authentication as well as for mutual authentication. In particular, the mechanism described above using variable authentication codes is suitable for mutual authentication. It is only necessary to do the same procedure in the other direction, too, using corresponding parameters (e.g. the next sequence number).

The following multiple pass authentication mechanisms are based on ISO/IEC CD 9798-2 (entity authentication using symmetric techniques). One of them may be implemented after UPT phase 1.

- Mechanisms without trusted third party

The mechanism proposed by ISO is described in figure 5.



r_S = random number
V_{DS} = f (K_{DS} ; r_S)
f = cryptological function
K_{DS} = secret key

Figure 5: Two pass authentication with random number

(1) The UPT system **S** sends a random number $\mathbf{r_S}$ to the user's UPT access device **D**.

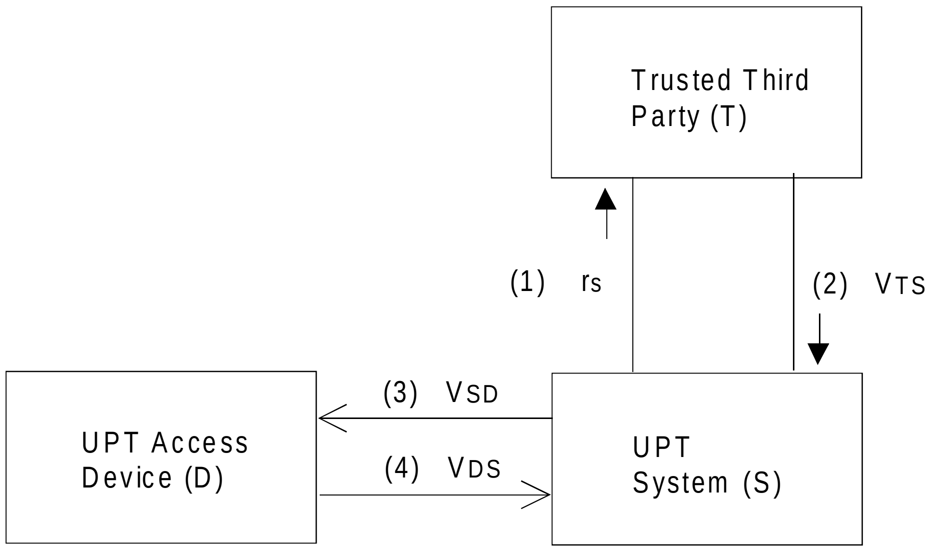
(2) **D** encrypts $\mathbf{r_S}$ by means of a cryptological function **f** and a secret key $\mathbf{K_{DS}}$, agreed (at subscription time) between **D** and **S**, and sends it to **S**. Then, **S** checks if **D** has used the correct key and the correct random number.

This procedure is, in principle, used in GSM. Furthermore, it is supported by the IC card architecture specified in prEN 726-3. In visited networks or when a trusted third party holds the authentication information, the UPT system can receive the needed authentication parameters on request. It could correspondingly also be used for authentication of the system to the device and hence mutual authentication.

- **Mechanisms with trusted third party**

The concept of a trusted third party makes authentication possible without sharing a secret key between the concerned entities prior to the authentication process. These entities have, however, to share each a common secret key with the trusted third party. In UPT, the trusted third party could be, for instance, the home service provider, whilst the UPT user roams at a visited UPT service provider.

The mechanism described in figure 6 authenticates the UPT access device to the UPT system.



r_S = random number
V_{TS} = f (K_{TS} ; r_S , K_{DS} , f(K_{TD} ; r_S , K_{DS})) = F (K_{TS} ; r_S , K_{DS} , V_{SD})
V_{SD} = f (K_{TD} ; r_S , K_{DS})
V_{DS} = f (K_{DS} ; r_S)
f = cryptological function
K_{XY} = secret keys

Figure 6: Four pass authentication

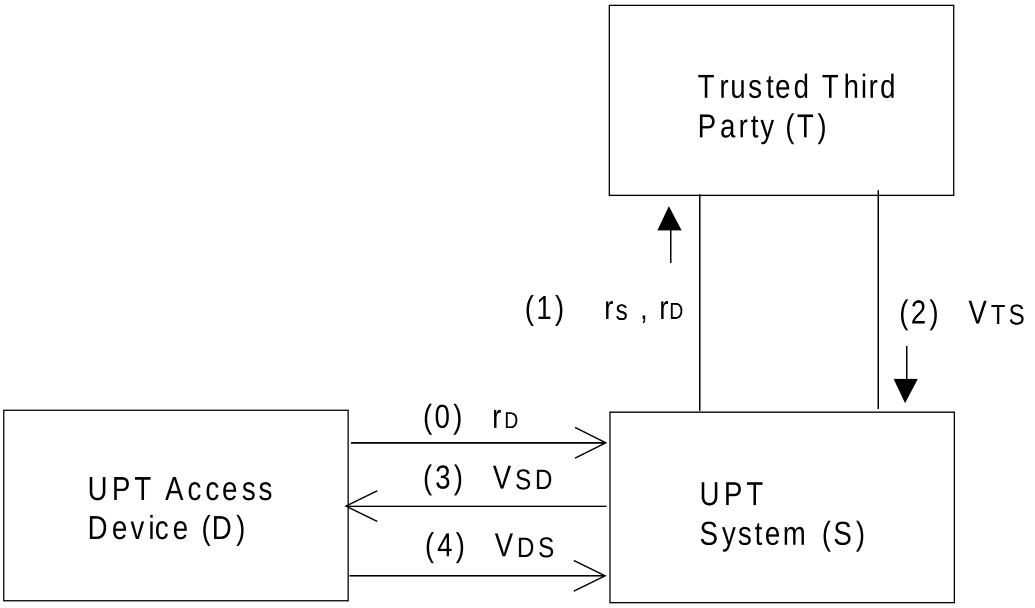
(1) The UPT system **S** sends a random number $\mathbf{r_S}$ to the trusted third party **T**.

(2) **T** generates a session key $\mathbf{K_{DS}}$ and encrypts it together with $\mathbf{r_S}$ by means of a cryptological function **f** and a secret key $\mathbf{K_{TD}}$, agreed (at subscription time) between **T** and **D**. Then, **T** encrypts the result $\mathbf{v_{SD}}$ together with $\mathbf{r_S}$ and $\mathbf{K_{DS}}$ by means of **f** and a secret key $\mathbf{K_{TS}}$, agreed between **T** and **S**, and sends it to **S**. Then **S** checks if **T** has used the correct key $\mathbf{K_{TS}}$ and the correct random number $\mathbf{r_S}$.

(3) **S** sends $\mathbf{v_{SD}}$ to **D**.

(4) **D** decrypts $\mathbf{v_{SD}}$ and gets $\mathbf{r_S}$ and $\mathbf{K_{DS}}$. Then **D** sends $\mathbf{v_{DS} = f (K_{DS} ; r_S)}$ to **S**. Finally, **S** checks if **D** has the correct key and the correct random number.

In the procedure described in figure 7, the UPT access device starts with an extra random number that has also to be handled by the three parties. Hence, the system will be authenticated to the device, too (mutual authentication).



r_S, r_D = random numbers

V_{TS} = $f\,(K_{TS}\,;\,r_S\,,\,K_{DS}\,,\,f(K_{TD}\,;\,r_S\,,\,r_D\,,\,K_{DS}\,)\,) \;=\; f\,(K_{TS}\,;\,r_S\,,\,K_{DS}\,,\,V_{SD}\,)$

V_{SD} = $f\,(K_{TD}\,;\,r_S\,,\,r_D\,,\,K_{DS}\,)$

V_{DS} = $f\,(K_{DS}\,;\,r_S\,)$

f = cryptological function

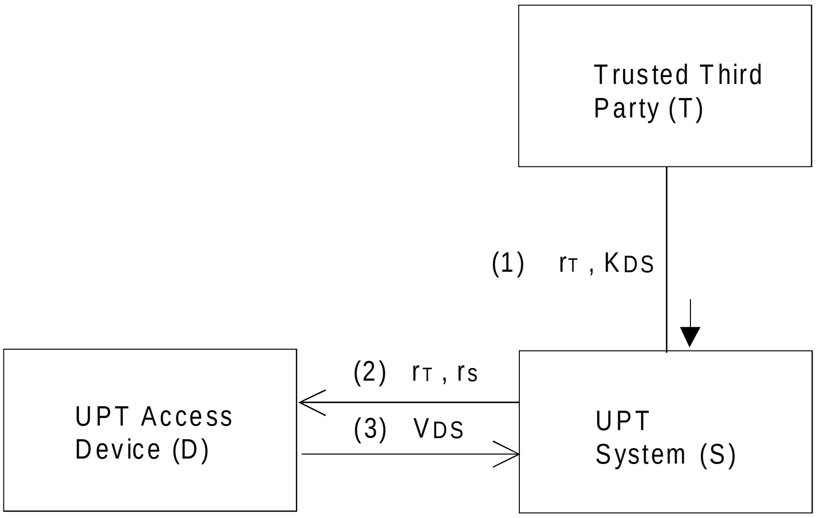
K_{XY} = secret keys

Figure 7: Five Pass Authentication

It might be recommended to use, additionally, time stamps or a counter and to send the relevant addresses in a protected form, in order to prevent misuse (forced delay, reflection).

Depending on the decision if mutual authentication is recommended, one of these two procedures could be appropriate for UPT phase 2 or later. An advantage is that they generate and distribute also a session key for the communication between the device and the UPT system. However, this may also be a problem, since the support of encryption could complicate the international acceptance. Furthermore, these procedures are not supported by the IC card architecture specified in prEN 726-3.

The authentication procedure described in figure 8 which does not support encryption is used by DECT. It can easily be extended to a mutual authentication. It can be implemented on an IC card, using the standard prEN 726-3.



r_T, r_S = random numbers
K_{DS} = f (K_{TD} ; r_T) = session key for authentication
V_{DS} = g (K_{DS} ; r_S) = authentication value, to be checked by S
f = key distribution function
g = internal authentication function
K_{TD} = secret key stored at T and D

Figure 8: DECT like Authentication

5.2.1.3 Authentication Using Asymmetric Techniques

The use of asymmetrical algorithms has many advantages, especially concerning key management. The above mentioned mechanisms can, in principle, also be used with asymmetrical algorithms. Protocols especially specified for asymmetrical techniques are described in CCITT Recommendation X.509 (the Directory - authentication framework) and ISO/IEC CD 9798-3 (entity authentication using asymmetric techniques).

Depending on the technical evolution, asymmetrical techniques might be used in UPT phase 2 or later. Details are for further study.

5.2.1.4 Zero-knowledge authentication techniques

Using zero-knowledge methods, entity authentication can be achieved without the claimant having to pass any knowledge at all to the verifier.

The features of zero-knowledge authentication techniques include the following:

- the computations involved in the authentication procedure are much simpler than, say, a public key system like RSA;
- the actual messages passed are short and to the point, unlike many public key and symmetric key systems which send rambling combinations of concatenations and encryptions;
- the verifier can decide how convinced he wants to be (by asking as many rounds of questions as he likes), unlike key systems where the remaining risk is predefined by the key length. To provide evidence beyond reasonable doubt that the claimant is who he says he is can require many rounds of questioning (i.e. well into two digits). It is the verifier's responsibility to ask enough questions;
- a suitable, tamper-proof random number generator should be used. Pseudo-randomness may not be good enough, and some analogue device may be necessary.

Zero-knowledge authentication techniques cannot be implemented before UPT phase 3. Details are for further study.

5.2.1.5 Biometrical procedures

Biometrical procedures are not yet mature for use in public networks. The probability that authorised persons are not accepted and unauthorised persons are accepted is still too high. Additionally, procedures like fingerprints would possibly not be accepted by users. If there existed secure techniques for voice recognition, this could be acceptable for telephone applications.

It has to be recognised, however, that the digital representation of a biometrical attribute is in principle constant and hence, without e.g. added challenge and response, in many respects equivalent to a fixed PIN.

Biometrical procedures are not relevant for the time being. Their usefulness, especially for device holder verification (instead of an LPIN), is for further study.

5.2.2 Access control mechanisms

Access control mechanisms have to be used for:

- access to the UPT access device;
- access to the UPT services;
- access to service profiles.

Access control to the UPT access device is described in subclause 5.4.

Access control to UPT services is based on the authentication mechanism. It is supported by white lists (access control lists or capability lists for authorisation), black lists (e.g. for lost or stolen devices), and hot lists (e.g. for UPT numbers which have been used fraudulently). The distribution of these lists between different UPT service providers (home location/visited location) is relevant from UPT phase 2 onwards. This is for further study.

Access control to service profiles shall be specified by the UPT service providers. They need to consider the different kinds of sensitive data as described in subclause 3.3.1.2 (see also ETR 055-6). Depending on the person who requires access (user, subscriber, operator) and on the access terminal (PC, videotex, telephone) the authentication procedure preceding the access to service profile data might be different.

Although access control mechanisms for UPT may be under the responsibility of the UPT service providers and may not be standardised, the distribution of access data between different service providers (from UPT phase 2 onwards) needs some standardisation effort.

5.2.3 Service limitations

The UPT services available to a user should be restricted if weak authentication is used. Access to services which entail high risk to any participant in UPT (see figure 2) should not be allowed with only weak authentication. It is up to the UPT service provider, whether to distinguish strictly between UPT subscriptions with weak authentication (and strong service limitations) and UPT subscriptions with strong authentication (without service limitations), or to specify in the access control lists (or capability lists, respectively) what kinds of authentication have to precede the individual services. Examples of service limitations are given in subclause 4.1.10.

NOTE: The authentication mechanisms used must not depend on the terminal. This would cause a threat (**rrg5**).

5.2.4 Bill limitations

The threat analysis has pointed out that many problems and threats arise from billing. Authentication, supplemented by access control mechanisms and management procedures, prevents these threats, or at least decreases the possibility of their occurrence.

However, above all, for acceptability purposes, it seems to be necessary to preserve the users from bills of unexpected amounts. Bill limitations are indispensable if only weak authentication is used (it may e.g. be allowed to break through a bill limitation, if a strong authentication precedes the access to the service). Possible mechanisms to realise this requirement are discussed below. Combinations are also possible.

- **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, the actual bill is sent to the subscriber, but this call is still accepted. If the total amount of the current bill exceeds the given limit and there is a bill outstanding, the user access is blocked, and subsequent calls are refused, until the outstanding bill is paid.

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

It seems to be hardly possible to abort a long call if the above explained blocking condition is fulfilled. This would, however, be desirable in order to prevent unexpectedly high bills completely.

- **Bill limitation with respect to time**

Another possible measure would be to limit the bill with respect to time. That means, if e.g. a limit per week is agreed and this limit is exceeded (at call set-up or during a call), the user access would be blocked for the rest of the week.

5.2.5 Confidentiality mechanisms

Since eavesdropping has not been evaluated as a significant threat to UPT, data confidentiality mechanisms (e.g. encipherment) as well as enhanced user location and user identity confidentiality mechanisms (e.g. traffic padding, temporary identification) are not studied in this ETR. The use of a private PUI as specified in ETR 055-9 will, however, to some extent offer user location confidentiality and user identity confidentiality.

5.2.6 Data integrity mechanisms

Since data integrity has not been evaluated as a significant threat to UPT, data integrity mechanisms are not foreseen for UPT phase 1. They may be an optional feature in later phases, used for the authentication of operation data (e.g. user profile) and of some signalling messages, e.g. charging records. Possible realisations are Message Authentication Codes (MACs), and digital signatures. MACs could be computed together with user authentication data, as proposed by CCITT (see subclause 5.2.1.1).

5.3 Security management aspects

5.3.1 Key management

In all security systems involving secret cryptographic keys, the overall security will stand or fall with the security of the keys. UPT security is, therefore, limited by the security practices and standards used for generating, distributing, and storing the secret keys. At the operational level in the UPT security architecture, only one authentication key K per authenticated entity is used.

In principle, key management is an administrative, isolated activity in the network, in user and in operator domains, respectively, and, therefore, should not be standardised within the specification of security features for UPT. However, the specification could include elements that support the key management of the authentication key K in case of roaming.

The following considerations are very general. A more detailed proposal for key management mechanisms, supported by prEN 726, is introduced in subclause 5.4.6.

5.3.1.1 Generation of authentication keys

Two options are possible for the generation of authentication keys:

- **generation independent of other information**

  in this case, the keys are generated independently of any other information related to the user, and then distributed and stored. Typically, the keys would be generated in a truly random or pseudo random way.

- **Generation related to other information**

  in this case, the keys are generated in a secret way from other data associated with the user. Such keys can be either stored subsequent to generation, or generated in real time whenever they are required.

The main advantage with second approach is that the network need not maintain a database of authentication keys. However, local derivation of keys from subscription data using secret key functions may pose a higher security risk than in the case where keys are generated centrally using random or pseudo random generators.

These techniques are not relevant if the authentication is performed by asymmetrical techniques. In this case the keys could be received in a certified form.

5.3.1.2 Initial distribution and installation of keys

There are a few options for the initial distribution of keys and installation in UPT devices:

- **installation at personalisation**

the service provider can install the key in the device when he attributes an identity to this device. This is the most natural option;

- **installation at manufacture**

keys might be installed in the equipment at manufacture;

- **remote distribution and manual installation**

The keys can be distributed remotely, e.g. on paper or by means of a telephone call, to the user who can enter them manually into the UPT device. From a user-friendly point of view and for technical reasons, this is not suitable, especially if asymmetrical techniques are used.

5.3.1.3 Use of keys within the system

In order to execute the security processes, keys or security parameters derived using these keys have to be available for the system.

If the actual key K is available at the point in the system where the authentication is performed, there is only one straightforward option for the use of K, namely that the actual authentication key is directly used to perform the authentication process.

The actual authentication key may not always be available at the point in the network where the security functions are performed. This can, for instance, be the case with a registration in a visited network or if a service operator chooses to hold this sensitive information centrally. To take care about situations like this, a scheme with session authentication keys may be used for UPT.

For roaming it is not necessary that the actual authentication K is stored at the point in the UPT system where the security functions are performed. The following three options in the roaming situation are described below:

- **use of actual authentication keys**

  the actual authentication key is, in this case, directly used to perform the authentication process. It is sent by the home network to the visited network to authenticate the UPT user in the subsequent UPT procedures;

- **use of session keys**

  it may be desirable not to send the authentication key K to the visited network. The UPT security architecture could support the use of session keys, instead of the key K, in this case. This session key can be used for an indefinite period by the visited network to authenticate the user, without the authentication key K being revealed to the visited network;

  if K is the authentication key corresponding to the user, the session keys are derived from K and a random number. The session keys and the random number are sent to the point in the network where authentication is performed. It can be used for an indefinite period. This option may be supported by the security specification to facilitate the authentication of visitors by a visited network. The relevant home network has to provide the visited network with information needed to authenticate a visitor, but it needs not transfer the authentication key K. This option can also be used for mutual authentication but is not so interesting if asymmetrical techniques are used;

  of course, this option can be applied within a single network for its own subscribers;

  this option is not relevant for UPT phase 1;

- **use of precalculated sets**

  it can also be considered that the home network computes a set of authentication data consisting of authentication challenges and responses. This set is transferred to the visited network on request, which can use it to authenticate the user.

5.3.2 Management of the subscription process

Personalisation of UPT access devices

In subclause 5.4, possible UPT access devices will be described. The devices recommended in this ETR contain an integrated security module or an IC card where the security related functions and personal data are implemented. There is no need to standardise the personalisation and distribution process of such UPT access devices. The mechanisms may be chosen by the service providers.

However, since the security of the UPT system heavily depends on the security of the access device and hence of its personalisation process, standardisation has at least to establish a minimum level of security in this area. Compatibility of the several UPT phases shall be taken into consideration as far as possible. Especially the recommendations for the personalisation of smart cards shall be considered (see prEN 726-2, see also subclause 5.4.6).

The following data should at least be entered in the personalisation process: the PUI; the user specific secret key K; the initial sequence number for user authentication n_0 (if the enhanced one pass authentication mechanism is used); the LPIN; and the SPIN (if device holder verification is done in the device). The user or subscriber should have the possibility to change the LPIN and to unblock a device by use of the SPIN.

Personalisation within the UPT system

User or subscriber specific system PINs (if used for authentication) shall be stored securely in the UPT system. They can only be changed by the service provider, possibly on request of the UPT subscriber or user. Especially, an unblocking of a user's access shall be combined with the change of the relevant PIN.

If a variable authentication code with counter is used, the service provider shall have the possibility to re-synchronise the sequence numbers.

The security relevant data and algorithms shall be implemented in security modules (see prEN 726-7) or separate authentication centres.

5.3.3 Security audit trail

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

The system should contain an audit component that is able to log the following events with the following data (see Information Technology Security Evaluation Criteria, Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom, June 1991, F-C2):

- 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 synchronisation 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 operators
  (date, time, user identity, type of action, name of the object to which the action relates (e.g. 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 some selected users.

Access to audit data shall only be permitted to authorised persons. They are responsible for the observance of privacy laws. A misuse of audit data needs to be impossible. 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 must not be possible to use them for the creation of electronic user profiles.

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. They are system specific. They may be supported by TMN security mechanisms.

5.3.4 Event handling

Dependent on the evaluation of audit data (on-line or off-line), adequate actions have to be carried through, in order to enforce the security policy. These actions might be alarms to the security administrator or blocking of user access to the system.

The mechanisms for event handling are out of the scope of UPT. They are system specific. They might be supported by TMN security mechanisms, e.g. a security control board for risk management.

5.3.5 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 or special dial tones.

For example, the following information should be given to the users of a line subscription:

- "EXTRA CHARGING" (if the called party is roaming and no charging split is arranged);
- "UPT REGISTRATIONS FOR THIS TELEPHONE" (the line subscriber should always be aware of UPT registrations, especially remote registrations).

For example, the following information should be given to UPT users after successful authentication:

- "SERVICE LIMITATION";
- "RESET OF REGISTRATION BY LINE SUBSCRIBER";
- "BILL LIMITATION EXCEEDED";
- "REGISTRATIONS ON OTHER TERMINALS" (if requested).

Information and announcements to UPT users and other parties could be given by speech, by display or by special dial tones.

The UPT service providers shall be careful not to give to much information. For instance, a distinction shall not be made between wrong identification and wrong authentication, in order to avoid an attacker who wants to get information about existing PUIs.

Furthermore, information and announcements shall not affect the privacy of UPT users and other parties. A calling person shall e.g. not get information about the location of the called UPT user.

5.3.6 Charging administration

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 list of charging records may contain the sequence number of the variable Authentication Code (if used for authentication, see subclause 5.2.1.1), in order to make a verification of doubtful charging records by comparing the sequence numbers possible.

Itemised bills are a mean for the UPT subscriber to check the correctness of the billing. However, to avoid conflicts with privacy requirements, the subscriber should also have the possibility to get only summarised bills.

5.4 Possible UPT access devices and their use

UPT terminals and UPT access devices are discussed in ETR 055-5.

UPT facilities shall be accessible, both for calls and for registrations, both from dial pulse and DTMF telephones. UPT access devices may be used in order to facilitate the UPT user's interactions with the UPT service and to increase the security level. They may be distributed by the UPT service providers.

Some specific physical realisations of UPT access devices are discussed in the following.

5.4.1 No UPT access device

The renunciation of a UPT device is not user-friendly. It requires the input of long commands, possibly with reference to a user manual.

There are only restricted possibilities for implementation of security mechanisms. Support by cryptological procedures will not be possible without intelligent UPT devices. Only PINs remain as authentication parameters, possibly supplemented by TANs, (taken from a list). This solution, with weak authentication may only be acceptable for a limited access to UPT services, e.g. registration for incoming calls. However, strong authentication is recommended in general.

5.4.2 Magnetic strip-card UPT access device

A magnetic strip-card UPT access device requires a terminal equipped with a magnetic strip card reader and a signalling interface to communicate with the network. From the security point of view, it is not of much help. It is only a substitute for a manual input of the UPT number (or PUI, respectively) and a (possibly long) PIN.

5.4.3 One-way tone type UPT access device

One-way tone type UPT access devices, e.g. Dual Tone Multi-Frequency (DTMF) devices, represent a well-established technique and are easy to use. DTMF devices are only intended to send, not to receive data. They can transmit at maximum eight numerals per second.

With a UPT specific DTMF device it is possible to use UPT function keys, to store special UPT numbers, and to have a display. If accessing the UPT service from non-DTMF terminals by a non-personalised DTMF device, the same simple PIN procedure as without device is possible, without enhancement of security.

Simple personalisation of DTMF devices

Simple personalisation of the DTMF device (with PUI and PIN) could increase security by storage of a long PIN (about 10 numerals) for authentication purposes. Hence, guessing of the PIN would be rendered more difficult. However, the long PIN has to be supplemented by a short LPIN (about 4 numerals), entered manually by the user. This is necessary in order to get some security in case of non-authorised use of the UPT access device.

Additionally, such a personalised DTMF device would increase user-friendliness by the possibility to store individual data and procedures.

Intelligent DTMF device

An intelligent DTMF device (personalised, UPT specific, and equipped with a micro processor) would increase security even more. Such a device can store secret parameters (cryptological key, LPIN, SPIN) and check the user's LPIN; it can manage time and a counter; and last but not least, it can enforce cryptological algorithms and procedures, especially the variable AC.

Such a device would prevent from replay if used in combination with strong authentication.

DTMF device with IC card reader

Instead of a personalised DTMF device, a non-personalised DTMF device with an IC card reader could be used. The security functions could then be implemented in the (multi-application) card (see subclause 5.4.5).

For the first UPT phases, we recommend the use of DTMF devices with intelligence in a security module within the device or in an IC card, together with the variable Authentication Code (AC) procedure.

The device shall have a time-out, in order to avoid misuse or malfunction if the user forgets to switch off. Additionally, a new LPIN entry should be required after each transmission of an authentication code.

5.4.4 Modem type UPT access device

Acoustically coupled modem type UPT access devices are about 10 times faster than DTMF devices. However, they cause much more implementation expense and would not increase the security, compared with DTMF devices. The use of such devices is not recommended.

Electrically coupled modem type UPT access devices are for further study.

5.4.5 IC cards

IC cards are a possible solution especially for the later UPT phases. They make multiple pass authentication possible, so that user authentication can be combined with provider authentication (mutual authentication). Furthermore, smart cards are very user-friendly.

There could be two applications implemented in an IC card:

- techniques (one-way or two-way transmission) for use at a **terminal** equipped with an IC card reader;

- techniques (one-way transmission) for use at a **DTMF device** equipped with an IC card reader (see subclause 5.4.3).

An IC card for UPT shall be defined in accordance with prEN 726-3.

Contactless smart cards and "super smart cards" (with own keyboard) are for further study and not recommended for the first two phases of UPT.

5.4.6 Compatibility with standards for IC cards

The standard for the IC card for telecommunication use (prEN 726) shall be applied as soon as IC cards are used for UPT. It is possible to apply this standard to a security module inside a DTMF device already in UPT phase 1. This would make it easier to fulfil the security requirements on that security module, and it would help to avoid compatibility problems with later UPT phases when standardised IC cards will be used for UPT. The following text describes how this can be done.

Verification of the device holder by an LPIN

The user shall enter a LPIN into the UPT device in order to self-authenticate to the DTMF type UPT access device. This authentication shall be done within a security module (e.g. an IC card or a physically secured chip) in the device by matching the entered LPIN with the securely stored value, (i.e. the CHV in the terminology of prEN 726).

Blocking of the device

After a given number of LPIN input failures, the device shall be blocked internally. This prevents guessing the LPIN, and hence a misuse of stolen devices. After correct input of the LPIN, the relevant counter shall be preset to the number of remaining attempts.

Unblocking of the device

It should be possible to unblock the device after input of a SPIN. The SPIN may be longer than the LPIN. It is up to the service provider to decide if this SPIN is distributed to the subscriber.

After s_1 input failures of the SPIN, the device shall be **completely** blocked, without possibility to unblock. After less than s_1 incorrect and one correct input of the SPIN, the relevant counter shall be preset to the number of remaining attempts.

After s_2 uses of the unblocking mechanism, the device shall also be **completely** blocked. The relevant counter shall never be reset. Hence, the unblocking of the device is limited by s_2. However, unintentional blocking shall be prevented.

NOTE: The SPIN is called UNBLOCK CHV in the terminology of prEN 726; s_1 is the CHV attempt counter preset value N, and s_2 is the maximum number of uses of the unblocking procedure.

One pass authentication: sequence number

It might be possible to use an enhanced one pass authentication mechanism as described in subclause 5.2.1.1 also for other applications. This can be done by the commands defined in prEN 726-3.

The Dedicated File (DF) for the IC card application UPT shall have a cyclic Elementary File (EF) that contains the sequence number. This sequence number shall be initialised by the service provider.

NOTE: Since the number of write cycles is limited (by about 50 000 to 200 000, depending on the implementation), it might be useful to increase the number of possible sequence number increments by requiring more than one record in this EF.

One pass authentication: commands

When the UPT user has pressed the function key for identification and authentication ("send function"), for example, the commands and information described in figure 9 could be exchanged between the DTMF device itself, the security module (or IC card) in it, and the UPT system.

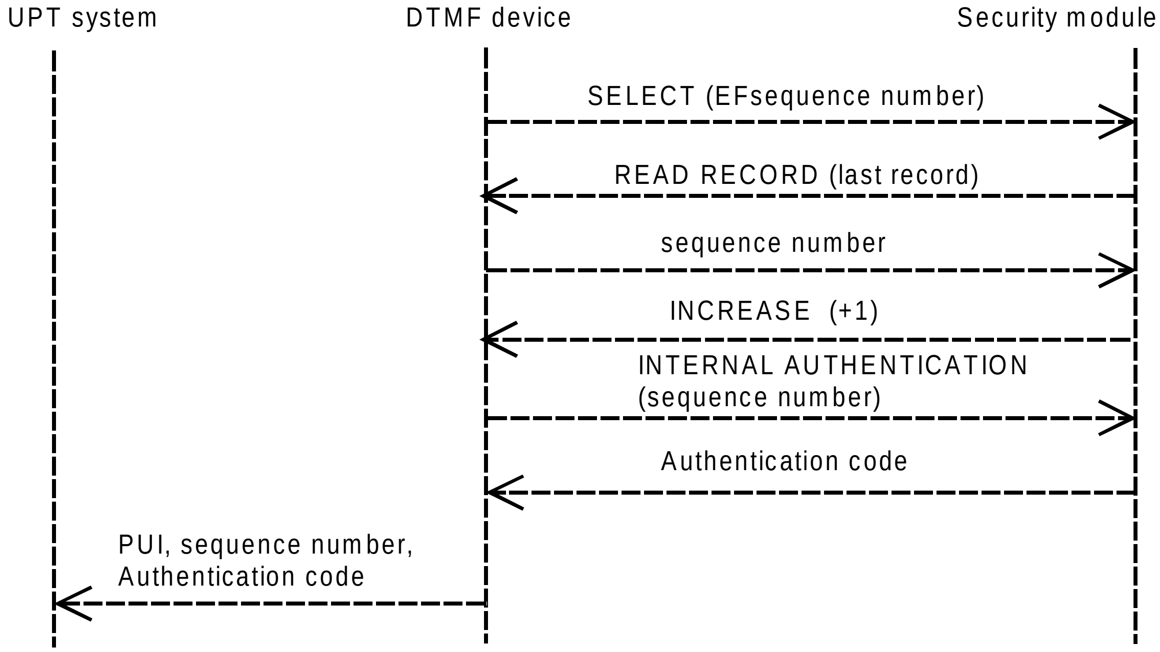


Figure 9: IC card commands for one pass authentication

Key management

There is some support for key management in prEN 726-3. 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 cryptological 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 TE 9 algorithm TESA-7 is used in the command.

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 personalisation or later, but it cannot be entered by the user himself, 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:

1) 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;

2) 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, generated by the card issuer. Now the manufacturer no longer knows any secret key in the card;

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

4) 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;

5) the UPT provider can use the "Load Key File" command and KTMUPT to replace KTMUPT with the UPT provider's own (UPT) management key(s), KMUPT. Now there is a separation between the UPT provider and the card issuer. From now on only the UPT provider can create files under the DF_{UPT};

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

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

5.5 Summary

5.5.1 General remarks

In Clause 4, the UPT service features providing security as well as the required security features for UPT have been identified. Tables 1 to 3 indicate where the necessary security mechanisms are dealt with. The specified UPT phases give information where mechanisms shall be implemented. However, in many cases, the mechanisms will be enhanced for later UPT phases.

5.5.2 Recommendations for the UPT phases

Not all of the described security mechanisms have to be standardised. The realisation is up to the service provider wherever no interaction between different domains is necessary. However, the stated security requirements shall be fulfilled, and the described realisations give hints and examples how to do this.

In order to provide a secure UPT service, a strong authentication is already recommended in UPT phase 1. If, however, a UPT service provider decides to allow weak authentication, then that UPT service provider shall consider the recommendations on service limitation and bill limitation.

The one pass authentication mechanism using a variable AC with a sequence number will be standardised in DE/NA-71401. The use of this mechanism is appropriate for the first two phases of UPT. If other authentication mechanisms are used, they should not provide a lower security. Multiple pass authentication mechanisms may be recommended for use after the first UPT phase.

For the first two UPT phases, the standard UPT access device should be a DTMF device as described in subclause 5.4.3, with respect to the considerations in subclause 5.4.6 on compatibility with IC card recommendations.

The use of IC cards in card reading DTMF devices and in card reading telephones will be standardised for UPT phase 2 (DE/NA-72501, DE/NA-72503). This does not preclude the use of IC cards already in phase 1.

Table 9: UPT service features providing security and their support by security mechanisms

UPT service features	UPT phase	mechanisms/relevant chapter
screening of incoming calls		-
screening of outgoing calls		-
special dialling tones	1	information management, subclause 5.3.5
announcements	1	information management, subclause 5.3.5
announcements on charging	1	information management, subclause 5.3.5; charging administration, subclause 5.3.6
restrictions on announcements	1	information management, subclause 5.3.5
itemised bills	1	charging administration, subclause 5.3.6
restriction on itemised bills	1	charging administration, subclause 5.3.6
activity monitoring	1	bill limitations, subclause 5.2.4
contractual agreements between user and subscriber	1	-
service profile restrictions	1	service limitations, subclause 5.2.3
reset		-
blocking of registrations		-
secure answer	2	authentication, subclause 5.2.1

Table 10: Security features and their realisations by security mechanisms

security features	UPT phase	mechanisms/relevant chapter
authentication of UPT user to UPT system	1	authentication, subclause 5.2.1
authentication of UPT subscriber to UPT system	1	authentication, subclause 5.2.1
authentication of UPT system to UPT user	2	authentication, subclause 5.2.1
authentication of UPT system to UPT subscriber	2	authentication, subclause 5.2.1
access control to the UPT service	1	access control mechanisms, subclause 5.2.2
access control to the UPT access device	1	UPT access device, subclause 5.4
access control to the UPT service profile information	1	access control mechanisms, subclause 5.2.2
secure management of the subscription process	1	subscription process, subclause 5.3.2
confidentiality of (signalling, process) data	-	confidentiality mechanisms, subclause 5.2.5
confidentiality of user location	-	confidentiality mechanisms, subclause 5.2.5
data integrity of (signalling, process) data	-	data integrity mechanisms, subclause 5.2.6

Table 11: General realisations of security

purpose	UPT phase	mechanisms/relevant chapter
support to security mechanisms	1	key management, subclause 5.3.1
preventive, reporting, deterrent	1	audit trail, subclause 5.3.3
restoring, deterrent	1	event handling, subclause 5.3.4

Annex A: Bibliography

For the purposes of this ETR, the following reference documents apply:

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

ETR 055-3 "Universal Personal Telecommunication (UPT); The service concept Part 3: Service aspects of charging, billing and accounting".

ETR 055-4 "Universal Personal Telecommunication (UPT); The service concept Part 4: Service requirements on security mechanisms".

ETR 055-5 "Universal Personal Telecommunication (UPT); The service concept Part 5: Types of UPT terminals and access devices".

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

ETR 055-7 "Universal Personal Telecommunication (UPT); The service concept Part 7: User procedures and user states".

ETR 055-8 "Universal Personal Telecommunication (UPT); The service concept Part 8: Man-machine interface aspects".

ETR 055-9 "Universal Personal Telecommunication (UPT); The service concept Part 9: Service requirements on numbering, addressing and identification".

ETR 055-10 "Universal Personal Telecommunication (UPT); The service concept Part 10: Supplementary services".

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

ETR 064 "Universal Personal Telecommunication (UPT); Requirements on feature interaction and network functionalities".

ETR 065 "Universal Personal Telecommunication (UPT); Requirements on charging, billing and accounting".

ETR 066 "Universal Personal Telecommunication (UPT); Requirements on information flows and protocols".

ETR 067 "Universal Personal Telecommunication (UPT); Network considerations and requirements on dialling, routeing and numbering".

DTR/NA-70303 "Universal Personal Telecommunication (UPT); Architecture and network interworking".

DTR/NA-70306 "Universal Personal Telecommunication (UPT); Management aspects".

ISO/IEC 7498-2 "OSI security architecture".

ISO/IEC 9798-2 "Entity authentication using symmetric technique", June 1992.

prEN 726 "Requirements for IC cards and terminals for telecommunication features".

CCITT Recommendation X.400 series "Message handling systems".

CCITT Recommendation X.509 "The Directory - Authentication framework".

CCITT Recommendation X.800 "Security architecture for OSI (ISO 7498-2)".

Annex B: Symbols and abbreviations

For the purposes of this ETR, the following symbols and abbreviations are used. The source of the abbreviations, where appropriate, are given on the right hand side:

AC	Authentication Code	SEG
ACT	Access Threat	SEG
CCAF	Call Control Access Function	IN
CCF	Call Control Function	IN
CS1	Capability Set 1, of the Intelligent Network as defined in CCITT	CCITT Q.121x series
DPT	Data Protection Threat	SEG
DTMF	Dual Tone Multiple Frequency	
ECMA	European Computer Manufacturers Association	
ECT	External Communications Threat	
FE	Functional Entity	IN
GSM	Global System for Mobile communications	ETSI
ICT	Internal Communication Threat	SEG
ID	Identity	SEG
IN	Intelligent Network	CCITT
Int	Intruder	SEG
ISDN	Integrated Services Digital Network	CCITT
LPIN	Local PIN	SEG
Lsb	Line subscriber	SEG
MAC	Message Authentication Code	ISO
MAP	Mobile Application Part	CCITT
MNT	Management Threat	SEG
NE	Network Element	
Nop	Network operator	SEG
OSI	Open Systems Interconnection	ISO
Otp	Other party	SEG
PAC	Privilege Attribute Certificate	ECMA
PCN	Personal Communications Network	
PIN	Personal Identification Number	

PLMN	Public Land Mobile Network	
PSTN	Public Switched Telecommunications Network	
PTN	Private Telecommunications Network	
PUI	Personal User Identity	ETSI NA7
SAGE	Security Algorithm Group of Experts	ETSI
SCF	Service Control Function	IN
SCP	Service Control Point	
SDF	Specialised Database Function	IN
SIT	System Integrity Threat	SEG
SMF	Service Management Function	IN
TAN	Transaction Number	SEG
Uop	UPT network operator	ETSI NA7
UPT(S)	Universal Personal Telecommunications (Services)	CCITT
Usb	UPT subscriber	ETSI NA7
Usp	UPT service provider	ETSI NA7
UTC	Coordinated Universal Time	
Uus	UPT user	ETSI NA7

Annex C: Requirements on personal data integrity

The following text summarises the requirements for the protection of personal data and privacy in the telecommunications sector as they result from the draft council directive SYN 288, 1990 version.

C.1 General issues

The EC assumes that these requirements are essential for the social acceptance of new digital networks and services. Therefore, these requirements apply also to IN-based services like UPT.

C.1.1 Intentions of the directive

The intentions of the directive are:

1) to prevent the development of different types of telecommunication terminal equipment as a result of different national laws for the protection of personal data, which would be an obstacle to the common European market;

2) to limit data collected, processed and stored in the context of public telecommunication operations;

3) to insure the right of the subscriber to self determination both with regard to the service provider as well as with regard to a second and third party in a call connection or transaction.

Excluded are issues of protection of personal data related to national security.

C.1.2 Definitions

Personal data: any information relating to an identifiable individual.

Telecommunication organisation: public or private body obtaining any rights to offer public telecommunication services or provide a public telecommunication network.

Public telecommunication network: infrastructure permitting the conveyance of signals between defined network termination points by any physical means.

Public telecommunication service: service the supply of which has been agreed between two or more telecommunication organisations.

C.1.3 Personal data to be protected during collection, processing and storage

The following personal data is to be protected during collection, processing and storage:

- subscriber related information;
- traffic and other operational data;
- detailed billing data;
- calling-line identification data;
- called-line identification data;
- automatic call-forwarding to third party data;
- unsolicited messages.

C.1.4 Locations of relevant data processing functions

Locations of relevant data process functions are:

- terminals;
- system components collecting, processing and storing subscribers' files;
- system components collecting, processing and storing traffic and billing data.

C.2 Provisions for telecommunication organisations

1) collection, processing and storage of personal data is justified only:
    - to establish connections;
    - to compile directories;
    - for legitimate operational purposes, e.g:
        - fault clearance;
        - prevention of misuse of equipment;
        - registration of incoming calls;

2) Setting up of subscribers' electronic profiles is not permitted;

3) Classifications of individual subscribers by category;

4) Collection and storage of personal data is only permitted to:
    - perform;
    - amend or;
    - terminate;

    the subscribers' contract with the telecommunication organisation;

5) Personal data are to be erased as soon as they are no longer required to:
    - deal with complaints;
    - recover charges or to;
    - to comply with other legal obligations, e.g. legal prosecution;

6) information transmitted must not be stored after the end of the transmission;

7) the subscriber is to be informed in an intelligible form and at reasonable intervals whether personal data related to him is stored;

8) the subscriber is entitled to obtain rectification or erasure or such data that was collected or stored against any law of the community or of the member state;

9) all personal data processed in telecommunication networks of services are to be kept confidential;

10) personal data may not be disclosed to people or systems outside the services or networks without the subscribers' prior consent;

11) the telecommunication organisations must not make the provision of any service dependent upon such a consent;

12) personal data must be protected adequately against unauthorised access and use;

13) in case of breach of the network security the subscribers are to be informed and offered an end-to-end encryption service;

14) the following data may be stored and processed only until the end of the period during which the bill may be challenged:

    - billing data;
    - subscriber's address;
    - type of station;
    - total number of units to be charged per period;
    - called number;
    - type and duration of call;
    - data volume transmitted;
    - advance payment information;
    - payment by instalments, disconnection, reminders;

15) traffic data containing personal data such as:

    - calling/called subscriber number;
    - beginning and end of call;
    - service used;

    may be collected, processed and stored to provide the service required only until the termination of the call unless they are used for billing or unless they are anonymised;

16) by request of the subscriber itemised call statements may be produced containing the subscriber's numbers shortened by the last four digits;

17) the calling subscriber should be able to block the calling line identification including the transmission of his number by a simple technical facility on a case by case basis;

18) the called subscriber may apply for permanent or a case by case elimination of the calling line identification;

19) the called subscriber may limit the receipt of incoming calls to the condition of a calling line identification on a case by case basis;

20) analogue subscribers must be informed about their called/calling line identification to digital subscribers and must be offered a permanent or case by case elimination of that feature;

21) service providers may override the elimination of the calling line identification for a limited period of time upon:

- a subscriber's request to trace malicious calls for the information to the relevant authority;
- specific court orders;

and permanently upon request of:

- emergency organisations; and
- fire brigades;

22) call forwarding is only allowed when the third party has agreed;

23) third parties may limit call forwarding to calling subscriber's identification;

24) third parties must be informed that a forwarded call is incoming;

25) the calling subscriber must be informed automatically during the establishment of a connection if the call is being forwarded to a third party;

26) the contents of calls may only be accessible to third parties via technical devices if all parties concerned are informed adequately, except in cases of legal prosecution;

27) the telecommunication organisation may forward personal data to other providers only by permission of the subscriber and for purposes to provide the service;

28) setting up electronic profiles of subscribers or classification of individual subscribers by category without their prior consent is not permitted;

29) telecommunication organisations must terminate the transmission of unsolicited calls for advertising purposes at the subscriber's request.

History

Document history	
July 1993	First Edition
February 1996	Converted into Adobe Acrobat Portable Document Format (PDF)