International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.366.1

(07/2007)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

IPCablecom

Organization of subscriber data specification

Recommendation ITU-T J.366.1

Recommendation ITU-T J.366.1

Organization of subscriber data specification

Summary

Recommendation ITU-T J.366.1 provides details concerning information to be stored in home subscriber servers, visitor location registers, general packet radio service (GPRS) support nodes and the call session control function (CSCF) concerning mobile subscribers.

This Recommendation provides the interoperability between 3GPP IMS and IPCablecom 2.0, which is based on 3GPP IMS and includes additional functionality necessary to meet the requirements of cable operators.

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. This Recommendation references the ETSI version of the 3GPP specification and specifies only the modifications necessary to optimize it for the cable environment.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T J.366.1	2007-07-29	9

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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 Assembly (WTSA), 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 WTSA 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.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

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, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T J.366.1

Organization of subscriber data specification

1 Scope

This Recommendation provides details concerning information to be stored in home subscriber servers, visitor location registers, GPRS support nodes and the call session control function (CSCF) concerning mobile subscribers.

Clause 2 of the base ETSI specification [ETSI TS 123 008] contains all the details concerning the definition of the parameters, often given by reference to other specifications, and indication of where the parameters are to be stored.

Clause 3 gives a summary overview and clause 4 identifies the reference information required for accessing the information.

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. This Recommendation references the ETSI version of the 3GPP specification and specifies only the modifications necessary to optimize it for the cable environment.

It is an important objective of this work that interoperability between IPCablecom 2.0 and 3GPP IMS be provided. IPCablecom 2.0 is based upon 3GPP IMS, but includes additional functionality necessary to meet the requirements of cable operators. Recognizing developing converged solutions for wireless, wireline, and cable, it is expected that further development of IPCablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IPCablecom 2.0.

The modifications to [ETSI TS 123 008] V6.8.0 (2005-12), *Digital cellular telecommunications system (Phase 2+)*; *Universal Mobile Telecommunications System (UMTS)*; *Organization of subscriber data*, are shown in clause 6.

2 References

[ETSI TS 123 008] ETSI TS 123 008 V6.8.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Organization of subscriber data*.

3 Definitions

This Recommendation uses the terms defined in [ETSI TS 123 008].

4 Abbreviations and acronyms

This Recommendation uses the abbreviations provided in [ETSI TS 123 008].

5 Conventions

This Recommendation uses the conventions provided in [ETSI TS 123 008].

6 Modifications to [ETSI TS 123 008]

Modifications introduced by this Recommendation are shown in revision marks. Unchanged text is replaced by ellipsis (…). Some parts of unchanged text (section numbers, etc.) may be kept to indicate the correct insertion points.

0 Scope

The present document provides details concerning information to be stored in home subscriber servers, visitor location registers, GPRS Support Nodes and Call Session Control Function (CSCF) concerning mobile subscriber.

Clause 2 contains all details concerning the definition of the parameters, often given by reference to other specifications, and where the parameter is to be stored.

~~Table 1 in clause 3 gives a summary~~ Clause 3 provides an overview and clause 4 identifies the reference information required for accessing the information.

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. The following modifications reference the ETSI version of the 3GPP specification and specify only the changes necessary to optimize it for the cable environment.

It is an important objective of this work that interoperability between IPCablecom 2.0 and 3GPP IMS is provided. IPCablecom 2.0 is based upon 3GPP IMS, but includes additional functionality necessary to meet the requirements of cable operators. Recognizing developing converged solutions for wireless, wireline, and cable, it is expected that further development of IPCablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IPCablecom 2.0.

The modifications to [ETSI TS 123 008] V6.8.0 (2005-12), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Organization of subscriber data*; Stage 3 are shown below.

0.1 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*
- IPCablecom2 defines several Recommendations which are based on 3GPP technical specifications. These IPCablecom2 Recommendations are commonly referred to as IPCablecom2 Delta Recommendations. For references within this Recommendation which have a corresponding IPCablecom2 Delta Recommendation, the IPCablecom2 Delta Recommendation must be used. The list of IPCablecom2 Delta Recommendations is:

ITU-T J.366.1 (TS-23.008)	ITU-T J.366.5 (TS-29.228)
ITU-T J.366.2 (TS-23.218)	ITU-T J.366.6 (TS-29.229)
ITU-T J.366.3 (TS-23.228)	ITU-T J.366.7 (TS-33.203)
ITU-T J.366.4 (TS-24.229)	ITU-T J.366.8 (TS-33.210)
ITU-T J.366.10 (TS-29.109)	ITU-T J.366. 9 (TS-33.220

References which have corresponding delta Recommendations are highlighted with an*.

[1] 3GPP TR 21.905: "*Vocabulary for 3GPP Specifications*".

• • •

[42] *3GPP TS 23.228: "*IP Multimedia Subsystem (IMS)*".

[43] *3GPP TS 29.228: "*IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents*".

[44] *3GPP TS 29.229: "*Cx and Dx Interfaces based on the Diameter protocol; Protocol details*".

• • •

[49] *3GPP TS 33.203: "*3G security; Access security for IP-based services*".

[50] 3GPP TS 23.002: "*Network Architecture*".

[51] IETF RFC 3588: "*Diameter Base Protocol*".

[52] 3GPP TS 33.102: "*3G Security; Security Architecture*".

[53] *3GPP TS 23.218: "*IP Multimedia (IM) session handling; IM call model; Stage 2*".

• • •

[58] *3GPP TS 33.220: "*Generic Authentication Architecture (GAA); Generic bootstrapping architecture*".

[59] *3GPP TS 29.109 "*Zh and Zn Interfaces based on the Diameter protocol; Protocol details*".

• • •

[66] 3GPP TS 32.252: "*Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging*".

[67] IETF RFC 2617: "*HTTP Authentication: Basic and Digest Access Authentication*".

0.2 Abbreviations

• • •

3.1.1 Private User Identity

The Private User Identity is applicable to IMS subscribers only. The Private User Identity is in the form of a Network Access Identifier (NAI), which is defined in RFC 2486 [48].

If the GAA bootstrapping is based on authentication data from the IM domain, the corresponding Private User Identity from the IM domain (IMPI) is used as it is. If the GAA bootstrapping is based on the authentication data from the CS/PS domain, a Private User Identity is derived from user's IMSI according 3GPP TS 23.003 [5] is used.

In the case of SIP Digest authentication, the Private User Identity is the Username.

The Private User Identity is permanent subscriber data and is stored in HSS and in S-CSCF.

3.1.2 Public User Identities

• • •

3.1.2B Public Service Identity

The Public Service Identity hosted by an application server may match either to a distinct PSI or a ~~wilcarded~~wildcarded PSI that is stored in the HSS. The PSI is defined in 3GPP TS 23.003 [5].

The Public Service Identity is permanent subscriber data and is stored in HSS and S-CSCF.

3.1.3 Barring indication

• • •

3.1.8 PSI Activation State

The PSI Activation State is specific for Public Service Identities and is defined in 3GPP TS 29.328 [54].

The PSI Activation State indicator is temporary subscriber data and is stored in the HSS.

3.1.9 Display Name

The Display Name is a string associated with a Public Identity.

The Display Name is permanent subscriber data and is stored in the HSS and in the S-CSCF.

3.2 Data related to registration

• • •

3.3.1 Random Challenge (RAND), Expected Response (XRES), Cipher Key (CK), Integrity Key (IK) and Authentication Token (AUTN)

For contents of Random Challenge (RAND), Expected Response (XRES), Cipher Key (CK), Integrity Key (IK) and Authentication Token (AUTN) see subclause 2.3.2.

A set of quintuplet vectors are calculated in the HSS, and sent from the HSS to the S-CSCF (see 3GPP TS 29.228 [43]).

These data are temporary subscriber data conditionally stored in the HSS and in the S-CSCF.

3.3.2 Data related to SIP-Digest Authentication

3.3.2.1 Realm

The Realm is a string to identify to the user the security space or partition. Realm is used as part of the HA1 hash calculation for SIP-Digest (see IETF RFC 2617 [67]).

The Realm is permanent subscriber data and is stored in the HSS.

3.3.2.2 Domain

The Domain is a quoted string of space separated URIs that defines the protection space of the resource being accessed (see IETF RFC 2617 [67]).

The Domain is permanent subscriber data and is stored in the HSS.

3.3.2.3 Password

The password is a credential shared only between the HSS and the UE being authenticated. It is used as part of the HA1 hash calculation (see IETF RFC 2617 [67]).

The Password is permanent subscriber data and is stored in the HSS.

3.3.2.4 Nonce

The nonce is a random (non-predictable) value selected by the S-CSCF (see 3GPP TS 29.228 [43]) and used by the client to calculate the authentication response (see IETF RFC 2617 [67]).

The Nonce is temporary subscriber data and is stored in the S-CSCF.

3.3.2.5 Opaque

Opaque is a string sent by the S-CSCF that is returned unchanged in the authentication response by the UE (see IETF RFC 2617 [67]). It is stored (or generated) in the HSS or S-CSCF (see 3GPP TS 29.228 [43]).

Opaque is temporary subscriber data and is stored in the S-CSCF.

3.3.2.6 Stale

Stale is a flag, indicating that the previous request from the client was rejected because the nonce value was stale, but the credentials presented were correct (see IETF RFC 2617 [67]).

Stale is temporary subscriber data and is stored in the S-CSCF.

3.3.2.7 Algorithm

The algorithm is a string conveying the choice of the hash algorithm used to produce the Digest and the Checksum to the client. If the algorithm is not provided, "MD5" is assumed (see IETF RFC 2617 [67]).

Algorithm is permanent subscriber data and is stored in the HSS.

3.3.2.8 QoP

Quality of Protection is a quoted string of one or more tokens indicating the "quality of protection" values supported by the server. Possible values include "auth" for authentication and "auth-int" for authentication with integrity protection. For auth-int, the client includes a hash of the entity-body in the calculations (see IETF RFC 2617 [67]).

QoP is permanent subscriber data and is stored in the HSS and the S-CSCF.

3.3.2.9 HA1

HA1 is the value calculated as defined in IETF RFC 2617 [67]. It is calculated by the HSS and used by the S-CSCF to create the Expected Response (see 3.3.2.14). It is also used to create the Response-Auth (see 3.3.2.15) after a successful authentication verification has occurred.

HA1 is temporary subscriber data and is stored in the S-CSCF.

3.3.2.10 Auth Param

Auth Param directive is for future extensions. If the provided value is unrecognized it must be ignored (see IETF RFC 2617 [67]).

Auth Param is permanent subscriber data and is stored in the HSS and the S-CSCF.

3.3.2.11 Next Nonce

Next Nonce is the nonce the server wishes the client to use for a future authentication response (see IETF RFC 2617 [67]).

Next Nonce is temporary subscriber data and is stored in the S-CSCF.

3.4 Data related S-CSCF selection information

• • •

5.3 IP Multimedia Service Data Storage

Table 5.3 – Overview of IMS subscriber data used for IP Multimedia services

PARAMETER	Subclause	HSS	S-CSCF	IM-SSF	AS	TYPE
Private User Identity	3.1.1	M	M		–	P
Public User Identity	3.1.2	M	M		–	P
Barring Indication	3.1.3	M	M		–	P
List of authorized visited network identifiers	3.1.4	M	–		–	P
Services related to Unregistered State	3.1.5	M	–		–	P
Implicitly registered Public User Identity sets	3.1.6	C	C	–	–	P
Default Public User Identity indicator	3.1.7	C	–	–	–	P
Display Name	3.1.9	C	C		–	P
Registration Status	3.2.1	M	–		–	T
S-CSCF Name	3.2.2	M	–		–	T
Diameter Client Address of S-CSCF	3.2.3	M	–		–	T
Diameter Server Address of HSS	3.2.4	–	M	–	C	T
RAND, XRES, CK, IK and AUTN	3.3.1	M	C		–	T
Realm	3.3.2.1	C				P
Domain	3.3.2.2	C				P
Password	3.3.2.3	C				P
Nonce	3.3.2.4	–	C			T
Opaque	3.3.2.5	–	C			T
Stale	3.3.2.6	–	C			T
Algorithm	3.3.2.7	C				P
QoP	3.3.2.8	C				P
HA1	3.3.2.9	–	C			T
Auth Param	3.3.2.10	C	C			P
Next Nonce	3.3.2.11	–	C			T
Server Capabilities	3.4.1	C	C		–	P
Initial Filter Criteria	3.5.2	C	C		–	P
Application Server Information	3.5.3	C	C	–	–	P
Service Indication	3.5.4	M	–		M	P
Shared iFC Set Identifier	3.5.5	C	C			P
Subscribed Media Profile Identifier	3.6.1	C	C		–	P
Primary Event Charging Function Name	3.7.1	C	C	–	–	P
Secondary Event Charging Function Name	3.7.2	C	C	–	–	P
Primary Charging Collection Function Name	3.7.3	C	C	–	–	P
Secondary Charging Collection Function Name	3.7.4	C	C	–	–	P
~~GsmSCF address for IM CSI~~	~~3.8.4~~	~~C~~	–		–	~~P~~
~~IM-SSF address for IM CSI~~	~~3.8.5~~	~~C~~	–		–	~~T~~
O-IM-CSI	3.8.1	C	–	C	–	P

Table 5.3 – Overview of IMS subscriber data used for IP Multimedia services

PARAMETER	Subclause	HSS	S-CSCF	IM-SSF	AS	TYPE
VT-IM-CSI	3.8.2	C	–	C	–	P
D-IM-CSI	3.8.3	C	–	C	–	P
GsmSCF address for IM CSI	3.8.4	C	–	–	–	P
IM-SSF address for IM CSI	3.8.5	C	–	–	–	T

Table 5.3A – Overview of PSI user data used for IP Multimedia services

PARAMETER	Subclause	HSS	S-CSCF	IM-SSF	AS	TYPE
• • •						

5.4 Generic Authentication Architecture Service Data Storage

Table 5.4 – Overview of data used for GAA services

PARAMETER	Subclause	HSS	BSF	NAF	TYPE
• • •					
NAF Address	3A.12		M		P
Key Expirytime	3A.13		M	M	T
~~Boostrapping~~Bootstrapping Info Creation Time	3A.14		M	M	T

The possible user's GBA User Security Settings (GUSS) are stored in HSS with User Private Identifier (IMPI) as retrieval key.

The bootstrapping procedure creates a bootstrapping information entity to the BSF with B-TID as retrieval key.

5.5 I-WLAN Service Data Storage

• • •

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
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	**Cable networks and 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	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
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, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2011