



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.



Documents
Document Sharing Hub

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.

© ITU 2001

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from ITU.

CONTENTS

	Page
1 Scope of Recommendation	1
2 References	1
3 Definitions of terms	1
3.1 Terms defined in Recommendation F.851 [1]	1
3.2 Terms not defined in Recommendation F.851 [1]	1
4 Abbreviation and acronyms	2
5 Introduction	2
5.1 Fraud	3
5.2 Confidentiality	3
5.3 Service availability	3
5.4 Protection scheme	3
6 General description	3
6.1 General objectives for security	3
6.2 General security requirements	4
7 UPT security threats	4
7.1 Threats associated with UPT features	5
7.2 Threats associated with internetwork communications	6
7.3 Unintentional situations	7
8 System requirements on security	7
8.1 Service related requirements	8
8.2 Access related requirements	8
8.3 Network operational requirements	8
8.4 Security management requirements	8
9 Security features for UPT	9
9.1 UPT service features providing security	9
9.2 Security features for user access	11
9.3 Security features for internetwork communications	12
9.3.1 Secure dialogue	12
9.3.2 Secure file transfer	12
9.4 Security limitation	12
9.4.1 DTMF based user access	12
9.4.2 Out-band DSS1 based user access	13
10 Security mechanisms for UPT	13

	Page
10.1 Access control mechanisms.....	13
10.1.1 Access control to services	13
10.1.2 Access control to service profile data	14
10.1.3 Access control to the data in the UPT device.....	14
10.2 User authentication mechanisms	14
10.2.1 Degrees of authentication	14
10.2.2 Types of UPT device.....	15
10.2.3 User signalling.....	15
10.3 Security management mechanisms.....	18
10.3.1 Security audit trail	18
10.3.2 Event handling actions	19
10.3.3 Charging control.....	19
10.3.4 Information management	19

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;
