3GPP TSG CT Plenary Meeting #28 **CP-050081**
1st – 3rd June 2005 Quebec, Canada.

Source: TSG CT WG4

Title: Corrections on Cx-interface Rel-5

Agenda item: 8.1

Document for: APPROVAL

Doc-2nd-Level	Spec	CR #	Rev	Rel	Tdoc Title	CAT	C_Version
C4-050848	29.228	189	1	Rel-5	Clarification of the content of SIP-Authetnication-Context	F	5.11.0
C4-050849	29.228	188	1	Rel-6	Clarification of the content of SIP-Authetnication-Context	A	6.6.1
C4-050731	29.228	190	1	Rel-5	Removal of the default handling in the service profile	F	5.11.0

3GPP TSG-CT WG4 Meeting #27 **C4-050731**
Cancun, MEXICO. 25th to 29th April 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **TS 29.228** **CR** **190** ⌘**rev** **1** ⌘ Current version: **5.11.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Removal of the default handling in the service profile
Source:	⌘	Orange
Work item code:	⌘	IMS-CCR
Date:	⌘	15/04/05
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	During the previous CN1 meeting (CN1#37), the CR N1-050287 "Default handling in TS 23.218, Release 5" has been agreed. This CR clarifies in TS 23.218 that the default handling procedure is not supported by the S-CSCF in Release 5. The specification TS 29.228 Release 5 has to be aligned with this change.
Summary of change:	⌘	The default handling defined in the service profile in the Annexes B and C is removed. For forward compatibility issue with release 6, the stage 3 definition of DefaultHandling data type is kept but stated as not to be used by release 5 nodes.
Consequences if not approved:	⌘	Misalignment between the TS 23.218 and the TS 29.228.

Clauses affected:	⌘	Annexes B, C and E and CxDataType.xsd file

		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

*** BEGINNING OF THE FIRST MODIFICATION ***

Annex B (informative):
User profile UML model

The purpose of this UML model is to define in an abstract level the structure of the user profile downloaded over the Cx interface and describe the purpose of the different information classes included in the user profile.

B.1 General description

The following picture gives an outline of the UML model of the user profile, which is downloaded from HSS to S-CSCF:

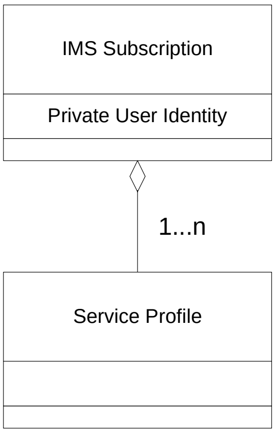

Figure B.1.1: User Profile

IMS Subscription class contains as a parameter the private user identity of the user in NAI format.

Each instance of the IMS Subscription class contains one or several instances of the class Service Profile. Service Profile class contains the meaningful data in the user profile: Public Identification, Core Network Service Authorization and Initial Filter Criteria.

B.2 Service profile

The following picture gives an outline of the UML model of the Service Profile class:

:

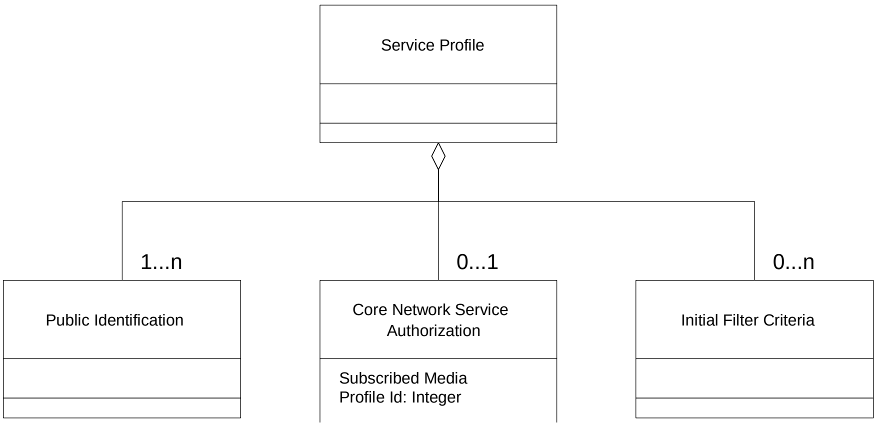

Figure B.2.1: Service Profile

Each instance of the Service Profile class consists of one or several instances of the class Public Identification. Public Identification class contains the public identities of the user associated with that service profile. The information in the Core Network Service Authorization and Initial Filter Criteria classes apply to all public identity instances, which are included in one Service profile class.

Each instance of the Service Profile class contains zero or one instance of the class Core Network Service Authorization. If no instance of the class Core Network Service Authorization is present, no filtering related to subscribed media applies in S-CSCF.

Each instance of the class Service Profile contains zero or several instances of the class Initial Filter Criteria.

B.2.1 Public Identification

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

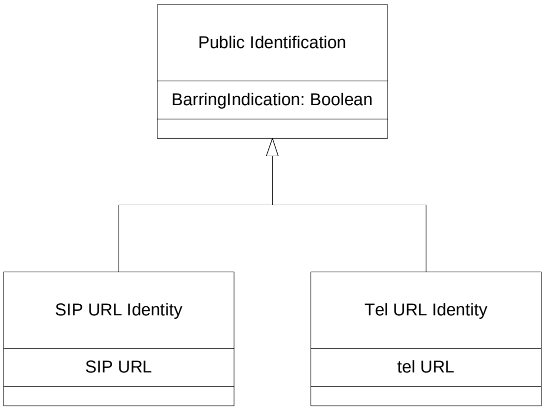

Figure B.2.1.1: Public Identification

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]..

B.2.2 Initial Filter Criteria

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

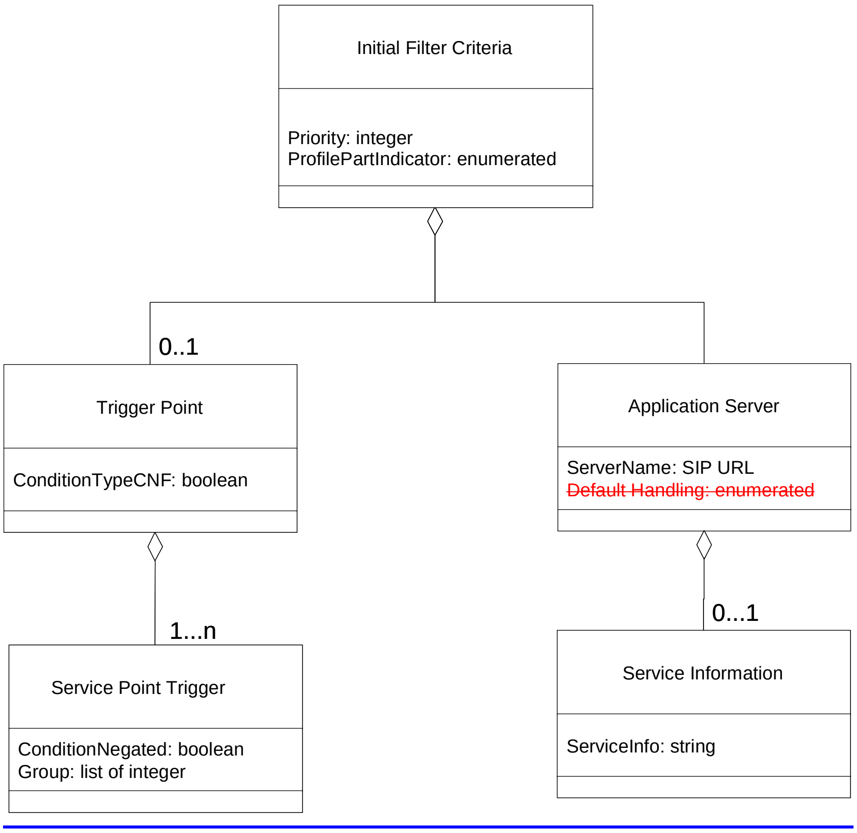

Figure B.2.2.1.1: Initial Filter Criteria

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 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 in Conjuctive Normal Form (CNF) and FALSE if the Trigger Point is expressed in Disjunctive Normal Form (DNF) (see Annex C).

Each Trigger Point is composed by 1 to n instances of the class Service Point Trigger.

Application Server class defines the application server, which is contacted, if the trigger points are met. Server Name is the SIP URL of the application server to contact. ~~Default Handling determines whether the dialog should be released if the Application Server could not be reached or not; it is of type enumerated and can take the values: SESSION_CONTINUED or SESSION_TERMINATED.~~

The Application Server class contains zero or one instance of the Service Information class. Service Information class allows to download to S-CSCF information that is to be transferred transparently to an Application Server when the trigger points of a filter criterion are satisfied. ServiceInformation is a string conveying that information. See 3GPP TS 23.218 [7] for a description of the use of this information element.

B.2.3 Service Point Trigger

The following picture gives an outline of the UML model of Service Point Trigger class:

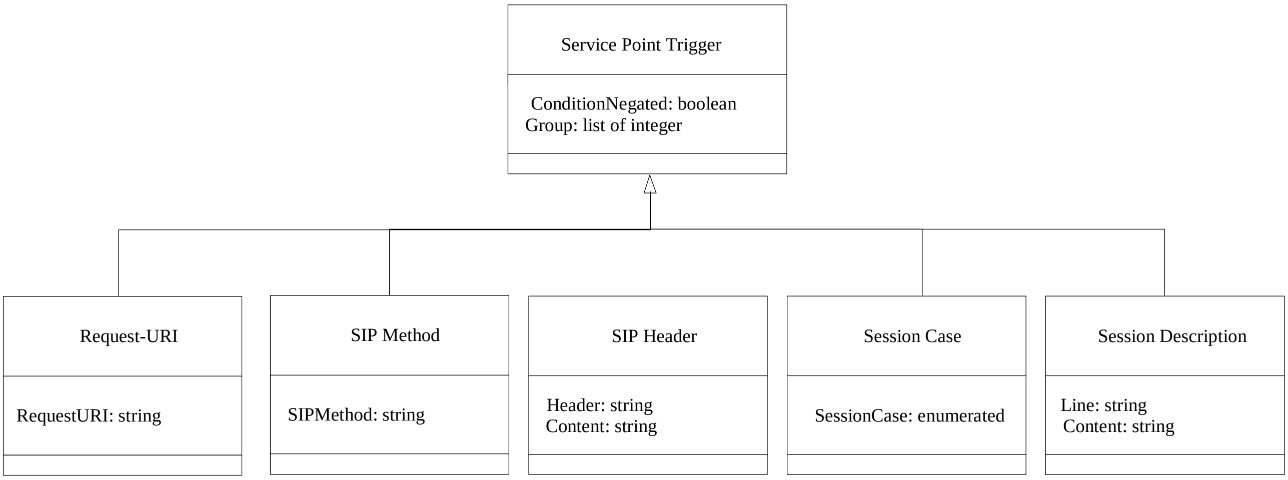

Figure B.2.3.1: Service Point Trigger

The attribute Group of the class Service Point Trigger allows the grouping of SPTs that will configure the sub-expressions inside a CNF or DNF expression. For instance, in the following CNF expression (A+B).(C+D), A+B and C+D would correspond to different groups.

In CNF, the attribute Group identifies the ORed sets of SPT instances. If the SPTbelongs to different ORed sets, SPTcan have more than one Group values assigned. At least one Group must be assigned for each SPT.

In DNF, the attribute Group identifies the ANDed sets of SPT instances. If the SPTbelongs to different ANDed sets, SPTcan have more than one Group values assigned. At least one Group must be assigned for each SPI.

The attribute ConditionNegated of the class Service Point Trigger defines whether the individual SPT instance is negated (i.e. NOT logical expression).

Request-URI class defines SPT for the Request-URI. Request-URI contains attribute RequestURI.

SIP Method class defines SPT for the SIP method. SIP Method contains attribute SIPMethod which can evaluate to any existent SIP method.

SIP Header class defines SPT for the presence or absence of any SIP header or for the content of any SIP header. SIP Header contains attribute Header which identifies the SIP Header, which is the SPT, and the Content attribute defines the value of the SIP Header if required.

The absence of the Content attribute and ConditionNegated = TRUE indicates that the SPTis the absence of a determined SIP header.

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 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.

*** END OF THE FIRST MODIFICATION ***

*** BEGINNING OF THE SECOND MODIFICATION ***

Annex C (informative):
Conjunctive and Disjunctive Normal Form

A Trigger Point expression is constructed out of atomic expressions (i.e. Service Point Trigger) linked by Boolean operators AND, OR and NOT. Any logical expression constructed in that way can be transformed to forms called Conjunctive Normal Form (CNF) and Disjunctive Normal Form (DNF).

A Boolean expression is said to be in Conjunctive Normal Form if it is expressed as a conjunction of disjunctions of literals (positive or negative atoms), i.e. as an AND of clauses, each of which is the OR of one of more atomic expressions.

Taking as an example the following trigger:

Method = “INVITE” OR Method = “MESSAGE” OR (Method=”SUBSCRIBE” AND NOT Header = “from” Content = “joe”)

The trigger can be split into the following atomic expressions:

Method=”INVITE”

Method=”MESSAGE”

Method=”SUBSCRIBE”

NOT header=”from” Content =”joe”

Grouping the atomic expressions, the CNF expression equivalent to the previous example looks like:

(Method=”INVITE” OR Method = “MESSAGE” OR Method=”SUBSCRIBE”) AND (Method=”INVITE” OR Method = “MESSAGE” OR (NOT Header = “from” Content = “joe”))

This result in two “OR” groups linked by “AND” (CNF):

(Method=”INVITE” OR Method = “MESSAGE” OR Method=”SUBSCRIBE”)

(Method=”INVITE” OR Method = “MESSAGE” OR (NOT Header = “from” Content = “joe”))

The XML representation of the trigger is:

```
<?xml version=”1.0” encoding=”UTF-8”?>
<testDatatype xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance” xsi:noNamespaceSchemaLocation=”D:\
\CxDataType.xsd”>
          <IMSSubscription>
            <PrivateID>IMPI1@homedomain.com</PrivateID>
            <ServiceProfile>
                <PublicIdentity>
                    <BarringIndication>1</BarringIndication>
                    <Identity> sip:IMPU1@homedomain.com </Identity>
                </PublicIdentity>
                <PublicIdentity>
                    <Identity> sip:IMPU2@homedomain.com </Identity>
                </PublicIdentity>
                <InitialFilterCriteria>
                    <Priority>0</Priority>
                    <TriggerPoint>
                        <ConditionTypeCNF>1</ConditionTypeCNF>
                        <SPT>
```

```
                            <ConditionNegated>0</ConditionNegated>
                            <Group>0</Group>
                            <Method>INVITE</Method>
                        </SPT>
                        <SPT>
                            <ConditionNegated>0</ConditionNegated>
                            <Group>0</Group>
                            <Method>MESSAGE</Method>
                        </SPT>
                        <SPT>
                            <ConditionNegated>0</ConditionNegated>
                            <Group>0</Group>
                            <Method>SUBSCRIBE</Method>
                        </SPT>
                        <SPT>
                            <ConditionNegated>0</ConditionNegated>
                            <Group>1</Group>
                            <Method>INVITE</Method>
                        </SPT>
                        <SPT>
                            <ConditionNegated>0</ConditionNegated>
                            <Group>1</Group>
                            <Method>MESSAGE</Method>
                        </SPT>

                        <SPT>
                            <ConditionNegated>1</ConditionNegated>
                            <Group>1</Group>
                            <SIPHeader>
                                <Header>From</Header>
                                <Content>”joe”</Content>
                            </SIPHeader>
                        </SPT>
                    </TriggerPoint>
                    <ApplicationServer>
                        <ServerName>sip:AS1@homedomain.com</ServerName>
                        ~~<DefaultHandling>0</DefaultHandling>~~
                    </ApplicationServer>
                </InitialFilterCriteria>
            </ServiceProfile>
          </IMSSubscription>
</testDatatype>
```

A Boolean expression is said to be in Disjunctive Normal Form if it is expressed as a disjunction of conjuctions of literals (positive or negative atoms), i.e. as an OR of clauses, each of which is the AND of one of more atomic expressions.

The previous example is already in DNF, composed by the following groups:

Method=”INVITE”

Method=”MESSAGE”

Method=”SUBSCRIBE” AND (NOT header=”from” Content =”joe”)

The XML representation of the trigger is:

```
<?xml version=”1.0” encoding=”UTF-8”?>
<testDatatype xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance” xsi:noNamespaceSchemaLocation=”D:\CxDataType.xsd”>
          <IMSSubscription>
            <PrivateID>IMPI1@homedomain.com</PrivateID>
          <ServiceProfile>
              <PublicIdentity>
                  <BarringIndication>1</BarringIndication>
                  <Identity> sip:IMPU1@homedomain.com </Identity>
              </PublicIdentity>
              <PublicIdentity>
                  <Identity> sip:IMPU2@homedomain.com </Identity>
              </PublicIdentity>
              <InitialFilterCriteria>
                  <Priority>0</Priority>
                  <TriggerPoint>
                      <ConditionTypeCNF>0</ConditionTypeCNF>
                      <SPT>
                          <ConditionNegated>0</ConditionNegated>
                          <Group>0</Group>
                          <Method>INVITE</Method>
                      </SPT>
                      <SPT>
                          <ConditionNegated>0</ConditionNegated>
                          <Group>1</Group>
                          <Method>MESSAGE</Method>
                      </SPT>
                      <SPT>
                          <ConditionNegated>0</ConditionNegated>
                          <Group>2</Group>
                          <Method>SUBSCRIBE</Method>
                      </SPT>
                      <SPT>
                          <ConditionNegated>1</ConditionNegated>
                          <Group>2</Group>
                          <SIPHeader>
                              <Header>From</Header>
                              <Content>"joe"</Content>
                          </SIPHeader>
                      </SPT>
                  </TriggerPoint>
                  <ApplicationServer>
                      <ServerName>sip:AS1@homedomain.com</ServerName>
                      ~~<DefaultHandling index="0">0</DefaultHandling>~~
                  </ApplicationServer>
              </InitialFilterCriteria>
          </ServiceProfile>
        </IMSSubscription>
</testDatatype>
```

*** END OF THE SECOND MODIFICATION ***

*** BEGINNING OF THE THIRD MODIFICATION ***

Annex E (normative): XML schema for the Cx interface user profile

The file CxDataType.xsd, attached to this specification, contains the XML schema for the Cx interface user profile. Such XML schema details all the data types on which XML documents containing Cx profile information shall be based. The XML schema file is intended to be used by an XML parser.

Table E.1 describes the data types and the dependencies among them that configure the XML schema.

Table E.1: XML schema for Cx interface: simple data types

Data type	Tag	Base type	Comments
tPriority	Priority	integer	>= 0
tProfilePartIndicator	ProfilePartIndicator	enumerated	Possible values: 0 (REGISTERED) 1 (UNREGISTERED)
tGroupID	Group	integer	>= 0
tDefaultHandling (*)	DefaultHandling	enumerated	Possible values: 0 (SESSION_CONTINUED) 1 (SESSION_TERMINATED)
tDirectionOfRequest	SessionCase	enumerated	Possible values: 0 (ORIGINATING_SESSION) 1 TERMINATING_ REGISTERED 2 (TERMINATING_UNREGISTERED)
tPrivateID	PrivateID	anyURI	Syntax described in RFC 2486
tSIP_URL	Identity	anyURI	Syntax described in RFC 3261
tTEL_URL	Identity	anyURI	Syntax described in RFC 2806
tIdentity	Identity	(union)	Union of tSIP_URL and tTEL_URL
tServiceInfo	ServiceInfo	string	
tString	RequestURI, Method, Header, Content, Line	string	
tBool	ConditionTypeCNF, ConditionNegated, BarringIndication	boolean	Possible values: 0 (false) 1 (true)
tSubscribedMediaProfileId	SubscribedMediaProfileId	integer	>=0
(*) the tDefaultHandling is not used in Release 5			

Table E.2: XML schema for Cx interface: complex data types

Data type	Tag	Compound of			
		Tag		Type	Cardinality
tIMSSubscription	IMSSubscription	PrivateID		tPrivateID	1
		ServiceProfile		tServiceProfile	(1 to n)
tServiceProfile	ServiceProfile	PublicIdentity		tPublicIdentity	(1 to n)
		InitialFilterCriteria		tInitialFilterCriteria	(0 to n)
		CoreNetworkServicesAuthorization		CoreNetworkServicesAuthorization	(0 to 1)
tCoreNetworkServicesAuthorization	CoreNetworkServicesAuthorization	SubscribedMediaProfileId		tSubscribedMediaProfileId	(0 to 1)
tPublicIdentity	PublicIdentity	BarringIndication		tBool	1
		Identity		tIdentity	1
tInitialFilterCriteria	InitialFilterCriteria	Priority		tPriority	1
		TriggerPoint		tTrigger	(0 to 1)
		ApplicationServer		tApplicationServer	1
		ProfilePartIndicator		tProfilePartIndicator	(0 to 1)
tTrigger	TriggerPoint	ConditionTypeCNF		tBool	1
		SPT		tSePoTri	(1 to n)
tSePoTri	SPT	ConditionNegated		tBool	(0 to 1)
		Group		tGroupID	(1 to n)
		Choice of	RequestURI	tString	1
			Method	tString	1
			SIPHeader	tHeader	1
			SessionCase	tDirectionOfRequest	1
			SessionDescription	tSessionDescription	1
tHeader	SIPHeader	Header		tString	1

		Content	tString	(0 to 1)
tSessionDescription	SessionDescription	Line	tString	1
		Content	tString	(0 to 1)
tApplicationServer	ApplicationServer	ServerName	tSIP_URL	1
		DefaultHandling (*)	tDefaultHandling	(0 to 1)
		ServiceInfo	tServiceInfo	(0 to 1)
NOTE: "n" shall be interpreted as non-bounded. (*): the DefaultHandling should not be sent by a Rel-5 HSS				

*** END OF THE THIRD MODIFICATION ***

3GPP TSG-CT WG4 Meeting #27 **C4-050848**
Cancun, MEXICO. 25th to 29th April 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.228** **CR** **189** ⌘**rev** **1** ⌘ Current version: **5.11.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Clarification of the content of SIP-Authentication-Context			
Source:	⌘	Ericsson, Vodafone, Nortel			
Work item code:	⌘	IMS-CCR	***Date:***	⌘	28/04/2005
Category:	⌘	**F**	***Release:***	⌘	Rel-5
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.			*Use one of the following releases:* *Ph2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)* *Rel-7 (Release 7)*

Reason for change:	⌘	**This is an essential correction.** 29.229 defines the SIP-Auth-Data-Item that is used in the Mulitmedia-Auth-Response defined in 29.228. SIP-Auth-Data-Item is a grouped AVP which contains the SIP-Authentication-Context shown in 29.229. However the use of SIP-Authentication-Context is unclear as it is not included in 29.228 in the Authentication Data Content.
Summary of change:	⌘	Add SIP-Authentication-Context to 29.228 in the table with the authentication data for the authentication procedures (6.3.3) and a new section with the description of the information element in 7.9. There are also three small editorial corrections in table 6.3.5 and an added reference.
Consequences if not approved:	⌘	The use of SIP-Authentication-Context will be unclear and there will be a mismatch between specifications.

Clauses affected:	⌘	2, 6.3, 7.9				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

>>>>>>>>>>> First modified section <<<<<<<<<<<

2 References

[1] 3GPP TS 23.228: "~~“~~IP Multimedia (IM) Subsystem – Stage 2 (Release 5)"~~”~~.

[2] 3GPP TS 24.228: "~~“~~Signalling flows for the IP multimedia call control based on SIP and SDP"~~”~~.

[3] 3GPP TS 33.203: "~~“~~Access security for IP-based services"~~”~~.

[4] 3GPP TS 23.002 "~~“~~Network architecture"~~”~~.

[5] 3GPP TS 29.229: "~~“~~Cx Interface based on Diameter – Protocol details"~~”~~

[6] 3GPP TS 23.218: "~~“~~IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model"~~”~~

[7] Freed, N. and N. Borestein, "~~“~~Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies"~~”~~, RFC 2045, November 1996.

[8] 3GPP TS 24.229: "~~“~~IP Multimedia Call Control Protocol based on SIP and SDP"~~”~~ – stage 3

[9] IETF RFC 3588 "~~“~~Diameter Base Protocol"~~”~~

[10] IETF RFC 3261 "SIP: Session Initiation Protocol"

[11] IETF RFC 2327 "SDP: Session Description Protocol"

[12] IEEE 1003.1-2004, Part 1: Base Definitions

[XX] IETF RFC 2617 "HTTP Authentication: Basic and Digest Access Authentication"

>>>>>>>>>>> End of first modified section <<<<<<<<<<<

>>>>>>>>>>> Second modified section <<<<<<<<<<<

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-Put (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.

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 detail the involved information elements.

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 identity of the user
Private User Identity (See 7.3)	User-Name	M	This information element contains the user private identity
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	M	This information element indicates the number of authentication vectors requested
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. 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.
S-CSCF Name (See 7.4)	Server-Name	M	This information element contains the name (SIP URL) of the S-CSCF.
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. For 3GPP R5 it shall contain “Digest-AKAv1-MD5”.
Authentication Context (See 7.9.X)	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

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For 3GPP R5 it shall contain “Digest-AKAv1-MD5”.
Authorization Information (See 7.9.4)	SIP-Authorization	M	It shall contain the concatenation of nonce, as sent to the terminal, and auts, as received from the terminal. Nonce and auts shall both be binary encoded.

Table 6.3.4: Authentication answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	C	User public identity. It shall be present when the result is DIAMETER_SUCCESS.
Private User Identity (See 7.3)	User-Name	C	User private 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.
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.
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

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number (See 7.9.1)	SIP-Item-Number	C	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of

			SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For 3GPP R5 it shall contain “Digest-AKAv1-MD5”.
Authentication Information (See 7.9.3)	SIP-Authenticate	M	It shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN.
Authorization Information (See 7.9.4)	SIP-Authorization	M	It shall contain, binary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES.
Confidentiality Key (See 7.9.5)	Confidentiality-Key	O	This information element, if present, shall contain the confidentiality key. It shall be binary encoded.
Integrity Key (See 7.9.6)	Integrity-Key	M	This information element shall contain the integrity key. It shall be binary encoded.

6.3.1 Detailed behaviour

The HSS shall, in the following order (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 user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. The HSS may check that the private and public identities belong to the same user. 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. 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.

5. Check the registration status of the public identity received in the request:

   - If it is registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

     - If they are different, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

     - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The Result-Code shall be set to DIAMETER_SUCCESS.

   - If it is unregistered (i.e. registered as a consequence of a terminating call to unregistered user or there is an S-CSCF keeping the user profile stored) or not registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

- If they are different or if there is no S-CSCF name stored in the HSS for any identity of the IMS subscription, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

- If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

Exceptions to the cases specified here shall be treated by HSS as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY. No authentication information shall be returned.

>>>>>>>>>>> End of second modified section <<<<<<<<<<<

>>>>>>>>>>> Third modified section <<<<<<<<<<<

7.9 Authentication Data

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

7.9.1 Item Number

This information element indicates the order in which the authentication vectors are to be consumed.

7.9.2 Authentication Scheme

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

For 3GPP Release 5 this scheme is "Digest-AKAv1-MD5".

7.9.3 Authentication Information

This information element is used to convey the challenge and authentication token user during the authentication procedure. See 3GPP TS 33.203 [3] for details.

7.9.4 Authorization Information

This information element is used, in an authentication request, to indicate a failure of synchronization. In a response, it is used to convey the expected response to the challenge used to authenticate the user. See 3GPP TS 33.203 [3].

7.9.5 Confidentiality Key

This information element contains the confidentiality key. See 3GPP TS 33.203 [3].

7.9.6 Integrity Key

This information element contains the integrity key. See 3GPP TS 33.203 [3].

7.9.X Authentication Context

This information element contains authentication-related information relevant for performing the authentication but that is not part of the SIP authentication headers. Some mechanisms (e.g. PGP, digest with quality of protection set to auth-int defined in IETF RFC 2617 [XX], digest with predictive nonces or sip access digest) request that part or the whole SIP request (e.g. the SIP method) is passed to the entity performing the authentication. In such cases the SIP-Authentication-Context AVP shall be carrying such information.

>>>>>>>>>>> End of third modified section <<<<<<<<<<<

3GPP TSG-CT WG4 Meeting #27 **C4-050849**
Cancun, MEXICO. 25th to 29th April 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.228**	**CR**	**188**	⌘ **rev**	**-**	⌘	Current version:	**6.6.1** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Clarification of the content of SIP-Authentication-Context		
Source:	⌘	Ericsson, Vodafone, Nortel		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	28/04/2005
Category:	⌘	**A**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	29.229 defines the SIP-Auth-Data-Item that is used in the Mulitmedia-Auth-Response defined in 29.228. SIP-Auth-Data-Item is a grouped AVP which contains the SIP-Authentication-Context shown in 29.229. However the use of SIP-Authentication-Context is unclear as it is not included in 29.228 in the Authentication Data Content.
Summary of change:	⌘	Add SIP-Authentication-Context to 29.228 in the table with the authentication data for the authentication procedures (6.3.3) and a new section with the description of the information element in 7.9. There are also three small editorial corrections in table 6.3.5 and an added reference.
Consequences if not approved:	⌘	The use of SIP-Authentication-Context will be unclear and there will be a mismatch between specifications.

Clauses affected:	⌘	2, 6.3, 7.9			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

>>>>>>>>>>> First modified section <<<<<<<<<<<

2 References

[1] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – Stage 2 (Release 5)".

[2] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP".

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

[4] 3GPP TS 23.002 "Network architecture".

[5] 3GPP TS 29.229: "Cx Interface based on Diameter – Protocol details"

[6] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model"

[7] Freed, N. and N. Borestein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[8] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP" – stage 3

[9] IETF RFC 3588 "Diameter Base Protocol"

[10] 3GPP TS 23.141: "Presence Service; Architecture and Functional Description"

[11] IETF RFC 3261 "SIP: Session Initiation Protocol"

[12] IETF RFC 2337 "SDP: Session Description Protocol"

[13] IEEE 1003.1-2004, Part 1: Base Definitions

[XX] IETF RFC 2617 "HTTP Authentication: Basic and Digest Access Authentication"

>>>>>>>>>>> End of first modified section <<<<<<<<<<<

>>>>>>>>>>> Second modified section <<<<<<<<<<<

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-Put (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.

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 detail the involved information elements.

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 identity of the user
Private User Identity (See 7.3)	User-Name	M	This information element contains the user private identity
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	M	This information element indicates the number of authentication vectors requested
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. 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.
S-CSCF Name (See 7.4)	Server-Name	M	This information element contains the name (SIP URL) of the S-CSCF.
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".
Authentication Context (See 7.9.X)	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

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. It shall contain "Digest-AKAv1-MD5".
Authorization Information (See 7.9.4)	SIP-Authorization	M	It shall contain the concatenation of nonce, as sent to the terminal, and auts, as received from the terminal. Nonce and auts shall both be binary encoded.

Table 6.3.4: Authentication answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	C	User public identity. It shall be present when the result is DIAMETER_SUCCESS.
Private User Identity (See 7.3)	User-Name	C	User private 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.
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.
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

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number (See 7.9.1)	SIP-Item-Number	C	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. It shall contain "Digest-AKAv1-MD5".
Authentication Information (See 7.9.3)	SIP-Authenticate	M	It shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN.
Authorization Information (See 7.9.4)	SIP-Authorization	M	It shall contain, binary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES.
Confidentiality Key (See 7.9.5)	Confidentiality-Key	O	-This information element, if present, shall contain the confidentiality key. It shall be binary encoded.
Integrity Key (See 7.9.6)	Integrity-Key	M	-This information element shall contain the integrity key. It shall be binary encoded.

6.3.1 Detailed behaviour

The HSS shall, in the following order (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 user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.
2. The HSS may check that the private and public identities belong to the same user. 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. 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.
5. Check the registration status of the public identity received in the request:
    - If it is registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:
        - If they are different, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The HSS shall set the public identity's authentication pending flag which is specific to the private identity which was received in the request. The Result-Code shall be set to DIAMETER_SUCCESS.

  - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The Result-Code shall be set to DIAMETER_SUCCESS.

- If it is unregistered (i.e. registered as a consequence of a terminating call to unregistered user or there is an S-CSCF keeping the user profile stored) or not registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

  - If they are different or if there is no S-CSCF name stored in the HSS for any identity of the IMS subscription, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The HSS shall set the public identity's authentication pending flag which is specific to the private identity which was received in the request. The Result-Code shall be set to DIAMETER_SUCCESS.

- If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The HSS shall set the public identity's authentication pending flag which is specific to the private identity that was received in the request. The Result-Code shall be set to DIAMETER_SUCCESS.

Exceptions to the cases specified here shall be treated by HSS as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY. No authentication information shall be returned.

>>>>>>>>>>> End of second modified section <<<<<<<<<<<

>>>>>>>>>>> Third modified section <<<<<<<<<<<

7.9 Authentication Data

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

7.9.1 Item Number

This information element indicates the order in which the authentication vectors are to be consumed.

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

This information element is used to convey the challenge and authentication token user during the authentication procedure. See 3GPP TS 33.203 [3] for details.

7.9.4 Authorization Information

This information element is used, in an authentication request, to indicate a failure of synchronization. In a response, it is used to convey the expected response to the challenge used to authenticate the user. See 3GPP TS 33.203 [3].

7.9.5 Confidentiality Key

This information element contains the confidentiality key. See 3GPP TS 33.203 [3].

7.9.6 Integrity Key

This information element contains the integrity key. See 3GPP TS 33.203 [3].

7.9.X Authentication Context

This information element contains authentication-related information relevant for performing the authentication but that is not part of the SIP authentication headers. Some mechanisms (e.g. PGP, digest with quality of protection set to auth-int defined in IETF RFC 2617 [XX], digest with predictive nonces or sip access digest) request that part or the whole SIP request (e.g. the SIP method) is passed to the entity performing the authentication. In such cases the SIP-Authentication-Context AVP shall be carrying such information.

>>>>>>>>>>> End of third modified section <<<<<<<<<<<