International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.366.5

(07/2007)

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

IPCablecom

IP multimedia subsystem Cx and Dx interfaces; Signalling flows and message contents specification

Recommendation ITU-T J.366.5

Recommendation ITU-T J.366.5

IP multimedia subsystem Cx and Dx interfaces; Signalling flows and message contents specification

Summary

Recommendation ITU-T J.366.5 specifies:

1) The interactions between the HSS (home subscriber server) and the CSCF (call session control functions), referred to as the Cx interface.

2) The interactions between the CSCF and the SLF (server locator function), referred to as the Dx interface.

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.366.5	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/.

Table of Contents

Recommendation ITU-T J.366.5

IP multimedia subsystem Cx and Dx interfaces; Signalling flows and message contents specification

1 Scope

This Recommendation specifies:

1) The interactions between the HSS (home subscriber server) and the CSCF (call session control functions), referred to as the Cx interface.

2) The interactions between the CSCF and the SLF (server locator function), referred to as the Dx interface.

The IP multimedia (IM) subsystem stage 2 is specified in [b-3GPP TS 23.228] and the signalling flows for the IP multimedia call control based on SIP and SDP are specified in [b-3GPP TS 24.228].

This Recommendation addresses the signalling flows for Cx and Dx interfaces. It also addresses how the functionality of the Px interface is accomplished.

The Presence Service Stage 2 description (architecture and functional solution) is specified in [b-3GPP TS 23.141].

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 129 228 V6.9.0 (2005-12), *IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents*, are shown in clause 6.

2 References

[ETSI TS 129 228] ETSI TS 129 228 V6.9.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents*.

3 Definitions

This Recommendation uses the terms defined in [ETSI TS 129 228].

4 Abbreviations and acronyms

This Recommendation uses the abbreviations provided in [ETSI TS 129 228].

5 Conventions

This Recommendation uses the conventions provided in [ETSI TS 129 228].

6 Modifications to [ETSI TS 129 228]

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.

1 Scope

This 3GPP Technical Specification (TS) specifies:

1) The interactions between the HSS (Home Subscriber Server) and the CSCF (Call Session Control Functions), referred to as the Cx interface.

2) The interactions between the CSCF and the SLF (Server Locator Function), referred to as the Dx interface.

The IP Multimedia (IM) Subsystem stage 2 is specified in 3GPP TS 23.228 [1] and the signalling flows for the IP multimedia call control based on SIP and SDP are specified in 3GPP TS 24.228 [2].

This document addresses the signalling flows for Cx and Dx interfaces.

This document also addresses how the functionality of Px interface is accomplished.

The Presence Service Stage 2 description (architecture and functional solution) is specified in 3GPP TS 23.141 [10].

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 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 29.228 V6.9.0 IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling Flows and Message Contents Specification TS 29.228 are listed below.

2 References

- 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.366.2 (TS 23.218)

ITU-T J.366.3 (TS 23.228)

ITU-T J.366.4 (TS 24.229)

ITU-T J.366.10 (TS 29.109)

ITU-T J.366.5 (TS 29.228)

ITU-T J.366.6 (TS 29.229)

ITU-T J.366.7 (TS 33.203)

ITU-T J.366.8 (TS 33.210)

ITU-T J.366. 9 (TS 33.220

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

[1] *3GPP TS 23.228: "IP Multimedia (IM) Subsystem – Stage 2".

•••

6.3 Authentication procedures

This procedure is used between the S-CSCF and the HSS to exchange information to support the authentication between the end user and the home IMS network. The procedure is invoked by the S-CSCF, corresponds to the combination of the operations Cx-AV-Req and Cx-AV-Req-Resp (see 3GPP TS 33.203 [3]) and is used:

– To retrieve authentication vectors from the HSS.

– To resolve synchronization failures between the sequence numbers in the UE and the HSS for authentication schemes that support this capability (e.g., IMS-AKA).

This procedure is mapped to the commands Multimedia-Auth-Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.3.1~~– 6.3.5~~ through 6.3.7 detail the involved information elements. Tables 6.3.1, 6.3.2 and 6.3.4 are common to all authentication schemes; Tables 6.3.3 and 6.3.5 are specific to IMS-AKA authentication; Tables 6.3.6 and 6.3.7 are specific to SIP-Digest authentication.

Table 6.3.1 – Authentication Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity (See 7.2)	Public-Identity	M	This information element contains the Public User Identity of the user
Private User Identity (See 7.3)	User-Name	M	This information element contains the Private User Identity
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	M	This information element indicates the number of authentication vectors requested. Certain authentication schemes may not support more than one set of authentication vectors (e.g., SIP-Digest). In these cases, the HSS will ignore the value of this AVP and assume a value of 1.
Authentication Data (See 7.9)	SIP-Auth-Data-Item	M	See Tables 6.3.2 and 6.3.3 for the contents of this information element for IMS-AKA. The content shown in table 6.3.2 shall be used for a normal authentication request; the content shown in table 6.3.3 shall be used for an authentication request after synchronization failure. See Table 6.3.6 for contents of this information element for SIP-Digest.
S-CSCF Name (See 7.4)	Server-Name	M	This information element contains the name (SIP URL) of the S-CSCF.

Table 6.3.1 – Authentication Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Routing Information (See 7.13)	Destination-Host	C	If the S-CSCF knows the HSS name this AVP shall be present. This information is available if the MAR belongs to an already existing registration, e.g., in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g., included in the MAA command. This information may not be available if the command is sent in case of the initial registration. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node, e.g., SLF, based on the Diameter routing table in the client.

Table 6.3.2 – Authentication Data content – Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	This information element indicates the authentication scheme. It shall contain: – "Digest-AKAv1-MD5" if the S-CSCF supports only IMS-AKA – "Unknown" if the S-CSCF supports multiple authentication schemes
Authentication Context (See 7.9.7)	SIP-Authentication-Context	C	It shall contain authentication-related information relevant for performing the authentication. When Authentication Scheme contains "Digest-AKAv1-MD5", this AVP is not used and shall be missing.

Table 6.3.3 – Authentication Data content – Request: Synchronization Failure for IMS-AKA

Information element name	Mapping to Diameter AVP	Cat.	Description
...			

Table 6.3.4 – Authentication Request Response

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	C	Public User Identity. It shall be present when the result is DIAMETER_SUCCESS.
Private User Identity (See 7.3)	User-Name	C	Private User Identity. It shall be present when the result is DIAMETER_SUCCESS.
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	C	This AVP indicates the number of authentication vectors delivered in the Authentication Data information element. It shall be present when the result is DIAMETER_SUCCESS. For SIP-Digest, this AVP shall be set to a value of 1.
Authentication Data (See 7.9)	SIP-Auth-Data-Item	C	If the SIP-Number-Auth-Items AVP is equal to zero or it is not present, then this AVP shall not be present. See Table 6.3.5 for the contents of this information element for IMS-AKA. See Table 6.3.6 for the contents of this information element for SIP-Digest.
Result (See 7.6)	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Table 6.3.5 – Authentication Data content – Response for IMS-AKA

Information element name	Mapping to Diameter AVP	Cat.	Description
• • •			

Table 6.3.6 – Authentication Data content – Response for SIP Digest

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	This information element indicates the authentication scheme. It shall contain "Digest".
Digest Authenticate (See 7.18)	SIP-Digest-Authenticate	M	See Table 6.3.7 for contents of this information element.

Table 6.3.7 – SIP-Digest-Authenticate content – Response for SIP Digest

Information element name	Mapping to Diameter AVP	Cat.	Description
Digest Realm (See 7.18.1)	Digest-Realm	M	This information element corresponds to the realm parameter as defined in IETF RFC 3261 [11].
Digest Domain (See 7.18.2)	Digest-Domain	O	This information element corresponds to the domain parameter as defined in IETF RFC 2617 [16].
Digest Algorithm (See 7.18.3)	Digest-Algorithm	O	This information element corresponds to the algorithm parameter as defined in IETF RFC 2617 [16]. If this information element is empty, then "MD5" is assumed.
Digest QoP (See 7.18.4)	Digest-QoP	O	This information element corresponds to the qop-options parameter as defined in IETF RFC 2617 [16].
Digest HA1 (See 7.18.5)	Digest-HA1	M	This information element corresponds to the operation H(A1) as defined in IETF RFC 2617 [16].
Digest Auth Param (See 7.18.6)	Digest-Auth-Param	O	This information element corresponds to the auth-param parameter as defined in IETF RFC 2617 [16]

6.3.1 Detailed behaviour

The HSS shall~~, in the following order ~~ perform the following steps in the order presented (in case of an error in any of the steps the HSS shall stop processing and return the corresponding error code, see 3GPP TS 29.229 [5]):

1) Check that the Private User Identity and the Public User Identity exist in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2) Check whether the Private and Public User Identities in the request are associated in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

3) Check that the authentication scheme indicated in the request is supported. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_AUTH_SCHEME_UNSUPPORTED.

4) This step is only applicable for IMS-AKA authentication. If the request indicates there is a synchronization failure, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

– If they are identical the HSS shall process AUTS as described in 3GPP TS 33.203 [3] and return the requested authentication information. The Result-Code shall be set to DIAMETER_SUCCESS.

•••

6.7 S-CSCF Assignment

•••

Table 6.7 – Server-Capability associated with feature

Capability	Mandatory or Optional (Note 1)	Description
Support of the feature "Wildcarded PSI"	M	If the S-CSCF does not support the wildcarded PSI it will not be able to take into account the wildcardedPSI public identity received from the HSS in the user profile. The behaviour of the S-CSCF related to this missing data is undefined.
Support of the feature "Display Name"	O	If the S-CSCF does not support the "Display Name" feature it will not be able to take into account the display name received from the HSS. In this situation, the S-CSCF behaves as though the HSS did not transmit the Display Name.
Support of the feature "SIP Digest"	M	If the S-CSCF does not support the "SIP Digest" feature it will not be able to authenticate the user.
NOTE 1 – Mandatory (M) corresponds to Mandatory Capability and means that if an S-CSCF that does not support the feature is selected during the S-CSCF assignment procedure, the feature does not work and no default behaviour is expected. Optional (O) corresponds to an Optional Capability and means that if an S-CSCF that does not support the feature is selected during the S-CSCF assignment procedure, the feature is not realized but will not adversely affect the network.		

• • •

7.9.2 Authentication Scheme

This information element contains the authentication scheme, which is used to encode the authentication parameters.

~~The scheme is "Digest-AKAv1-MD5"~~

7.9.3 Authentication Information

• • •

7.17 Associated Private Identities

This information element indicates to the S-CSCF the Private Identities, which belong to the same IMS Subscription as the Private Identity received in the request command. See 3GPP TS 29.229 [5].

7.18 Digest Authenticate

This information element is composed of the following sub-elements.

7.18.1 Digest Realm

This Information element is part of the Digest authentication challenge, and corresponds to the realm parameter as defined in IETF RFC 3261 [11]. This information element is used to convey the realm to the S-CSCF during the SIP Digest authentication procedure.

7.18.2 Digest Domain

This Information element is part of the Digest authentication challenge, and corresponds to the domain parameter as defined in IETF RFC 2617 [16]. This information element is used to convey the domain to the S-CSCF during the SIP Digest authentication procedure.

7.18.3 Digest Algorithm

This Information element is part of the Digest authentication challenge, and corresponds to the algorithm parameter defined in IETF RFC 2617 [16]. This information element is used to convey the algorithm to the S-CSCF during the SIP Digest authentication procedure.

7.18.4 Digest QoP

This Information element is part of the Digest authentication challenge, and corresponds to the qop-options as defined in IETF RFC 2617 [16]. This information element is used to convey the QoP to the S-CSCF during the SIP Digest authentication procedure. It provides the Quality of Protection indication and has an effect on the digest computation.

7.18.5 Digest HA1

This Information element is part of the Digest authentication challenge, and corresponds to the operation H(A1) as defined in IETF RFC 2617 [16]. This information element is used to convey the HA1 to the S-CSCF during the SIP Digest authentication procedure.

7.18.6 Digest Auth Param

This Information element is part of the Digest authentication challenge, and corresponds to the auth-param as defined in IETF RFC 2617 [16].This information element is used to convey the Auth Param to the S-CSCF during the SIP Digest authentication procedure.

8 Error handling procedures

…

Annex A (normative)

Mapping of Cx operations and terminology to Diameter

A.1 Introduction

…

A.3 Cx message parameters to Diameter AVP mapping

The following table gives an overview about the mapping:

Table A.3.1 – Cx message parameters to Diameter AVP mapping

Cx parameter	AVP Name
Visited Network Identifier	Visited-Network-Identifier
Public Identity	Public-Identity
Private Identity	User-Name
S-CSCF Name	Server-Name
AS Name	
S-CSCF capabilities	Server-Capabilities
Result	Result-Code
	Experimental-Result-Code
User profile	User-Data
Server Assignment Type	Server-Assignment-Type
Authentication data	SIP-Auth-Data-Item
Item Number	SIP-Item-Number
Authentication Scheme	SIP-Authentication-Scheme
Authentication Information	SIP-Authenticate
Authorization Information	SIP-Authorization
Confidentiality Key	Confidentiality-Key
Integrity Key	Integrity-Key
Number Authentication Items	SIP-Number-Auth-Items
Reason for de-registration	Deregistration-Reason
Charging Information	Charging-Information
Routing Information	Destination-Host
Type of Authorization	Authorization-Type
Associated Private Identities	Associated-Identities
Digest Authenticate	Digest-Authenticate
Digest Realm	Digest-Realm
Digest Domain	Digest-Domain
Digest Algorithm	Digest-Algorithm
Digest QoP	Digest-QoP
Digest HA1	Digest-HA1
Digest Auth Param	Digest-Auth-Param

A.4 Message flows

The following message flows give examples regarding which Diameter messages shall be sent in scenarios described in 3GPP TS 23.228 [1].

A.4.1 Registration– user not registered

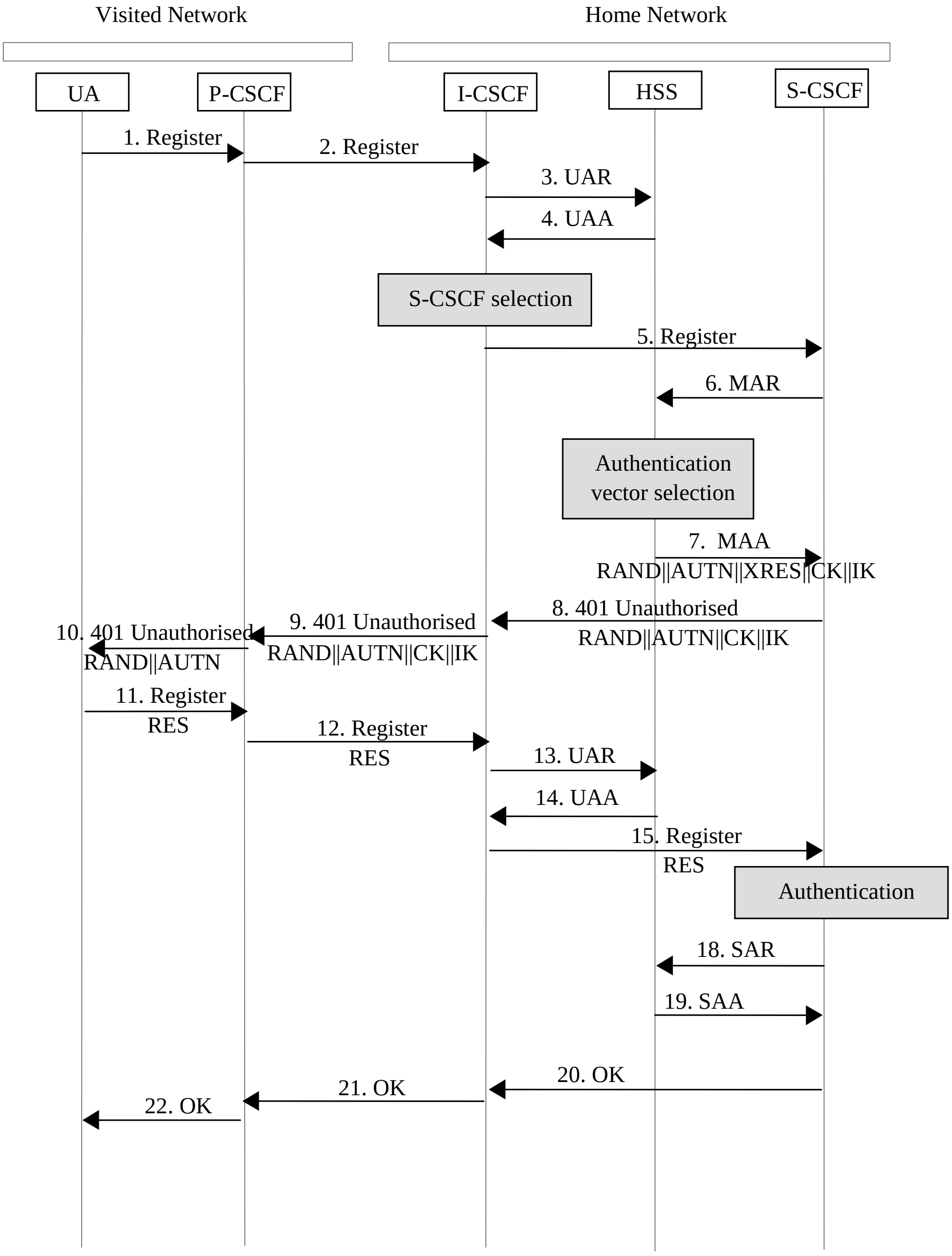

Figure A.4.1.1 – Registration using IMS AKA Authentication – user not registered

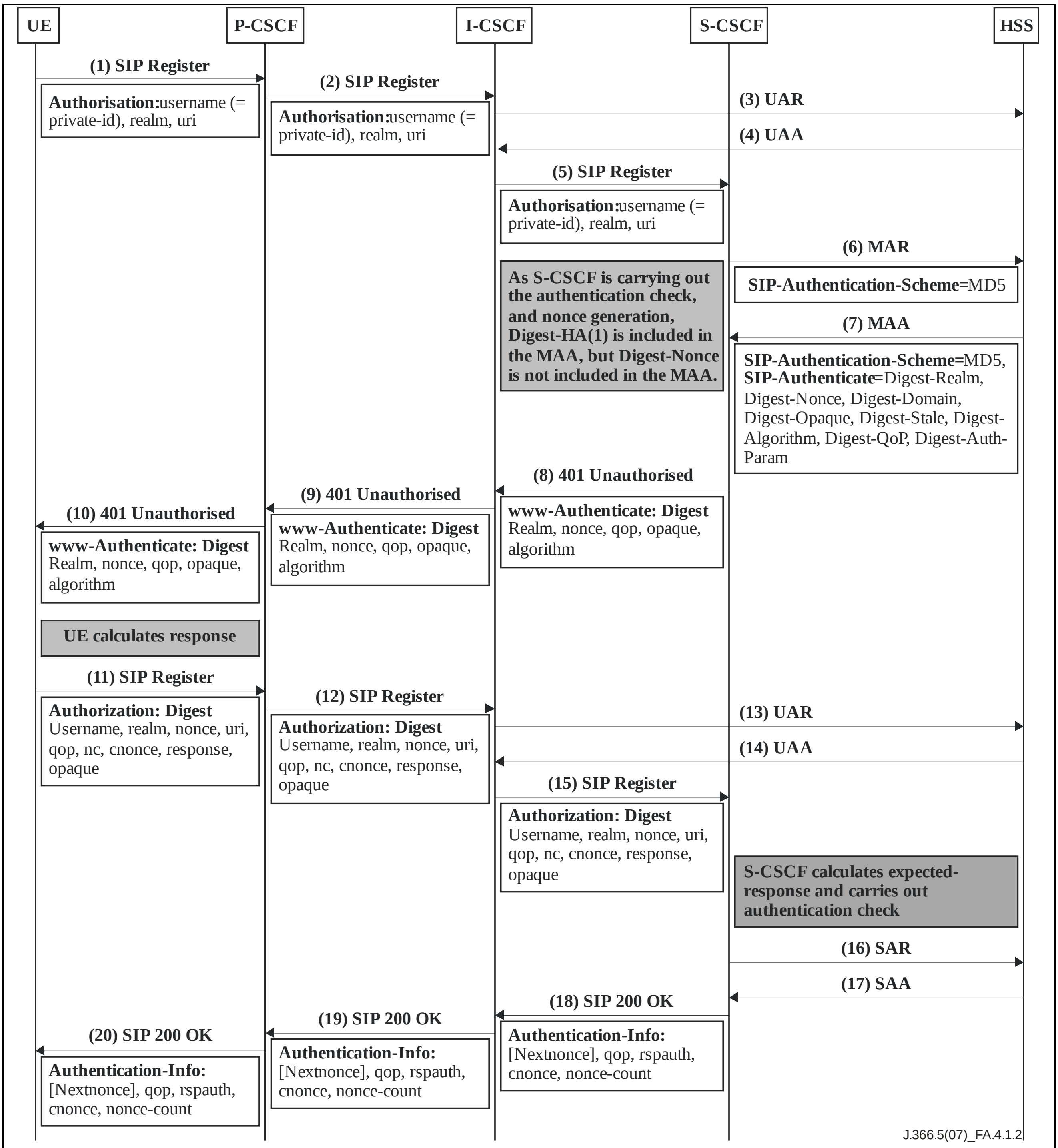
UE
P-CSCF
I-CSCF
S-CSCF
HSS
(1) SIP Register
Authorisation:username (= private-id), realm, uri
(2) SIP Register
Authorisation:username (= private-id), realm, uri
(3) UAR
(4) UAA
(5) SIP Register
Authorisation:username (= private-id), realm, uri
(6) MAR
SIP-Authentication-Scheme=MD5
As S-CSCF is carrying out the authentication check, and nonce generation, Digest-HA(1) is included in the MAA, but Digest-Nonce is not included in the MAA.
(7) MAA
SIP-Authentication-Scheme=MD5, SIP-Authenticate=Digest-Realm, Digest-Nonce, Digest-Domain, Digest-Opaque, Digest-Stale, Digest-Algorithm, Digest-QoP, Digest-Auth-Param
(8) 401 Unauthorised
www-Authenticate: Digest Realm, nonce, qop, opaque, algorithm
(9) 401 Unauthorised
www-Authenticate: Digest Realm, nonce, qop, opaque, algorithm
(10) 401 Unauthorised
www-Authenticate: Digest Realm, nonce, qop, opaque, algorithm
UE calculates response
(11) SIP Register
Authorization: Digest Username, realm, nonce, uri, qop, nc, cnonce, response, opaque
(12) SIP Register
Authorization: Digest Username, realm, nonce, uri, qop, nc, cnonce, response, opaque
(13) UAR
(14) UAA
(15) SIP Register
Authorization: Digest Username, realm, nonce, uri, qop, nc, cnonce, response, opaque
S-CSCF calculates expected-response and carries out authentication check
(16) SAR
(17) SAA
(18) SIP 200 OK
Authentication-Info: [Nextnonce], qop, rspauth, cnonce, nonce-count
(19) SIP 200 OK
Authentication-Info: [Nextnonce], qop, rspauth, cnonce, nonce-count
(20) SIP 200 OK
Authentication-Info: [Nextnonce], qop, rspauth, cnonce, nonce-count
J.366.5(07)_FA.4.1.2

Figure A.4.1.2 – Registration using SIP-Digest authentication– user not registered (Nonce generated in S-CSCF, S-CSCF authenticates the user)

A.4.2 Registration – user currently registered

•••

Annex B (informative)

User profile UML model

…

B.2.1 Public Identification

The following picture gives an outline of the UML model of Public Identification class:

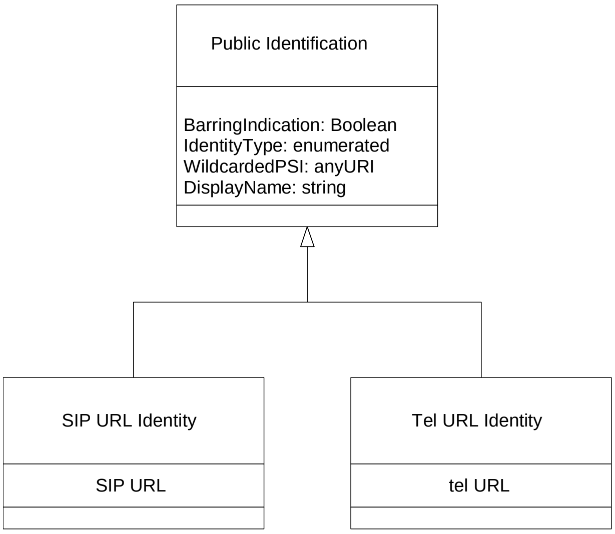

Figure B.2.1.1 – Public Identification

Public Identification class can contain either SIP URL Identity, i.e., SIP URL, or Tel URL Identity class, i.e., tel URL.

The attribute BarringIndication is of type Boolean. If it is set to TRUE, the S-CSCF shall prevent that public identity from being used in any IMS communication except registrations and re-registrations, as specified in 3GPP TS 24.229 [8].

The attribute IdentityType indicates if the identity is a Public User Identity, a distinct Public Service Identity or a Public Service Identity matching a Wildcarded Public Service Identity. If the identity type is not present, it is assumed to be Public User Identity.

The attribute WildcardedPSI shall be present and contain the Wildcarded Public Service Identity that matched the Public Service Identity if the identity is a Public Service Identity matching a Wildcarded Public Service Identity. This Wildcarded Public Service identity shall be sent as stored in the HSS, that is including the delimiter described in 3GPP TS 23.003 [17].

The attribute DisplayName allows a name to be associated with a Public Identity.

B.2.2 Initial Filter Criteria

The following picture gives an outline of the UML model of Initial Filter Criteria class:

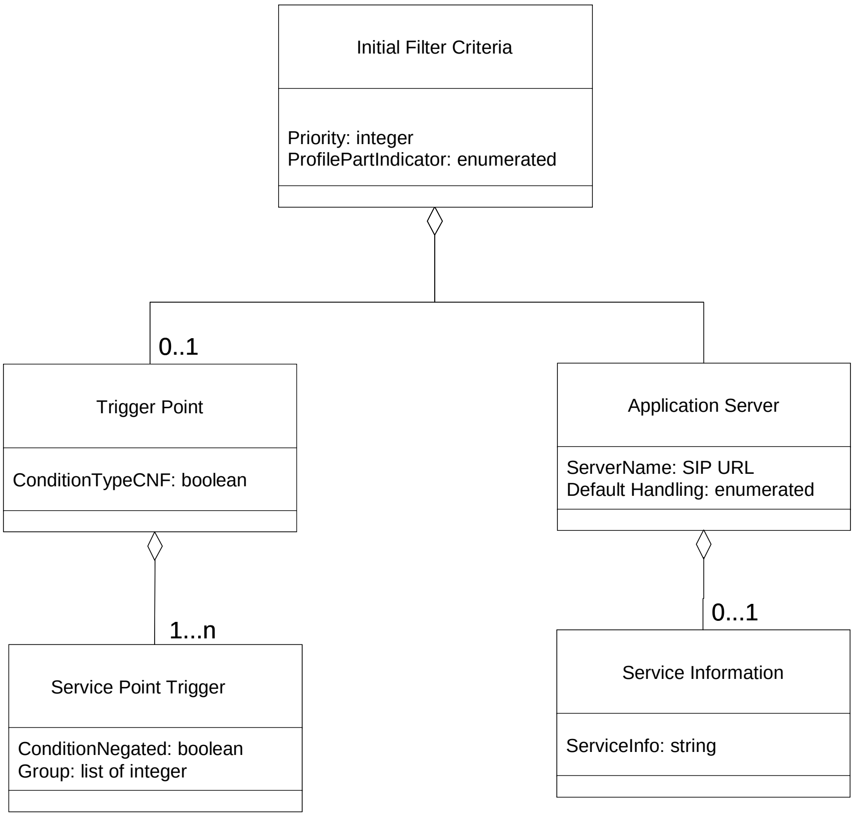

Figure B.2.2.1.1 – Initial Filter Criteria

Each instance of the Initial Filter Criteria class is composed of zero or one instance of a Trigger Point class and one instance of an Application Server class. Priority indicates the priority of the Filter Criteria. The higher the Priority Number the lower the priority of the Filter Criteria is; i.e., a Filter Criteria with a higher value of Priority Number shall be assessed after the Filter Criteria with a smaller Priority Number have been assessed. The same priority shall not be assigned to more than one initial Filter Criterion.

ProfilePartIndicator attribute is an enumerated type, with possible values "REGISTERED and UNREGISTERED, indicating if the iFC is a part of the registered or unregistered user profile. If ProfilePartIndicator is missing from the iFC, the iFC is considered to be relevant to both the registered and unregistered parts of the user profile, i.e., belongs to the common part of the user profile.

Trigger Point class describes the trigger points that should be checked in order to find out if the indicated Application Server should be contacted or not. Each TriggerPoint is a boolean expression in ~~Conjuctive~~Conjunctive or Disjunctive Normal form (CNF of DNF). The absence of Trigger Point instance will indicate an unconditional triggering to Application Server.

The attribute ConditionTypeCNF attribute defines how the set of SPTs are expressed, i.e., either an Ored set of ANDed sets of SPT statements or an ANDed set of Ored sets of statements. Individual SPTstatements can also be negated. These combinations are termed, respectively, Disjunctive Normal Form (DNF) and Conjunctive Normal Form (CNF) for the SPT (see Annex C). Both DNF and CNF forms can be used. ConditionTypeCNF is a boolean that is TRUE when the Trigger Point associated with the FilterCriteria is a boolean ~~expresion~~expression in ~~Conjuctive~~Conjunctive Normal Form (CNF) and FALSE if the Trigger Point is expressed in Disjunctive Normal Form (DNF) (see Annex C).

• • •

B.2.3 Service Point Trigger

•••

Session Case class represents an enumerated type, with possible values "Originating", "Terminating_Registered", "Terminating_Unregistered" indicating if the filter should be used by the S-CSCF handling the Originating, Terminating for a registered end user or Terminating for an unregistered end user services.

Session Description Information class defines ~~SPTfor~~SPT for the content of any SDP field within the body of a SIP Method. The Line attribute identifies the line inside the session description. Content is a string defining the content of the line identified by Line. Perl-like regular expressions shall be taken as a model for regular expressions for this function (as described above).

•••

Annex E (normative)

XML schema for the Cx interface user profile

…

Table E.1 – XML schema for the Cx interface user profile: simple data types

Data type	Tag	Base type	Comments
…			
tBool	ConditionTypeCNF, ConditionNegated, BarringIndication	boolean	Possible values: 0 (false) 1 (true)
tSubscribedMediaProfileId	SubscribedMediaProfileId	integer	>=0
tDisplayName	**DisplayName**	**string**	

Table E.2 – XML schema for the Cx interface user profile: complex data types

Data type	Tag	Compound of		
		Tag	Type	Cardinality
…				
tPublicIdentityExtension	Extension	IdentityType	tIdentityType	(0 to 1)
		WildcardedPSI	tWildcardedPSI	(0 to 1)
		Extension	**tPublicIdentityExtension2**	**(0 to 1)**
tPublicIdentityExtension2	**Extension**	**DisplayName**	**tDisplayName**	**(0 to 1)**
NOTE – "n" shall be interpreted as non-bounded.				

…

Bibliography

[b-3GPP TS 23.141] 3GPP Technical Specification TS 23.141, *Presence service; Architecture and functional description*.

[b-3GPP TS 23.228] 3GPP Technical Specification TS 23.228, *IP Multimedia Subsystem (IMS); Stage 2*.

[b-3GPP TS 24.228] 3GPP Technical Specification TS 24.228, *Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)*.

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