INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.1531

(06/2000)

SERIES Q: SWITCHING AND SIGNALLING

Intelligent Network

UPT security requirements for service set 1

ITU-T Recommendation Q.1531

(Formerly CCITT Recommendation)

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4 AND No. 5	Q.120–Q.249
SPECIFICATIONS OF SIGNALLING SYSTEM No. 6	Q.250–Q.309
SPECIFICATIONS OF SIGNALLING SYSTEM R1	Q.310–Q.399
SPECIFICATIONS OF SIGNALLING SYSTEM R2	Q.400–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	**Q.1200–Q.1699**
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
BROADBAND ISDN	Q.2000–Q.2999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation Q.1531

UPT security requirements for service set 1

Summary

This Recommendation specifies UPT security requirements for both user-to-network and internetwork communication applicable to UPT Service Set 1 as defined within Recommendation F.851 [1]. This Recommendation covers all aspects of security for UPT using DTMF accesses and out-band DSS1 based user accesses.

Source

ITU-T Recommendation Q.1531 was prepared by ITU-T Study Group 11 (1997-2000) and approved under the WTSC Resolution 1 procedure on 15 June 2000.

Keywords

Security, UPT.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSC Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation Q.1531

UPT security requirements for service set 1

1 Scope of Recommendation

This ITU-T Recommendation specifies UPT security requirements for both user-to-network and internetwork communication applicable to UPT Service Set 1 as defined within Recommendation F.851 [1]. Generally, there are two user-access methods for UPT. One is in-band DTMF based user access, and the other is out-band user access such as DSS1 based signalling. The requirements depend on the use of these methods. This Recommendation covers all aspects of security for UPT using DTMF access and out-band DSS1 based user accesses.

2 References

The following ITU-T Recommendation, and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T Recommendation F.851 (1995), *Universal Personal Telecommunication (UPT) – Service description (Service Set 1).*

3 Definitions of terms

3.1 Terms defined in Recommendation F.851 [1]

The following terms are defined in Recommendation F.851 [1].

– authentication;

– identification;

– personal mobility;

– UPT (Universal Personal Telecommunication);

– UPT service profile;

– UPT service profile management;

– UPT service provider;

– UPT subscriber;

– UPT user.

3.2 Terms not defined in Recommendation F.851 [1]

This Recommendation defines the following terms:

3.2.1 authorization: A property by which the access rights to resources are established and enforced.

3.2.2 confidentiality: A property by which information relating to an entity or party is not made available or disclosed to unauthorized individuals, entities or processes.

3.2.3 **integrity**: A property by which the information content of an object is prevented from being modified in an unauthorized manner.

3.2.4 **privacy**: The provision of capabilities to prevent users from suffering of freedom of actions.

4 Abbreviation and acronyms

This Recommendation uses the following abbreviations:

CS-1	Capability Set 1
CS-2	Capability Set 2
DSS1	Digital Subscriber Signalling System No. 1
DTMF	Dual Tone Multiple Frequency
IC-card	Integrated Circuit-card
IN	Intelligent Network
ISDN	Integrated Services Digital Network
MAC	Message Authentication Code
OCPIN	Outgoing Call PIN
OSI	Open Systems Interconnection
PIN	Personal Identification Number
PINX	Private Integrated Network eXchange
PLMN	Public Land Mobile Network
PUI	Personal User Identity
SAPIN	Secure Answering PIN
SCP	Service Control Point
SDP	Service Data Point
SS7	Signalling System No. 7
TMN	Telecommunications Management Network
UPT	Universal Personal Telecommunication

5 Introduction

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

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

Security in a UPT context refers to issues of:

a) fraud;

b) confidentiality;

c) service availability;

d) protection scheme.

5.1 Fraud

Fraud is the abuse of UPT facilities by unauthorized users, 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:

a) authentication of users and subscribers;

b) call details;

c) auditing.

5.2 Confidentiality

Confidentiality 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:

a) the content of communication;

b) account details;

c) call details;

d) registration details.

5.3 Service availability

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

a) service reliability;

b) service denial.

5.4 Protection scheme

The UPT specifications must define appropriate security mechanisms to protect from any security threats:

a) UPT users;

b) UPT capable network operators and service providers;

c) UPT service,

because of the circumstances in which UPT is expected to be provided. UPT will be an open system with worldwide access, and the possibility for fraud should be minimized.

6 General description

6.1 General objectives for security

The following general objectives for security in UPT apply:

a) the UPT user may use the UPT service with minimal risk of violated privacy or erroneous charging due to fraudulent use;

b) the security provided to a UPT user when using UPT services should be comparable to the security provided by the contemporary fixed or mobile networks when using the same services;

c) the security provided to a UPT service provider or network operator should be at least comparable to the security provided by the contemporary fixed or mobile networks and should protect the business interests of such providers or operators;

d) the legal, regulatory and commercial aspects of the security provided by UPT should accommodate worldwide availability;

e) the security to be provided by UPT should be adequately standardized to provide secure international interoperability and roaming.

6.2 General security requirements

The introduction of UPT and the powerful communication capabilities enabled by it, necessitate that various security mechanisms be made available to affected users. The security levels afforded by these mechanisms depend on various factors:

a) the particular security mechanisms of choice;

b) the choice of UPT terminals and UPT devices;

c) the actual use of the UPT procedures;

d) the choice of access and authentication procedures.

It is noted that some security mechanisms appear as integral parts of certain UPT procedures. It is, in general, desirable that all security mechanisms supported by the UPT service be simple to use and appear as part of the general UPT procedures.

It is desirable that a range of security levels be supported by UPT service providers. These would be offered to UPT users to choose from at subscription time.

The security level offered to the UPT user depends heavily on the choice of the degree of authentication.

7 UPT security threats

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 malicious person might abuse the UPT subscribers account from any terminal in the world. It is prudent for the UPT service specifically to protect:

a) subscribers' accounts;

b) users' responsibility to their subscribers;

c) users' personal details;

d) the integrity of the network;

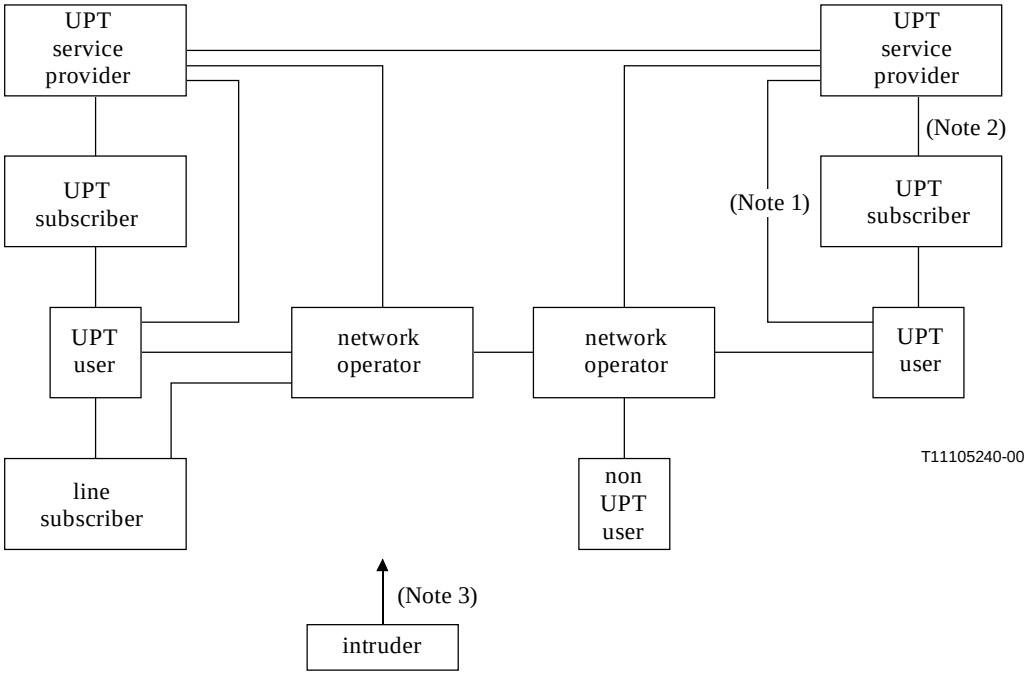
e) network operators' revenue streams;

f) network operators' reputations;

against fraudulent or malicious attack, by any party.

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 1. The intruder is not specifically placed within the diagram as the relationship depends purely on the type of intrusion perpetrated.



NOTE 1 – For example, access and service profile management.
NOTE 2 – For example, charging and service profile management.
NOTE 3 – An intruder might attack any party and any link between them.

Figure 1/Q.1531 – Model of UPT parties and their relations

7.1 Threats associated with UPT features

The major threats to the UPT service are listed below.

Masquerading as a UPT user

An intruder could use the eavesdropped authentication data to make outgoing calls on a UPT number, so the UPT subscriber of this UPT number would have to pay the charges for the intruder's calls.

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

Masquerading as a UPT service provider

If a third party is succeeding to masquerade as a UPT service provider, a number of major threats are paused to the UPT user security.

Unauthorized reading or modification of subscription data by the user/subscriber

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

Incorrectness of the billing data

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

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. All other threats could be the consequence.

Unauthorized 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. UPT user may have to pay for the call in the case of split charging.

Unauthorized 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.

The threats associated with specific UPT optional features and third party protection mechanisms are listed below.

Threats associated with OutCall registration (including AllCall registration and linked registration remotely activated or not)

Some people can take a subscription, intensively use it and avoid paying the bill. The impact is emphasized by the possibility to make several OutCall registrations at the same time.

Masquerading as a UPT user for OutCall registration, AllCall registration and linked registration shall be a great economic risk in the case that an intruder acquires valid authentication data.

A registered user may be unable to supervise the registered terminal(s) so that any intruder can make calls without paying the bill (see also the item "Masquerading as a UPT user").

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

Threats associated with called party specified secure answering of incoming calls

If a third party is succeeding to masquerade as a UPT service provider, he may require an authentication to be performed simply by making a telephone call to the UPT user. The resulting authentication code can be recorded and reused later on for an illegal registration or outgoing call etc., if only weak authentication is used.

Threats associated with call pick up

Any invalid user may pick up the call unless user authentication is performed.

Threats associated with multiple terminal address registration

In case of multiple terminal address registration, the threat of misuse of subscription (no intention to pay the bill) and the masquerading threat will have increased risks and evaluation level.

Threats associated with reset of registrations

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

7.2 Threats associated with internetwork communications

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

The threats related to internetwork communications to UPT service are listed as follows:

Masquerading as UPT entities

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

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.

Eavesdropping of UPT signalling data

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

Masquerading as originator, repudiation, modification, deletion and replay of files and messages

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

Eavesdropping of files and messages

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

Data privacy in a competitive environment

Internetwork communications may also invoke security concerns over the competitive nature of the service subscriber's data.

7.3 Unintentional situations

The threats related to unintentional situations are listed as follows:

Network connection to the wrong database

An unintentional situation occurs when SCP is not connected to the right SDP. In that 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.

8 System requirements on security

System requirements on security are described in this clause. They apply to one or more of the parties involved in the UPT service.

The system requirements on UPT security are grouped into the following categories:

a) service related requirements;

b) access related requirements;

c) network operational requirements;

d) security management requirements.

8.1 Service related requirements

The following service related requirements on security apply to UPT:

a) security features provided for the protection of the UPT users should be user-friendly and easy to use. They should as far as possible be transparent to the users, and should require as little interaction between user and network as possible;

b) security features provided for the protection of the UPT users should not significantly increase call set-up times;

c) security features should work without reduced security level when roaming;

d) security features provided by UPT should work with the various environments of UPT, and not be constrained by any one physical layer or access method;

e) the privacy of non-UPT users should not be affected by the use of UPT equipments or services.

8.2 Access related requirements

The following access related service requirements on security apply to UPT:

a) it should be very difficult for intruders to impersonate the UPT user or subscriber;

b) it should be very difficult for intruders to impersonate a UPT service provider/network operator in communication with a UPT user, or in communication with another UPT service provider;

c) it should be very difficult for intruders to access, read or modify UPT users' stored or transmitted subscription information;

d) the UPT service provider shall have mechanisms to prove the correctness and authenticity of transactions carried out with UPT users;

e) it should be very difficult for an intruder to access or implant false commands in the UPT capable network signalling structure and related control functions.

8.3 Network operational requirements

The following network operational related requirements on security apply to UPT:

a) the security to be provided by UPT should be adequately standardized to provide secure international interoperability and roaming. However, within the security mechanisms of UPT, the maximum independence between the parties involved in the UPT operation should be allowed, as well as the maximum freedom for all parties to make their own security policies and mechanisms;

b) the security mechanisms of UPT should require the least possible of long-distance real-time signalling connections (e.g. in order to avoid international signalling connections at every location update or call when roaming).

8.4 Security management requirements

The following security management related requirements on security apply to UPT:

a) security keys and devices distributed to UPT users should be easily and securely managed and updated;

b) management of security keys within and between UPT service providers should be secure;

c) the UPT service provider should have secure mechanisms to record events associated with UPT users or subscribers;

d) it should be very difficult for intruders to impersonate a UPT service provider in communication with UPT capable network operators, and vice versa;

e) the security mechanisms provided by UPT should have means for version management, and should be easy to update during the lifetime of UPT.

9 Security features for UPT

In UPT, as in all practical systems accessible by the general public, many different security features need to be presented and cooperate to give the required level of overall security.

Security services may be distinguished as having one of the following properties:

Preventive: Intending to make the threat impossible.

Reporting: Giving the system management or the user information about security.

Limiting: Introducing restrictions into the system in order to limit the consequences of possible security breaches.

Restoring: Making a quick, safe and orderly return to normal operation after security problems have occurred.

Deterrent: Having the property that potential misusers restrain themselves because they know about this security feature.

All these properties are needed and valuable elements in the overall UPT security architecture.

The following security features can be identified for UPT:

a) confidentiality;

b) authentication;

c) integrity;

d) authorization and access control;

e) privacy and anonymity;

f) service availability;

g) event limitation;

h) event reporting.

9.1 UPT service features providing security

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

Bill limitation

Bill limitation or credit is the only effective way to limit the consequences of extensive, possibly unauthorized use by the user or fraudulent use by masquerading intruders. The limit for accumulated charges should be set by the service provider in cooperation with the subscriber. To be effective the control should be performed in connection with the authentication for every outgoing call (this may even be extended to incoming call control dependent on the operator's charging and security policy). In case of overrun of the limit, the service provider shall not allow any additional calls that increase the charges. The user should be made aware of this situation immediately before the limit is reached and attempts for calls after the limit has been reached.

For extra protection, OutCall follow-on, OutCall registration, or remote OutCall registration may be restricted by the service provider.

Itemized bills

Itemized bills play 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 scrutinized in detail. Knowledge of the fact that itemized billing is used will give a deterrent effect, which may restrain people from some abuse or misuse of the service.

Special caution may be necessary in order to protect privacy.

Activity monitoring

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

Announcements

Given 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.

Special caution may be necessary in order to protect privacy.

Blocking of registration

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

Local registrations, where registration to a specific line terminal is made from the same terminal, should be excluded from this requirement.

Reset of registration

Reset of registration is an essential part of the UPT service. However, it does not give full protection against problems with unwanted registrations as third parties cannot in general be expected to be familiar with the reset procedures.

Contractual agreements

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

a) to follow the rules (as declared by the UPT service provider and adjoined to the subscription contract) regarding secure handling of PUI and PIN for weak authentication and the corresponding rules regarding use of UPT device;

b) to report to the service provider immediately loss of PIN or device or other conditions which might lead to fraud or misuse;

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

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

e) to accept limitations of service which the service provider later on may find necessary to introduce to protect the UPT service as such against misuse or fraud;

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

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

9.2 Security features for user access

Many threats will be covered by features already defined in the UPT service concept. These features are described in ITU-T F.851 [1] as general UPT service offer. The required specific security services for the main part of the threats are listed here.

The following security features have been identified as required for UPT to measure against threats:

Authentication of the UPT user/UPT subscriber

The threats concerning masquerading towards the UPT service provider are the strongest identified and authentication of the UPT user (and UPT subscriber) is the most important security feature for UPT. For this reason, strong authentication using an advanced UPT device which has the intelligence (e.g. DTMF type device or IC-card type device), is recommended. Weak authentication is not a sufficient solution in itself and could only be accepted if accompanied by several other security features and limitations of the service.

Access control to UPT access device

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

a) authentication of user/owner towards the device;

b) strong physical protection, e.g. using IC-card type of microprocessor.

Access control system to service profile information

Users, subscribers and the service provider's staff shall have access to different parts of the service profile. For controlled access to the service profile databases there is a need for an access control system. Part of the access control will of course be the authentication of UPT user/subscriber. Authentication of personal and access control in the service provider's local environment should have a dedicated state of the solution for this hardware and software environment.

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.

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 designated to cover threats like:

a) unauthorized modification of subscription data by user or subscriber;

b) unauthorized withdrawal of subscription;

c) denial of service by device malfunction;

d) incorrect delivery of UPT devices.

The security features to attain the needed level of security management may vary substantially depending on the different environments to be found with service providers and is out of the scope of this Recommendation.

9.3 Security features for internetwork communications

The following security requirements should be considered for internetwork communications:

a) secure dialogues;

b) secure file transfers.

The security requirements described here can be applied not only to UPT but could be used also for the protection of other IN internetwork communications. For efficiency reasons, security functions should be commonly used by all IN services where possible.

Therefore, the allocation of security features within the OSI structure should be considered. The following requirements are identified:

a) security functions should be independent of the underlying network as far as possible;

b) 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 entities. The network links are part of the SS7.

The security features mentioned in the following are shown as examples. The necessary security features and mechanisms should be considered in connection with the development of a general IN security architecture.

9.3.1 Secure dialogue

Secure dialogues should consist of a mutual authentication procedure, a confidentiality service and a data integrity service on the communication link. Possible security mechanisms provided are:

a) mutual authentication;

b) link encryption;

c) link data integrity;

d) key management to support this.

9.3.2 Secure file transfer

Files should be protected by two security features: file data integrity and file confidentiality. Possible security mechanisms provided are:

a) digital signature or MAC for file data integrity;

b) file encryption;

c) key management to support this.

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

9.4 Security limitation

This subclause identifies the threats which may not be covered by relevant security features. Some of these threats can be considered to be of less importance either because of low likelihood or because they have only small consequences, often both. For other threats, no feasible (cost justified) way to protect against them has been identified.

9.4.1 DTMF based user access

Threats not covered include all those concerned with eavesdropping or active manipulation of the lines used for UPT registrations. The eavesdropping threats have high vulnerability especially if authentication data (e.g. PUI, PIN) is recorded. There is, however, a substantial difference in risk if weak authentication is used instead of the recommended strong authentication. This is especially true if the registration is passing over the air, e.g. in a PLMN access or if it passes some equipment that

has inherent recording facilities, e.g. some PINX. This is one reason to limit the service of UPT when weak authentication is used.

Protection against nuisance registrations to terminals of unknowing or unwilling third parties is not given a definite solution on DTMF based user access, because reset of registrations is not generally available. The recommended indications, dial tones, etc. are not sufficient. Default blocking conditions and active agreement through preregistration or online agreements are possible, but may not be sufficient.

9.4.2 Out-band DSS1 based user access

Since two-way authentication is available on DSS1 accesses, only threats related to active line manipulation and eavesdropping of personal data are not covered.

Active line manipulation related to nuisance registration can be partly covered by security management features such as reset of registration, bill limitation and service limitation.

Eavesdropping of authentication codes has no impact when strong authentication is used.

10 Security mechanisms for UPT

10.1 Access control mechanisms

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

a) access to the service based on the user's or subscriber's identity;

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

c) access to the data in the UPT access device.

10.1.1 Access control to services

Access control to the UPT service or certain service functions can be seen as a combined process with identification and authentication of the involved parties.

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

White lists

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

Black lists

Black lists specify those identities that shall not be accepted to get access to the UPT service, for example, because the UPT user has exceeded the credit limit. Black lists shall be updated as often as necessary. They shall be realized in the authenticating entity (e.g. SCP, SDP).

Grey lists

The UPT provider may define grey lists, too, for those identities where additional measures should take place, e.g. if a detailed activity monitoring should be activated.

For weak authentication, a PUI is blocked if the access is temporarily denied because of too many consecutive wrong authentication attempts. Blocking shall be realized in authenticating entity. An unblocking procedure should be provided, because it is possible to maliciously block someone's PUI. Nevertheless, the user with the blocked PUI suffers great inconvenience.

For strong authentication, an identity should not be blocked because the authentication can be considered secure enough. The user key should be changed if his key and algorithm would be disclosed.

10.1.2 Access control to service profile data

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

a) UPT user;

b) UPT subscriber;

c) UPT service provider.

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

The UPT service provider is responsible that only authorized personnel have access to the data. The specification of the mechanisms is the responsibility of the UPT service provider and is out of the scope of this Recommendation. The signalling access (e.g. by SS7) shall be protected by authentication of the network entities and authorization lists containing service providers with roaming contracts, according to the contract between the service providers.

10.1.3 Access control to the data in the UPT device

The access control mechanism shall use a strong physical protection against reading.

The access control mechanism for the use of the UPT device can be supported by a device holder verification.

10.2 User authentication mechanisms

10.2.1 Degrees of authentication

The degree of authentication (strong or weak) depends on the authentication method used. The degree of authentication used should be sufficient to abate the anticipated security risks.

In general, authentication should also be strong enough to guarantee a sufficient level of security when UPT services are accessed through UPT-supporting networks visited by UPT users. The authentication procedure to be adopted may be negotiated between the UPT service provider and the visited networks. UPT users and UPT service providers have the options to support various authentication mechanisms to meet the required degree of authentication.

UPT authentication can be classified into several types, including the following:

One-way with a fixed PIN

In this case, the authentication procedure is completed by sending the correct PIN by the UPT user.

One-way with variable authentication codes

In this case, the authentication procedure still uses one-way transmission, but with a variable authentication code.

Two-way with variable authentication codes

In this case, the authentication procedure employs two-way transmission in a challenge-response mode.

10.2.2 Types of UPT device

If UPT user identity authentication is provided by using a UPT device, the level of protection depends on how the device is realized. UPT devices may exist in different realizations depending on the networks, terminals and services used, which put different restrictions on the security mechanisms that can be provided in a simple and user-friendly way. For this reason, it may be necessary to have different authentication procedures for different realizations of the UPT devices. Possibly realizations include the following:

No UPT device

In this case, the PUI may have to manually be input for identification, and it may be necessary to restrict the authentication procedure to the use of a PIN code only.

Magnetic strip-card UPT device

This type of UPT device requires a terminal equipped with a magnetic strip card reader and a signalling interface to communicate with the network.

Tone type UPT device one way (e.g. DTMF)

This device could either simply simulate the sequence of tones that would be generated by the UPT user who uses a PIN for authentication, or it could contain the intelligence to provide authentication procedures similar to that possible with an intelligent-card using one-way authentication (the UPT device transmits data only). The intelligence should have the capability to store and generate synchronizing information. In case of using authentication key, it should also have the capability to store authentication key and generate authentication code.

Modem type UPT device

This would be similar in functionality to the Tone Type Device, but with the physical acoustic in-band signalling using a modem standard. Ideally, the authentication procedures should in this case be the same as with an intelligent-card using one-way or two-way authentication (i.e. the UPT device transmits and receives data). The intelligence should have the capability to store and generate synchronizing information. In case of using authentication key, it should also have the capability to store authentication key and generate authentication code.

Intelligent-card type UPT device

Either a one-way or a two-way authentication procedure could be used. UPT service provider authentication could be combined with subscriber identity authentication (mutual authentication). An intelligent card should have the capability to store authentication key and generate authentication code.

10.2.3 User signalling

10.2.3.1 DTMF based user access (compliant with IN CS-1)

Limitation

For UPT Service Set 1, UPT will be provided over existing networks. Because of the limitations of this network and its connected terminal, authentication can only be performed in certain ways.

The options for authentication mechanisms are limited; information exchange will take place only in one direction and the signalling is limited to DTMF tones.

One-way signalling allows UPT users to authenticate themselves to the network. It does not allow the UPT users to authenticate the network. Its use also restricts the mechanisms available to perform the authentication.

Selection of authentication type

There may be two authentication types for DTMF based user access. One is that one-way authentication with a fixed PIN. The other is that one-way authentication with variable authentication codes. If the UPT user needs a stronger authentication procedure, then the latter is better than the former.

Authentication key

An authentication key is an identity issued to a user, for use in an authentication process. This usually takes the form of a specified number of digits or bits.

An authentication key is usually a long value stored in hardware and used as input to a cryptographic function.

Features for one-way authentication with a PIN

a) this authentication belongs to a weak authentication;

b) UPTN should not be changed even if the service provider could recognize that his PIN was disclosed by unauthorized users. The use of PUI would be one of solutions;

c) the device should have a secret PUI for user-friendliness;

d) a UPT user sends his PIN to the service provider;

e) the pair of PUI and PIN is compared with the same values stored in the service provider;

f) if they do not match, the access would be failed;

g) a counter for failed authentication attempts would need to protect his PIN from fraudulent use;

h) the PUI would be blocked when the counter reaches the maximum value;

i) as it is possible to maliciously block someone's PUI, a special PIN would be needed to unblock it. Nevertheless, the user with the blocked PUI suffers great inconvenience.

Features for one-way authentication with variable authentication codes

a) this authentication belongs to a strong authentication;

b) the secret PUI is not necessarily needed because it is extremely difficult to disclose someone's authentication key and algorithm. The use of PUI may be optional;

c) the device sends a variable authentication code and synchronizing information between the device and network (e.g. time indication, serial number);

NOTE – Several variable authentication codes are also possible.

d) the device and the service provider have a user key and an algorithm;

e) the service provider calculates the variable authentication code using a user key, an algorithm and the synchronizing information provided by the user;

f) the authentication could be valid for a given period of time;

g) the calculated variable authentication code is compared with the one sent by the user;

h) if they do not match, the authentication fails;

i) there may be no counter for failed attempts and its maximum value. Therefore, there is no limitation to the number of failed attempts;

j) the UPTN should not be blocked even if the key and algorithm would be disclosed;

k) the user key should be changed when his key and algorithm would be disclosed;

l) the device would require the UPT user to be authenticated to the device to prevent unauthorized users from fraudulently using the device. This could be done using, for example, a local PIN. The way that the UPT user authenticates himself to the device is an

implementation issue. The local PIN is available for only UPT user-device interface. Considering user-friendliness, to enter the PIN to the device may be an optional function;

m) the device would use a standardized protocol to communicate authentication and command data with the local UPT service provider (e.g. through a voice channel).

Additional weak authentication for outgoing calls after OutCall registration

a) this authentication is optionally used for each call in case outgoing call registration is active in addition to the normal authentication at registration time;

b) at subscription time each user will be attributed a special OCPIN. If the user is allowed to use weak authentication, the OCPIN value shall be different from the PIN value;

c) the user sends his OCPIN each time he wants to set up a call from the terminal he is registered on. OCPIN may be stored in the device for user-friendliness;

d) the OCPIN value is checked by the network and if its value is correct then the user is allowed to proceed.

Additional weak authentication for called party specified secure answering of incoming UPT calls

a) this authentication is used for called party specified secure answering of incoming calls in case of DTMF access if the user is unable to use his UPT device. It is a service provider option to give the user an option to use only strong authentication or both strong authentication and this feature;

b) at subscription time each user may get a SAPIN. If the user is allowed to use weak authentication, the SAPIN value shall be different from the PIN value;

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

d) the user sends his SAPIN. SAPIN may be stored in the device for user-friendliness;

e) the SAPIN value is checked by the network and if its value is correct then the call is completed.

10.2.3.2 Out-band DSS1 based user access

Limitation

In UPT based on IN CS-2 or later, the use of the out-band user access such as DSS1 based signalling would be available. Therefore, limitation concerning networks and terminals would be decreased. As far as the out-band DSS1 based user access is concerned, various types of authentication could be used such as one-way authentication, two-way authentication in a challenge-response mode, mutual authentication, etc. And various types of UPT devices described in 10.2.2 could be implemented. Under such circumstances, strong authentication using intelligent device should be applied.

Selection of authentication type

ISDN has a capability to offer easy two-way signalling which gives the opportunity to use two-way authentication mechanisms. It also allows mutual authentication, that is, the ability of users both to authenticate themselves towards the UPT service provider, and to authenticate the UPT service provider to the users.

Authentication key

An authentication key is an identity issued to a user, for use in an authentication process. This usually takes the form of a specified number of digits or bits.

An authentication key is usually a long value and used as input to a cryptographic function.

Features for challenge-response type authentication

a) this authentication belongs to a strong authentication;

b) the service provider sends a random number to the device;

c) the device uses an authentication key and the random number, and calculates the variable authentication code. Then it sends it to the service provider;

d) the device and the service provider have a user key and an algorithm;

e) the service provider calculates the variable authentication code using the user key and the algorithm;

f) the calculated variable authentication code is compared with the one sent by the user;

g) if they do not match, the authentication fails;

h) there may not be counter for failed attempts and its maximum value;

i) the UPTN is not changed even if the key is disclosed. Another key and algorithm would be provided to the user;

j) the challenge-response type authentication needs the use of a device with intelligent function;

k) the device would require the UPT user to be authenticated to the device to prevent unauthorized users from fraudulently using the device. This could be done using, for example, a local PIN. The way that the UPT user authenticates himself to the device is an implementation issue. The local PIN is available for only UPT user-device interface. Considering user-friendliness, to enter the PIN to the device may be an optional function;

l) the device would use a standardized challenge-response mode protocol through ISDN D-channel signalling.

10.3 Security management mechanisms

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

10.3.1 Security audit trail

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

The system may contain audit components that are able to log the following events with the following data:

a) use of the identification and authentication mechanism (date, time, user identity, calling line identity or originating area code, number dialled, success or failure of the attempt, number of synchronization updates);

b) attempted access to the service profile (date, time, user identity, name of the object, type of access attempt, success or failure of the attempt);

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

The mechanisms to obtain, maintain and evaluate an audit trail are out of the scope of this Recommendation. They are system specific and might be supported by TMN security mechanisms.

10.3.2 Event handling actions

Dependent on the evaluation of audit data (online or off-line), adequate actions shall be carried through, in order to enforce the security policy. These actions might be:

a) alarm to the security administrator;

b) blocking of user access to the system;

c) interrupt of calls (e.g. especially excessively long international calls).

The mechanisms for event handling are out of the scope of this Recommendation. They are system specific and might be supported by TMN security mechanisms.

10.3.3 Charging control

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

The threat analysis has pointed out that many problems and threats relate to charging and 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 may be necessary to preserve the users from bills of unexpected amount. Bill limitations are recommended especially when weak authentication is used.

10.3.4 Information management

There should be a facility to inform UPT users, UPT subscribers, and other parties about actions that affect their privacy and security or the charging. As far as possible, this information should be given online by announcements (speech or display) or by special dial tones. It is up to the service provider to specify the information that is given to the involved parties. The contents of the information are out of the scope of this Recommendation.

The UPT service providers shall be careful not to give too much information. Potential intruders should not be able to misuse such information for their attacks. Furthermore, information and announcements should be carefully chosen not to affect the privacy of UPT users and other parties.

The UPT user shall be informed about the risks of the UPT features and supplementary services and ways to minimize them.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

Geneva, 2001