3GPP TSG CT Plenary Meeting #28 **CP-050086**
1st – 3rd June 2005 Quebec, Canada.

Source: TSG CT WG4

Title: Corrections on IP-based multimedia services on Cx-interface

Agenda item: 9.1

Document for: APPROVAL

Doc-2nd-Level	Spec	CR #	Rev	Rel	Tdoc Title	CAT	C_Version
C4-050559	29.228	181		Rel-6	TEL-URI reference correction	F	6.6.1
C4-050584	29.228	183		Rel-6	Clarification on Server Capabilities	F	6.6.1
C4-050606	29.228	185		Rel-6	Incorrect Implementation of CR172	F	6.6.1
C4-050742	29.228	192		Rel-6	Syntax correction for XML	F	6.6.1
C4-050676	29.229	087		Rel-6	Correction of reference	F	6.4.0
C4-050800	29.229	089	1	Rel-6	Editorial corrections	F	6.4.0
C4-050887	29.229	088	2	Rel-6	Corrections to message parameters	F	6.4.0

3GPP TSG-CT WG4 Meeting #27 **C4-050559**
Cancun, MEXICO. 25th to 29th April 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.228** **CR** **181** ⌘ **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:	⌘	TEL-URI reference correction
Source:	⌘	Nokia
Work item code:	⌘	IMS2-CCR
Date:	⌘	14/04/2005
Category:	⌘	**F**
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:	⌘	IETF RFC 2806 has been obsoleted by IETF RFC 3966. SA2 and CT1 have updated Rel-6 specs regarding this change.
Summary of change:	⌘	IETF RFC 3966 is referenced for TEL-URI. The RFCs that are referred in Annex E are added to Section 2.
Consequences if not approved:	⌘	Stage 3 specifications are not in sync with stage 2 specifications. Rel-6 29.229 refers to an obsoleted RFC.

Clauses affected:	⌘	2, Annex E

Other specs affected: ⌘	Y	N	
		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.

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 2486 "The Network Access Identifier"

[yy] IETF RFC 3966 "The tel URI for Telephone Numbers"

***** next modified section *****

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 user profile that is sent over the Cx interface. The user profile XML schema defines that are used in the user profile XML. The data that is allowed to be sent in the user profile may vary depending on the features supported by the Diameter end points, see 3GPP TS 29.229 [5]. The user profile XML schema file is intended to be used by an XML parser. The version of the Cx application sending the user profile XML shall be the same as the version of the sent user profile XML and thus it implies the version of the user profile XML schema to be used to validate it.

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

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

Data type	Tag	Base type	Comments
tPriority	Priority	integer	>= 0
tProfilePartIndicator	ProfilePartIndicator	enumerated	Possible values: 0 (REGISTERED) 1 (UNREGISTERED)
tSharedIFCSetID	SharedIFCSetID	integer	>= 0
tGroupID	Group	integer	>= 0
tRegistrationType	RegistrationType	enumerated	Possible values: 0 (INITIAL_REGISTRATION) 1 (RE-REGISTRATION) 2 (DE-REGISTRATION)
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 IETF RFC 2486 [xx]
tSIP_URL	Identity	anyURI	Syntax described in IETF RFC 3261 [11]
tTEL_URL	Identity	anyURI	Syntax described in IETF RFC ~~280~~3966 [yy]
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)
tSubscribedMediaPr	SubscribedMediaPr	integer	>=0

ofileId	ofileId		

3GPP TSG-CT WG4 Meeting #27 **C4-050584**
Cancun, MEXICO. 25th to 29th April 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.228** **CR** **183** ⌘ **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 on Server Capabilities
Source:	⌘	Siemens
Work item code:	⌘	IMS2-CCR
Date:	⌘	11/04/2005
Category:	⌘	**F**
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:	⌘	to clarify that the HSS shall return to the I-CSCF all server capabilities associated with the IMS subscription.
Summary of change:	⌘	replace the sentence "The returned capabilities must satisfy the most restrictive service profile of the user." with "The returned capabilities must satisfy all the requirements of all the service profiles associated with the IMS subscription."
Consequences if not approved:	⌘	Given two service profiles it is not defined which one is more restrictive. This may lead to selecting an inappropriate S-CSCF.

Clauses affected:	⌘	6.1.1.1

Other specs affected: ⌘	Y	N	
		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.

6.1.1.1 Detailed behaviour

The HSS shall, in the following order (if there is an error in any of the following 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. Check that the private and public identities received in the request belong to the same user. If not Experimental-Result-Code shall be set to DIAMETER_ERROR _IDENTITIES_DONT_MATCH.

3. Check whether the public identity received in the request is barred for the establishment of multimedia sessions.

   - If it is, the HSS shall check whether there are other non-barred public identities to be implicitly registered with that one.

     - If so, continue to step 4.

     - If not, Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED.

4. Check the User-Authorization-Type received in the request:

   - If it is REGISTRATION or if User-Authorization-Type is absent from the request, the HSS shall check that the user is allowed to roam in the visited network (if not Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED). Continue to step 5.

   - If it is DE_REGISTRATION, the HSS may not perform any check regarding roaming. Continue to step 5.

   - If it is REGISTRATION_AND_CAPABILITIES, the HSS shall check that the user is allowed to roam in the visited network (if not Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED). The HSS shall return the Server-Capabilities AVP, which enables the I-CSCF to select an S-CSCF. The returned capabilities must satisfy all the requirements of all ~~most~~ the ~~restrictive~~ service profiles associated with ~~of~~ the IMS subscription~~user~~. The Server-Capabilities AVP may be absent, to indicate to the I-CSCF that it can select any available S-CSCF. Result-Code shall be set to DIAMETER_SUCCESS. The HSS shall not return any S-CSCF name. Stop processing.

5. Check the state of the public identity received in the request:

   - If it is registered, the HSS shall return the stored S-CSCF name. No S-CSCF capabilities shall be present in the response. If User-Authorization-Type is equal to REGISTRATION, Experimental-Result-Code shall be set to DIAMETER_SUBSEQUENT_REGISTRATION. If User-Authorization-Type is equal to DE-REGISTRATION, Result-Code shall be set to DIAMETER_SUCCESS.

   - If it is unregistered (i.e registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored) and User-Authorization-Type is equal to DE-REGISTRATION, Result-Code shall be set to DIAMETER_SUCCESS. If the User-Authorization-Type is equal to REGISTRATION, then:

     - If the selection of a new S-CSCF is not necessary, the HSS shall return the stored S-CSCF name and the Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.

     - Otherwise, the HSS shall return the name of the S-CSCF assigned to the unregistered user, the S-CSCF capabilities and the Experimental-Result-Code set to DIAMETER_SERVER_SELECTION. Considering the information received from the HSS, the I-CSCF shall determine whether or not it has to select a new S-CSCF.

- If it is not registered yet, the HSS shall check the value of User-Authorization-Type received in the request:
  - If the value of User-Authorization-Type is DE_REGISTRATION, then the HSS shall not return any S-CSCF name or S-CSCF capabilities. The HSS shall set the Experimental-Result-Code to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED in the response.
  - If the value of User-Authorization-Type is REGISTRATION, then the HSS shall check if there is at least one identity of the user with an S-CSCF name assigned.
    - If there is at least one identity of the user that is registered the HSS shall return the S-CSCF name assigned for the user and Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
    - If there is at least one identity of the user that is unregistered (i.e registered as a consequence of a terminating call or there is an S-CSCF keeping the user profile stored), then:
      - If the selection of a new S-CSCF is not necessary, the HSS shall return the stored S-CSCF name and the Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
      - Otherwise, the HSS shall return the name of the S-CSCF assigned to the unregistered user, the S-CSCF capabilities and the Experimental-Result-Code set to DIAMETER_SERVER_SELECTION. Considering the information received from the HSS, the I-CSCF shall determine whether or not it has to select a new S-CSCF.
    - If there is not any identity of the user with an S-CSCF name assigned, then the HSS shall return the Server-Capabilities AVP, which enables the I-CSCF to select an S-CSCF. The returned capabilities shall satisfy all the requirements of all the ~~most restrictive~~ service profiles associated with ~~of~~ the IMS subscription ~~user~~. The Server-Capabilities AVP may be absent, to indicate to the I-CSCF that it may select any available S-CSCF. Experimental-Result-Code shall be set to DIAMETER_FIRST_REGISTRATION. The HSS shall not return any S-CSCF name.

If the HSS cannot fulfil received request, e.g. due to database error, it shall set Result-Code to DIAMETER_UNABLE_TO_COMPLY. No S-CSCF name or S-CSCF capabilities shall be present in the response.

3GPP TSG-CT WG4 Meeting #27 **C4-050606**
Cancun, MEXICO. 25th to 29th April 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.228** **CR** **185** ⌘ **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:	⌘	Incorrect Implementation of CR172
Source:	⌘	Nortel
Work item code:	⌘	IMS-CCR2
Date:	⌘	14/04/2005
Category:	⌘	**F**
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:	⌘	CN4#26 in Sydney agreed N4-050197 CR172 to align 29.228 and 33.203 regarding the distribution of the Cipher Key and Integrity Key to the P-CSCF. 29.228 Annex A.4.1 was modified to show that the Cipher Key and Intergity Key are distributed to the P-CSCF from the S-CSCF with RAND||AUTN when the user is unauthorised. However, updated figure was added in addition to the existing figure rather than replacing it in 29.228 6.6.1.
Summary of change:	⌘	Remove the redundant Figure A.4.1.1 to show that the Cipher Key and the Integrity Key are sent to the P-CSCF with RAND||AUTN when the user is unauthorised.
Consequences if not approved:	⌘	Misalignment between specifications leading to interoperability issues.

Clauses affected:	⌘	A.4.1

Other specs affected:	⌘	Y	N		⌘
			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.

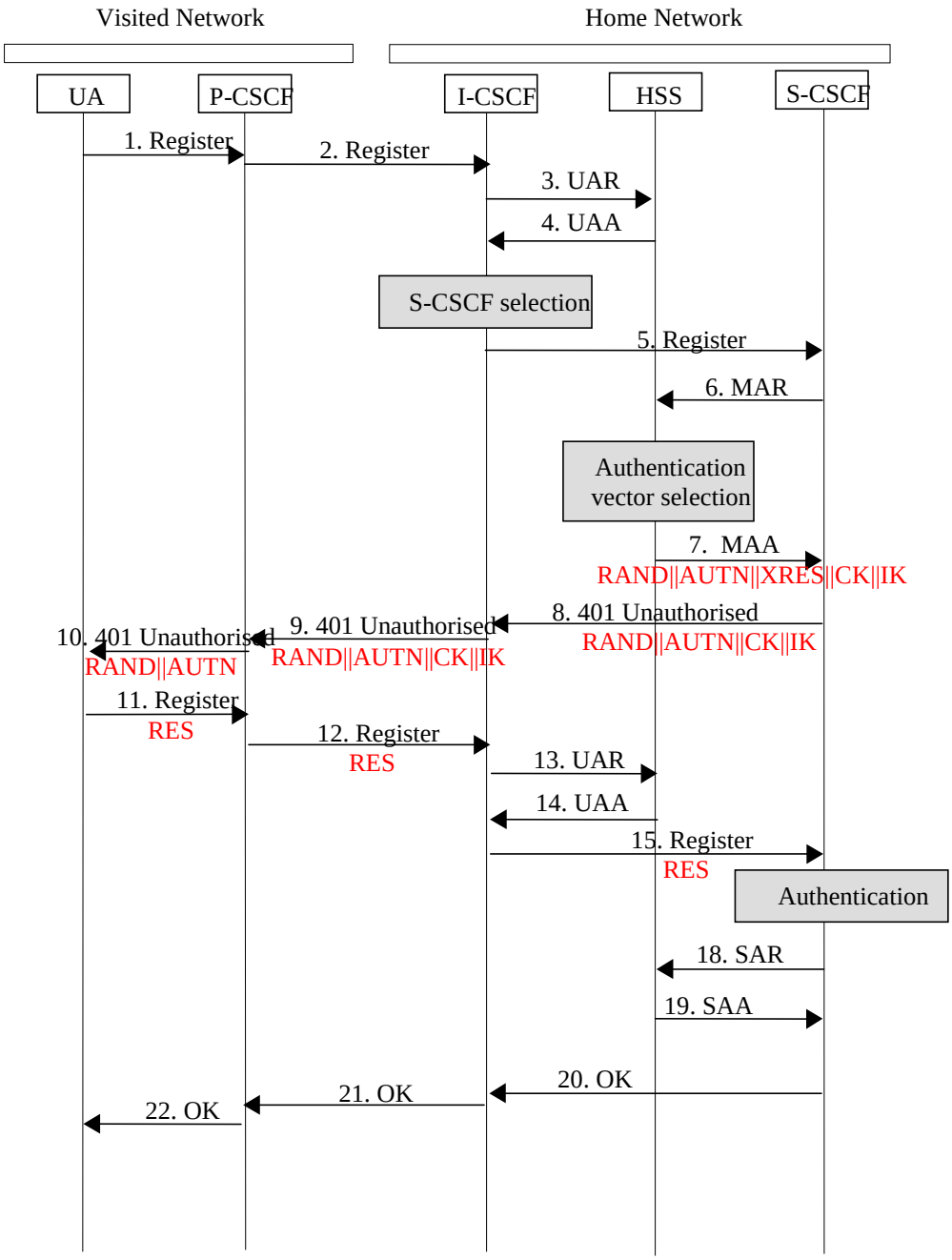
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

*** First Modification ***

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


Visited Network
Home Network
UA
P-CSCF
I-CSCF
HSS
S-CSCF
1. Register
2. Register
3. UAR
4. UAA
S-CSCF selection
5. Register
6. MAR
Authentication vector selection
7. MAA
RAND||AUTN||XRES||CK||IK
8. 401 Unauthorised
RAND||AUTN||CK||IK
9. 401 Unauthorised
RAND||AUTN||CK||IK
10. 401 Unauthorised
RAND||AUTN
11. Register
RES
12. Register
RES
13. UAR
14. UAA
15. Register
RES
Authentication
18. SAR
19. SAA
20. OK
21. OK
22. OK

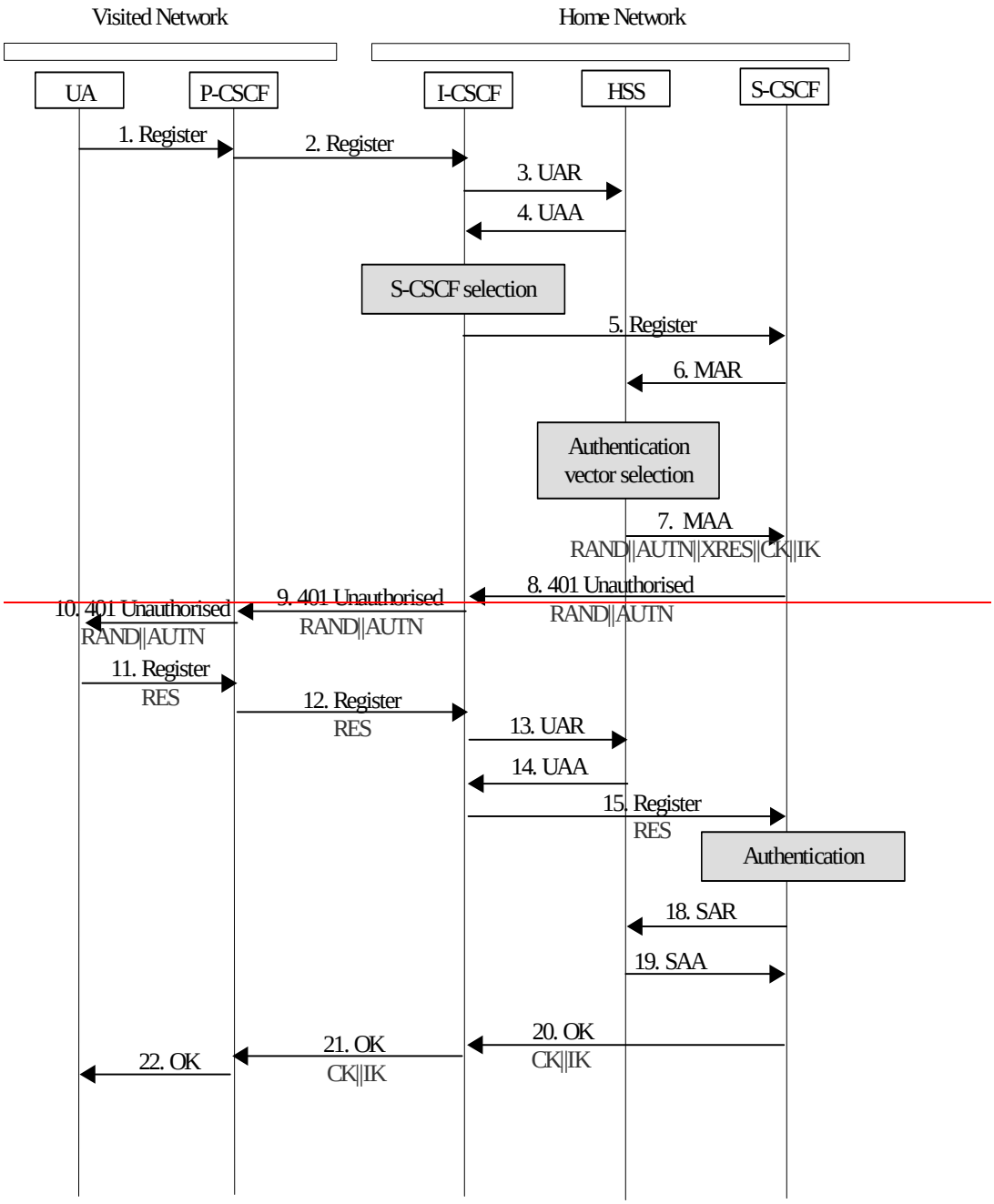


Figure A.4.1.1: Registration – user not registered

3GPP TSG-CT WG4 Meeting #27 **C4-050676**
Cancun, MEXICO. 25th to 29th April 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.229** **CR** **087** ⌘ **rev** **-** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Correction of references to latest release
Source:	⌘	Qualcomm Incorporated
Work item code:	⌘	IMS2-CCR
Date:	⌘	13/4/2005
Category:	⌘	**F**
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:	⌘	Several references to 3GPP TS reference specifically Release 5 versions. Release 6 versions of these documents are now available. The references need to be modified to reflect this.
Summary of change:	⌘	References are corrected to refer to the versions in the same release as the current document
Consequences if not approved:	⌘	The document will refer to Release 5 specifications and hence implementations conforming to it would not be able to support Release 6 enhancements.
Clauses affected:	⌘	2

	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 reques

2 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*.

[1] 3GPP TS 29.228 "IP Multimedia (IM) Subsystem Cx and Dx interface; signalling flows and message contents ~~(Release 5)~~ "

[2] 3GPP TS 33.210 "3G Security; Network Domain Security; IP Network Layer Security ~~(Release 5)~~ "

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

[4] IETF RFC 2396: "Uniform Resource Identifiers (URI): generic syntax"

[5] IETF RFC 2960 "Stream Control Transmission Protocol"

[6] IETF RFC 3588 "Diameter Base Protocol"

[7] IETF RFC 2234 "Augmented BNF for syntax specifications"

[8] IETF RFC 3966 "The tel URI for Telephone Numbers"

[9] void

[10] IETF RFC 3309: "SCTP Checksum Change"

[11] 3GPP TS 29.329 "Sh Interface based on the Diameter protocol; protocol details"

[12] IETF RFC 3589 "Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5"

3GPP TSG-CT WG4 Meeting #27 **C4-050742**
Cancun, MEXICO. 25th to 29th April 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.228** **CR** **192** ⌘ **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:	⌘	Syntax correction for XML
Source:	⌘	Siemens
Work item code:	⌘	IMS2-CCR
Date:	⌘	22/04/2005
Category:	⌘	**F**
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:	⌘	to correct the syntax of the .xml file in order to allow XML-parsers to successfully parse the file.
Summary of change:	⌘	correct quotation in .xsd file
Consequences if not approved:	⌘	incorrect syntax

Clauses affected:	⌘	.xsd file which is attached to the spec

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

Other comments:	⌘	The proposed modification does not affect the spec but only the .xsd file which is attached to the spec.

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.

3GPP TSG-CT WG4 Meeting #27 **C4-050800**
Cancun, MEXICO. 25th to 29th April 2005. **(Revision of C4-050678)**

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.229** **CR** **089** ⌘ **rev** **1** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Miscellaneous corrections
Source:	⌘	Qualcomm Incorporated
Work item code:	⌘	IMS2-CCR
Date:	⌘	26/4/2005
Category:	⌘	**F**
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:	⌘	Removing erroneous statements, improved readability, incorrect section numbers and material not referenced elsewhere
Summary of change:	⌘	See below
Consequences if not approved:	⌘	Incorrect statements lead to incorrect implementations leading to interoperability problems
Clauses affected:	⌘	1, 5, 5.3, 5.6, 6.1.2, 6.1.4, 6.1.6, 6.1.8, 6.1.9, 6.1.10, 6.1.12, 6.2.1, 6.2.1.1, 6.2.2.10, 6.3, 6.3.3, 6.3.8, 6.3.10, 6.3.11, 6.3.14, 6.3.15, 6.3.31, 6.4.2, 7.1, 7.1.1, 7.1.2, 7.2, 7.2.1

		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 reques

1 Scope

The present document defines a transport protocol for use in the IP multimedia (IM) Core Network (CN) subsystem based on Diameter.

The present document is applicable to:

- The Cx interface between the I-CSCF/S-CSCF and the HSS.
- The Dx interface between the I-CSCF/S-CSCF and the SLF.

Whenever it is possible, this document specifies the requirements for this protocol by reference to specifications produced by the IETF within the scope of Diameter. Where this is not possible, extensions to Diameter are defined within this document.

[…]

5 Use of the Diameter base protocol

With the clarifications listed in the following subclauses, the Diameter Base Protocol defined by IETF RFC 3588 [6] shall apply.

[…]

5.3 Use of sessions

Both between the I-CSCF and the HSS and between the S-CSCF and the HSS, Diameter sessions are implicitly terminated. An implicitly terminated session is one for which the server does not maintain state information. The client does not need to send any re-authorization or session termination requests to the server.

The Diameter base protocol includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in IETF RFC 3588 [6]. As a consequence, the server does not maintain any state information about this session and the client does not need to send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

[…]

5.6 Advertising Application Support

The HSS, S-CSCF and I-CSCF shall advertise support of the Diameter Multimedia Application by including the value of the application identifier (see chapter 6) in the Auth-Application-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

~~the~~The vendor identifier value of 3GPP (10415) shall be included in the Supported-Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands, and in the Vendor-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

Note: The Vendor-Id AVP included in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands that is not included in the Vendor-Specific-Application-Id AVPs as described above shall indicate the manufacturer of the Diameter node as per RFC 3588 [6].

6 Diameter application for Cx interface

[...]

6.1.2 User-Authorization-Answer (UAA) Command

The User-Authorization-Answer (UAA) command, indicated by the Command-Code field set to 300 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the User-Authorization-Request command. The ~~Result-Code AVP or~~ Experimental-Result AVP may contain one of the values defined in section 6.2 ~~in addition to the values defined in IETF RFC 3588 [6]~~.

Message Format

< User-Authorization-Answer> ::= < Diameter Header: 300, PXY, 16777216 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
***[Supported-Features]**
[Server-Name]
[Server-Capabilities]
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

[...]

6.1.4 Server-Assignment-Answer (SAA) Command

The Server-Assignment-Answer (SAA) command, indicated by the Command-Code field set to 301 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Server-Assignment-Request command. The ~~Result-Code or~~ Experimental-Result AVP may contain one of the values defined in section 6.2 ~~in addition to the values defined in IETF RFC 3588 [6]~~. If Result-Code or Experimental-Result does not inform about an error, the User-Data AVP shall contain the information that the S-CSCF needs to give service to the user.

Message Format

<Server-Assignment-Answer> ::= < Diameter Header: 301, PXY, 16777216 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
***[Supported-Features]**
[User-Data]
[Charging-Information]
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

[…]

6.1.6 Location-Info-Answer (LIA) Command

The Location-Info-Answer (LIA) command, indicated by the Command-Code field set to 302 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Location-Info-Request command. The ~~Result-Code or~~ Experimental-Result AVP may contain one of the values defined in section 6.2 ~~in addition to the values defined in IETF RFC 3588 [6]~~.

Message Format

<Location-Info-Answer> ::= < Diameter Header: 302, PXY, 16777216 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
***[Supported-Features]**
[Server-Name]
[Server-Capabilities]
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

6.1.8 Multimedia-Auth-Answer (MAA) Command

The Multimedia-Auth-Answer (MAA) command, indicated by the Command-Code field set to 303 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Multimedia-Auth-Request command. The ~~Result-Code or~~ Experimental-Result AVP may contain one of the values defined in section 6.2 ~~in addition to the values defined in IETF RFC 3588 [6]~~.

Message Format

< Multimedia-Auth-Answer > ::= < Diameter Header: 303, PXY, 16777216 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
***[Supported-Features]**
[Public-Identity]
[SIP-Number-Auth-Items]
***[SIP-Auth-Data-Item]**
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

6.1.9 Registration-Termination-Request (RTR) Command

The Registration-Termination-Request (RTR) command, indicated by the Command-Code field set to 304 and the 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia server to a Diameter Multimedia client in order to request the de-registration of a user.

Message Format

<Registration-Termination-Request> ::= < Diameter Header: 304, REQ, PXY, 16777216 >

< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User-Name }
***[Supported-Features]**
***[Public-Identity]**
{ DerRegistration-Reason }
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.10 Registration-Termination-Answer (RTA) Command

The Registration-Termination-Answer (RTA) command, indicated by the Command-Code field set to 304 and the 'R' bit cleared in the Command Flags field, is sent by a client in response to the Registration-Termination-Request command. The ~~Result-Code or~~ Experimental-Result AVP may contain one of the values defined in section 6.2 ~~in addition to the values defined in IETF RFC 3588 [6]~~.

Message Format

<Registration-Termination-Answer> ::= < Diameter Header: 304, PXY, 16777216 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
***[Supported-Features]**
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

[…]

6.1.12 Push-Profile-Answer (PPA) Command

The Push-Profile-Answer (PPA) command, indicated by the Command-Code field set to 305 and the 'R' bit cleared in the Command Flags field, is sent by a client in response to the Push-Profile-Request command. The ~~Result-Code or~~ Experimental-Result AVP may contain one of the values defined in section 6.2 ~~in addition to the values defined in IETF RFC 3588 [6]~~.

Message Format

< Push-Profile-Answer > ::=< Diameter Header: 305, PXY, 16777216 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
***[Supported-Features]**
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

6.2 Result-Code AVP values

This section defines new result code values that must be supported by all Diameter implementations that conform to this specification. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and Result-Code AVP shall be absent.

6.2.1 Success

Result codes ~~Errors~~ that fall within the Success category are used to inform a peer that a request has been successfully completed.

6.2.1.1 DIAMETER_FIRST_REGISTRATION (2001)

The HSS informs the I-CSCF that:

- The user is authorized to register this public identity;
- A S-CSCF shall be assigned to ~~that~~ the user.

[...]

6.2.2 Permanent Failures

[...]

6.2.2.10 DIAMETER_MISSING_USER_ID (5010)

The HSS informs the S-CSCF that the message did not contain a Private Identity~~Private Id~~ and/or a Public Identity~~Public Id~~ and so the message could not be processed.

[...]

6.3 AVPs

The following table describes the Diameter AVPs defined for the Cx interface protocol, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in this specification shall be set to 3GPP (10415).

Table 6.3.1: Diameter Multimedia Application AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
Visited-Network-Identifier	600	6.3.1	OctetString	M, V				No
Public-Identity	601	6.3.2	UTF8String	M, V				No
Server-Name	602	6.3.3	UTF8String	M,V				No
Server-Capabilities	603	6.3.4	Grouped	M, V				No
Mandatory-Capability	604	6.3.5	Unsigned32	M, V				No
Optional-Capability	605	6.3.6	Unsigned32	M, V				No

User-Data	606	6.3.7	OctetString	M, V				No
SIP-Number-Auth-Items	607	6.3.8	Unsigned32	M, V				No
SIP-Authentication-Scheme	608	6.3.9	UTF8String	M, V				No
SIP-Authenticate	609	6.3.10	OctetString	M, V				No
SIP-Authorization	610	6.3.11	OctetString	M, V				No
SIP-Authentication-Context	611	6.3.12	OctetString	M, V				No
SIP-Auth-Data-Item	612	6.3.13	Grouped	M, V				No
SIP-Item-Number	613	6.3.14	Unsigned32	M, V				No
Server-Assignment-Type	614	6.3.15	Enumerated	M, V				No
Deregistration-Reason	615	6.3.16	Grouped	M, V				No
Reason-Code	616	6.3.17	Enumerated	M, V				No
Reason-Info	617	6.3.18	UTF8String	M, V				No
Charging-Information	618	6.3.19	Grouped	M, V				No
Primary-Event-Charging-Function-Name	619	6.3.20	DiameterURI	M, V				No
Secondary-Event-Charging-Function-Name	620	6.3.21	DiameterURI	M, V				No
Primary-Charging-Collection-Function-Name	621	6.3.22	DiameterURI	M, V				No
Secondary-Charging-Collection-Function-Name	622	6.3.23	DiameterURI	M, V				No
User-Authorization-Type	623	6.3.24	Enumerated	M, V				No
User-Data-Already-Available	624	6.3.26	Enumerated	M, V				No
Confidentiality-Key	625	6.3.27	OctetString	M, V				No
Integrity-Key	626	6.3.28	OctetString	M, V				No
~~User-Data-Request-Type~~	~~627~~	~~6.3.25~~	~~Enumerated~~	~~M, V~~				~~No~~
Supported-Features	628	6.3.29	Grouped	V	M			No
Feature-List-ID	629	6.3.30	Unsigned32	V			M	No
Feature-List	630	6.3.31	Unsigned32	V			M	No
Supported-Applications	631	6.3.32	Grouped	V			M	No

NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see IETF RFC 3588 [6].
NOTE 2: Depending on the concrete command.

[…]

6.3.3 Server-Name AVP

The Server-Name AVP~~3~~ is of type UTF8String. This AVP contains a SIP-URL (as defined in IETF RFC 3261 [3] and IETF RFC 2396 [4]), used to identify a SIP server (e.g. S-CSCF name).

[…]

6.3.8 SIP-Number-Auth-Items AVP

The SIP-Number-Auth-Items AVP is of type Unsigned32 ~~and indicates the number of authentication vectors provided by the Diameter server~~.

When used in a request, the SIP-Number-Auth-Items~~it~~ indicates the number of authentication vectors~~SIP-Auth-Data-Item's~~ the S-CSCF is requesting. This can be used, for instance, when the client is requesting several pre-calculated authentication vectors. In the answer message, the SIP-Number-Auth-Items AVP indicates the actual number of SIP-Auth-Data-Item AVPs ~~items~~ provided by the Diameter server.

[…]

6.3.10 —SIP-Authenticate AVP

The SIP-Authenticate AVP is of type OctetString and contains specific parts of the data portion of the WWW-Authenticate or Proxy-Authenticate SIP headers that are to be present in a SIP response. The identification and encoding of the specific parts are defined in 3GPP TS 29.228 [1].

6.3.11 —SIP-Authorization AVP

The SIP-Authorization AVP is of type OctetString and contains specific parts of the data portion of the Authorization or Proxy-Authorization SIP headers suitable for inclusion in a SIP request. The identification and encoding of the specific parts are defined in 3GPP TS 29.228 [1].

[…]

6.3.14 SIP-Item-Number AVP

The SIP-Item-Number AVP is of type Unsigned32, and is included in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVP~~s~~, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVP~~s~~ with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.

6.3.15 Server-Assignment-Type AVP

The Server-Assignment-Type AVP is of type Enumerated, and indicates the type of server update being performed in a Server-Assignment-Request operation. The following values are defined:

NO_ASSIGNMENT (0)

This value is used to request from HSS the user profile assigned to one or more public identities, without affecting the registration state of those identities.

REGISTRATION (1)

The request is generated as a consequence of a first registration of an identity.

RE_REGISTRATION (2)

The request corresponds to the re-registration of an identity.

UNREGISTERED_USER (3)

The request is generated because the S-CSCF received an INVITE for a public identity that is not registered.

TIMEOUT_DEREGISTRATION (4)

The SIP registration timer of an identity has expired.

USER_DEREGISTRATION (5)

The S-CSCF has received a user initiated de-registration request.

TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME (6)

The SIP registration timer of an identity has expired. The S-CSCF keeps the user data stored in the S-CSCF and requests HSS to store the S-CSCF name.

USER_DEREGISTRATION_STORE_SERVER_NAME (7)

The S-CSCF has received a user initiated de-registration request. The S-CSCF keeps the user data stored in the S-CSCF and requests HSS to store the S-CSCF name.

ADMINISTRATIVE_DEREGISTRATION (8)

The S-CSCF, due to administrative reasons, has performed the de-registration of an identity.

AUTHENTICATION_FAILURE (9)

The authentication of a user has failed.

AUTHENTICATION_TIMEOUT (10)

The authentication timeout has occurred~~expired~~.

DEREGISTRATION_TOO_MUCH_DATA (11)

The S-CSCF has requested user profile information from the HSS and has received a volume of data higher than it can accept.

[…]

6.3.31 Feature-List AVP

The Feature-List AVP is of type Unsigned32 and it contains a bit mask indicating the supported features of an application. For the Cx application, the meaning of the bits has been defined in 7.1.1~~y~~.

[…]

6.4 Use of namespaces

[…]

6.4.2 Experimental-Result-Code AVP values

This specification has assigned Experimental-Result-Code AVP values 2001-2005 and 5001-5011~~0~~. See section 6.2.

[....]

7 Special Requirements

7.1 Version Control

New functionality - i.e. functionality beyond the Rel-5 standard - shall be introduced by post-Rel-5 versions of this specification to the Diameter applications as follows:

1. If possible, the new functionality shall be defined optional.
2. If backwards incompatible changes can not be avoided, the new functionality should be introduced as a feature, see 7.1.1~~3~~.
3. If the change would be backwards incompatible even as if it was defined as a feature, a new version of the interface shall be created by changing the application identifier of the Diameter application, see 7.1.2.

7.1.1 Defining a new feature

The base functionality for the Cx is the 3GPP Rel-5 standard and a feature is an extension to that functionality. A feature is a functional entity that has a significant meaning to the operation of a Diameter application i.e. a single new parameter without a substantial meaning to the functionality of the Diameter endpoints should not be defined to be a new feature. If the support for a feature is defined mandatory in a post-Rel-5 versions of this specification, the feature concept enables interworking between Diameter endpoints regardless of whether they support all, some or none of the features of the application. Features should be defined so that they are independent from one another.

The content of a feature shall be defined as a part of the specification of the affected application messages. If new AVPs are added to the commands because of the new feature, the new AVPs shall have the 'M' bit cleared and the AVP shall not be defined mandatory in the command ABNF. The support for a feature may be defined to be mandatory behaviour of a node.

The following table of features shall apply to the Cx interface.

Table 7.1.1: Features of Feature-List-ID 1 used in Cx

Feature bit	Feature	M/O	Description
0	SiFC	O	Shared iFC sets This feature is applicable for the SAR/SAA and PPR/PPA command pairs. If both the HSS and the S-CSCF support this feature, subsets of Initial Filter Criteria may be shared by several service profiles and the HSS shall download the shared iFC sets implicitly by downloading the unique identifiers of the shared iFC sets to the S-CSCF. By means of a locally administered database, the S-CSCF then maps the downloaded identifiers onto the shared iFC sets. If the S-CSCF does not support this feature, the HSS shall not download identifiers of shared iFC sets. Instead as a default behavior the HSS shall (by means of a locally administered database) download the iFCs of a shared iFC set explicitly. If the HSS does not support this feature, no special default behaviour is required for the S-CSCF. Note: In using this feature option, the network operator is responsible for keeping the local databases in the S-CSCFs and HSSs consistent.

Feature bit: The order number of the bit within the Supported-Features AVP, e.g. “1”. Feature: A short name that can be used to refer to the bit and to the feature, e.g. “MOM”. M/O: Defines if the implementation of the feature is mandatory (“M”) or optional (“O”). Description: A clear textual description of the feature.

The origin host may discover the supported features of the destination host with the dynamic discovery mechanism defined in 7.2 or via local O&M interfaces.

7.1.2~~1~~ Changing the version of the interface

The version of an interface shall be changed by a future version of this specification only if there is no technically feasible means to avoid backwards incompatible changes to the Diameter application, i.e. to the current version of the interface. However, if the incompatible changes can be capsulated within a feature, there is no need to change the version of the interface. The versioning of an interface shall be implemented by assigning a new application identifier for the interface. This procedure is in line with the Diameter base protocol (see IETF RFC 3588) which defines that if an incompatible change is made to a Diameter application, a new application identifier shall be assigned for the Diameter application.

The following table shall apply to the Cx interface, column Application identifier lists the used application identifiers on Cx and 3GPP.

Table 7.1.y: Application identifiers used in Cx

Application identifier	First applied
16777216	3GPP Rel-5

The origin host may discover which versions of an interface the destination host supports within the capabilities exchange (i.e. CER/CEA command), via the error messages defined in the chapter 7.3 or via local O&M interfaces.

7.2 Supported features

Features that are not indicated in the Supported-Features AVPs within a given application message shall not be used to construct that message. A request application message shall always be compliant with the list of supported features indicated in the Supported-Features AVPs within the application message. If a feature does not effect on constructing an application message, the message is by definition compliant with the feature. If no features are indicated in the application message, no features - i.e. no extensions to Rel-5 - shall be used to construct the application message. An answer application message shall always indicate in the Supported-Features AVPs the complete set of features supported by the sender of the answer application message. An answer application message shall be compliant with the features commonly supported by the sender of the request and answer application messages.

The sender of a request application message shall discover for a given application message pair which features a destination host supports as described in 7.2.1. The discovery of the supported features shall apply only to the exchanged application message pair type, the discovered features of one command pair shall not be applicable to other command pairs within the application. Different commands within an application may support a different set of features. After discovering the features a destination host supports for a given application message pair, the sender of the request application message may store the information on the supported features of the destination host and it may use the features the destination host supports to construct the subsequent~~next~~ request application messages sent to the destination host.

7.2.1 Dynamic discovery of supported features

When sending a request application message to a destination host whose supported features the sender does not know, the request application message shall include the Supported-Features AVP containing the complete set of features supported by the sender. An exception to this is where the origin host does not use any features to construct the request application message and it is not prepared to accept an answer application message which is constructed by making use

of any features. For this exception, the origin host need not include the Supported-Features AVP within the message. The Supported-Features AVP within a request application message shall always have the 'M' bit set and within an answer application message the AVP shall never have the 'M' bit set.

On receiving a request application message, the destination host shall do one of the following:

- If it supports all features indicated in the Supported-Features AVPs within the request message, the answer application message shall include Supported-Features AVPs identifying the complete set of features that it supports. The Experimental-Result-Code AVP shall not be set to DIAMETER_FEATURE_UNSUPPORTED.

- If the request application message does not contain any Supported-Features AVPs, the answer application message shall include either Supported-Features AVPs identifying the complete set of features that it supports or, if it does not support any features, no Supported-Features AVPs shall be present. The Experimental-Result-Code AVP shall not be set to DIAMETER_FEATURE_UNSUPPORTED.

- If it is a post Rel-5 destination host and it does not support all the features indicated in the Supported-Features AVPs, it shall return the answer application message with the Experimental-Result-Code AVP set to DIAMETER_FEATURE_UNSUPPORTED and it shall include also Supported-Features AVPs containing lists of all features that it supports.

- If it is a Rel-5 destination host and it receives a request application message containing Supported-Features AVPs, it will return the answer application message with the Result-Code AVP set to DIAMETER_AVP_UNSUPPORTED and a FAILED_AVP AVP containing at least one Supported-Features AVP as received in the request application message.

If an answer application message is received with the Experimental-Result-Code AVP set to DIAMETER_FEATURE_UNSUPPORTED or with the Result-Code AVP set to DIAMETER_AVP_UNSUPPORTED, the sender of the request application message may, based on the information in the received Supported-Features AVP or the lack of the AVP in the message, re-send the Diameter message containing only the common supported features.

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

C4-050887
(Revision of C4-050778)

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.229** **CR** **088** ⌘ **rev** **2** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Correction to message parameters
Source:	⌘	Qualcomm Incorporated
Work item code:	⌘	IMS2-CCR
Date:	⌘	30/4/2005
Category:	⌘	**F**
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:	⌘	The ABNF description of grouped AVPs is missing items (AVP code and vendor id) in the header
Summary of change:	⌘	Complete ABNF is provided
Consequences if not approved:	⌘	The description will remain incomplete

Clauses affected:	⌘	6.3.4, 6.3.13, 6.3.16, 6.3.19, 6.3.29, 6.3.32

	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 reques

6.3.4 Server-Capabilities AVP

The Server-Capabilities AVP is of type Grouped. This AVP contains information to assist the I-CSCF in the selection of an S-CSCF.

AVP format

Server-Capabilities ::= <AVP header: 603 10415~~TBD~~>

*[Mandatory-Capability]

*[Optional-Capability]

*[Server-Name]

*[AVP]

6.3.13 SIP-Auth-Data-Item AVP

The SIP-Auth-Data-Item is of type Grouped, and contains the authentication and/or authorization information for the Diameter client.

AVP format

SIP-Auth-Data-Item :: = < AVP Header : 612 10415~~TBD~~ >

[SIP-Item-Number]

[SIP-Authentication-Scheme]

[SIP-Authenticate]

[SIP-Authorization]

[SIP-Authentication-Context]

[Confidentiality-Key]

[Integrity-Key]

* [AVP]

[…]

6.3.16 Deregistration-Reason AVP

The Deregistration-Reason AVP is of type Grouped, and indicates the reason for a de-registration operation.

AVP format

Deregistration-Reason :: = < AVP Header : 615 10415~~TBD~~ >

{ Reason-Code }

[Reason-Info]

* [AVP]

[…]

6.3.19 Charging-Information AVP

The Charging-Information is of type Grouped, and contains the addresses of the charging functions.

AVP format

Charging-Information :: = < AVP Header : 618 10415~~TBD~~ >

[Primary-Event-Charging-Function-Name]

[Secondary-Event-Charging-Function-Name]

{ Primary-Charging-Collection-Function-Name }

[Secondary-Charging-Collection-Function-Name]

*[AVP]

[…]

6.3.29 Supported-Features AVP

The Supported-Features AVP is of type Grouped. If this AVP is present it may inform the destination host about the features that the origin host supports. The Feature-List AVP contains a list of supported features of the origin host. The Vendor-ID AVP and the Feature-List AVP shall together identify which feature list is carried in the Supported-Features AVP.

Where a Supported-Features AVP is used to identify features that have been defined by 3GPP, the Vendor-ID AVP shall contain the vendor ID of 3GPP. Vendors may define proprietary features, but it is strongly recommended that the possibility is used only as the last resort. Where the Supported-Features AVP is used to identify features that have been defined by a vendor other than 3GPP, it shall contain the vendor ID of the specific vendor in question.

If there are multiple feature lists defined by the same vendor, the Feature-List-ID AVP shall differentiate those lists from one another. The destination host shall use the value of the Feature-List-ID AVP to identify the feature list.

AVP format

Supported-Features ::= <AVP header: 628 10415~~xx~~>

{ Vendor-ID }

{ Feature-List-ID }

{ Feature-List }

*[AVP]

[…]

6.3.32 Supported-Applications AVP

The Supported-Applications AVP is of type Grouped and it contains the supported application identifiers of a Diameter node.

AVP format

Supported-Applications ::= <AVP header: 631 10415~~xx~~>

*{ Auth-Application-Id }

*{ Acct-Application-Id }

*{ Vendor-Specific-Application-Id }

*[AVP]