3GPP TSG CN Plenary Meeting #27 **NP-050030**
9th – 11th March 2005 Tokyo, JAPAN.

Source: TSG CN WG4

Title: Corrections on Cx/Dx-interface Rel-5

Agenda item: 8.1

Document for: APPROVAL

Doc-2nd-Level	Spec	CR	Rev	Phase	Subject	Cat	Ver_C
N4-050147	29.228	165		Rel-5	Avoiding undesired deregistration	F	5.10.0
N4-050148	29.228	166		Rel-6	Avoiding undesired deregistration	A	6.5.0
N4-050331	29.228	177		Rel-5	HSS initiated deregistration using the network initiated de-registration procedure	F	5.10.0
N4-050336	29.229	81	1	Rel-5	Introduction of Failed AVP	F	5.9.0
N4-050337	29.229	82	1	Rel-6	Introduction of Failed AVP	A	6.3.0
N4-050456	29.229	077	2	Rel-5	Correction of Authentication-related AVPs	F	5.9.0
N4-050457	29.229	078	2	Rel-6	Correction of Authentication-related AVPs	A	6.3.0
N4-050334	29.228	167	1	Rel-5	Correction to authentication procedures in not registered case	F	5.10.0
N4-050335	29.228	168	1	Rel-6	Correction to authentication procedures in not registered case	A	6.5.0

3GPP TSG-CN WG4 Meeting #26 **N4-050147**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.228 CR 165** ⌘ **rev** **-** ⌘ Current version: **5.10.0** ⌘

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:	⌘	Avoiding undesired deregistration		
Source:	⌘	CN4		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	04/02/2005
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. When the HSS receives a MAR command for a user from a S-CSCF, it shall compare whether the S-CSCF name (i.e. SIP URI) has been changed. The comparison of the S-CSCF name is made according to the SIP URI comparison rules, which are defined in the IETF RFC 3261 (see chapter 6 in TS 29.228). If the HSS detects that the S-CSCF name has changed, it may send an RTR message to the old S-CSCF to remove the user data there. However, according to the SIP URI comparison rules the two URIs are considered to be different if, for example, the port is different or some uri parameter has different value. That will cause the HSS to send an unwanted RTR message to the current S-CSCF.
Summary of change:	⌘	The HSS shall check if the user's Diameter client address is changed or not before sending an RTR to remove the user data from the old S-CSCF.
Consequences if not approved:	⌘	Undesired de-registrations will occur causing negative end user experience.

Clauses affected:	⌘	8.1.1			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	Rel-6 mirror CR in N4-050148.

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.

8 Error handling procedures

8.1 Registration error cases

This section describes the handling of error cases, which can occur during the registration process. If the new and previously assigned S-CSCF names sent in the Multimedia-Auth-Request command are different, and the Multimedia-Auth-Request is not indicating synchronisation failure (i.e.the request does not contain auts parameter) then the HSS shall overwrite the S-CSCF name.

If the new and previously assigned S-CSCF names sent in a command other than the Multimedia-Auth-Request command are different, then the HSS shall not overwrite the S-CSCF name; instead it shall send a response to the S-CSCF indicating an error.

8.1.1 Cancellation of the old S-CSCF

It is possible that in certain situations the HSS receives a Multimedia-Auth-Request (MAR) command including a S-CSCF name, which is not the same as the previously assigned S-CSCF for the user. This can happen e.g. in case the new S-CSCF is selected due to a failure in the re-registration if the previously assigned S-CSCF does not respond to REGISTER message sent from the I-CSCF after a timeout.

In this case the new S-CSCF is assigned for the user and if registrations in the previously assigned S-CSCF exist for the user, these registrations in the old S-CSCF are handled locally in the old S-CSCF, e.g. re-registration timers in the old S-CSCF shall cancel the registrations. Alternatively, the HSS may de-register the registrations in the old S-CSCF by using the Registration-Termination-Request command. In this case the HSS shall first check whether the deregistration is really required by comparing the Diameter client address of the newly assigned S-CSCF received in the MAR command to the Diameter client address stored in the HSS. If the Diameter client addresses match, the deregistration shall not be initiated. Otherwise the deregistration may be initiated and it ~~de-registration~~ must be done in the following order:

1. Deregistration-Reason AVP value set to NEW_SERVER_ASSIGNED, for the public identity, which is registered in the new S-CSCF.
2. Deregistration-Reason AVP value set to SERVER_CHANGE, for the user public identities, which are not registered in the new S-CSCF.

8.1.2 Error in S-CSCF name

If the S-CSCF name sent in the Server-Assignment-Request command and the previously assigned S-CSCF name stored in the HSS are different, then, the HSS shall not overwrite the S-CSCF name; instead it shall send a response to the S-CSCF with Experimental-Result-Code value set to DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

8.1.3 Error in S-CSCF assignment type

If the Server-Assignment-Type in the Server-Assignment-Request command sent by the S-CSCF to the HSS is not allowed, e.g. Server-Assignment-Type set to UNREGISTERED_USER for a user already registered, the HSS shall send a response to the S-CSCF with the Experimental-Result-Code value set to DIAMETER_ERROR_IN_ASSIGNMENT_TYPE.

3GPP TSG-CN WG4 Meeting #26 **N4-050148**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.228** **CR** **166** ⌘**rev** **-** ⌘ Current version: **6.5.0** ⌘

*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:	⌘	Avoiding undesired deregistration		
Source:	⌘	CN4		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	04/02/2005
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:	⌘	This is an essential correction. When the HSS receives a MAR command for a user from a S-CSCF, it shall compare whether the S-CSCF name (i.e. SIP URI) has been changed. The comparison of the S-CSCF name is made according to the SIP URI comparison rules, which are defined in the IETF RFC 3261 (see chapter 6 in TS 29.228). If the HSS detects that the S-CSCF name has changed, it may send an RTR message to the old S-CSCF to remove the user data there. However, according to the SIP URI comparison rules the two URIs are considered to be different if, for example, the port is different or some uri parameter has different value. That will cause the HSS to send an unwanted RTR message to the current S-CSCF.
Summary of change:	⌘	The HSS shall check if the user's Diameter client address is changed or not before sending an RTR to remove the user data from the old S-CSCF.
Consequences if not approved:	⌘	Undesired de-registrations will occur causing negative end user experience.

Clauses affected:	⌘	8.1.1				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	Rel-5 CR in N4-050147.

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.

8 Error handling procedures

8.1 Registration error cases

This section describes the handling of error cases, which can occur during the registration process. If the new and previously assigned S-CSCF names sent in the Multimedia-Auth-Request command are different and the Multimedia-Auth-Request is not indicating synchronisation failure (i.e.the request does not contain auts parameter), then the HSS shall overwrite the S-CSCF name.

If the new and previously assigned S-CSCF names sent in a command other than the Multimedia-Auth-Request command are different, then the HSS shall not overwrite the S-CSCF name; instead it shall send a response to the S-CSCF indicating an error.

8.1.1 Cancellation of the old S-CSCF

It is possible that in certain situations the HSS receives a Multimedia-Auth-Request (MAR) command including a S-CSCF name, which is not the same as the previously assigned S-CSCF for the user. This can happen e.g. in case the new S-CSCF is selected due to a failure in the re-registration if the previously assigned S-CSCF does not respond to REGISTER message sent from the I-CSCF after a timeout.

In this case the new S-CSCF is assigned for the user and if registrations in the previously assigned S-CSCF exist for the user, these registrations in the old S-CSCF are handled locally in the old S-CSCF, e.g. re-registration timers in the old S-CSCF shall cancel the registrations. Alternatively, the HSS may de-register the registrations in the old S-CSCF by using the Registration-Termination-Request command. In this case the HSS shall first check whether the deregistration is really required by comparing the Diameter client address of the newly assigned S-CSCF received in the MAR command to the Diameter client address stored in the HSS. If the Diameter client addresses match, the deregistration shall not be initiated. Otherwise the deregistration may be initiated and it ~~de-registration~~ must be done in the following order:

1. Deregistration-Reason AVP value set to NEW_SERVER_ASSIGNED, for the public identity, which is registered in the new S-CSCF.

2. Deregistration-Reason AVP value set to SERVER_CHANGE, for the user public identities, which are not registered in the new S-CSCF.

8.1.2 Error in S-CSCF name

If the S-CSCF name sent in the Server-Assignment-Request command and the previously assigned S-CSCF name stored in the HSS are different, then, the HSS shall not overwrite the S-CSCF name; instead it shall send a response to the S-CSCF with Experimental-Result-Code value set to DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

8.1.3 Error in S-CSCF assignment type

If the Server-Assignment-Type in the Server-Assignment-Request command sent by the S-CSCF to the HSS is not allowed, e.g. Server-Assignment-Type set to UNREGISTERED_USER for a user already registered, the HSS shall send a response to the S-CSCF with the Experimental-Result-Code value set to DIAMETER_ERROR_IN_ASSIGNMENT_TYPE.

3GhPP TSG-CN WG4 Meeting #26 **N4-050331**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.228 CR 177** ⌘**rev** **-** ⌘ Current version: **5.10.0** ⌘

*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:	⌘	HSS initiated deregistration using the network initiated de-registration procedure
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	15/02/2005
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:	⌘	Too early implementation of CR 141
Summary of change:	⌘	The change introduced by CR 141, conditionnaly approved in CN4#25, are removed, coming back to the exact previous version of the TS.
Consequences if not approved:	⌘	The specification doesn't define any longer the S-CSCF behavior for Network initiated de-registration by HSS procedure, this is a backward regression.

Clauses affected:	⌘	6.1.3

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 ***

6.1.3 Network initiated de-registration by the HSS, administrative

In case of network initiated de-registration of the user initiated by the HSS, the HSS shall de-register the user and send a notification to the S-CSCF indicating the identities that shall be de-registered. The procedure is invoked by the HSS, corresponds to the functional level operation Cx-Deregister (see 3GPP TS 23.228 [1]).

HSS may decide to de-register:

- Only one public identity or a list of public identities
- All the public identities of a user.

This procedure is mapped to the commands Registration-Termination-Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.1.3.1 and 6.1.3.2 describe the involved information elements.

Table 6.1.3.1 : Network Initiated Deregistration by HSS request

Information element name	**Mapping to Diameter AVP**	**Cat.**	**Description**
Public User Identity (See 7.2)	Public-Identity	O	It contains the list of public user identities that are de-registered, in the form of SIP URL or TEL URL.
Private User Identity (See 7.3)	User-Name	M	It contains the private user identity in the form of a NAI.
Reason for de-registration (See 7.11)	Deregistration -Reason	M	The HSS shall send to the S-CSCF a reason for the de-registration. The de-registration reason is composed of two parts: one textual message (if available) that is intended to be forwarded to the user that is de-registered, and one reason code (see 3GPP TS 29.229 [5]) that determines the behaviour of the S-CSCF.
Routing Information (See 7.13)	Destination-Host	M	It contains the name of the S-CSCF which originated the last update of the name of the multimedia server stored in the HSS for a given multimedia user. The address of the S-CSCF is the same as the Origin-Host AVP in the message sent from the S-CSCF.

Table 6.1.3.2 : Network Initiated Deregistration by HSS response

Information element name	**Mapping to Diameter AVP**	**Cat.**	**Description**
Result (See 7.6)	Result-Code / Experimental-Result	M	This information element indicates the result of de-registration. 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.

6.1.3.1 Detailed behaviour

The HSS shall de-register the affected identities and invoke this procedure to inform the S-CSCF. The HSS can determine in different cases that the user (only one public identity, one or more public identities or all the public identities registered) has to be de-registered.

The HSS may de-register:

- Only one public identity or a list of public identities. In this case the S-CSCF shall remove all the information stored in the S-CSCF for those public identities.

- The user with all his/her public identities (no public identity sent in the Cx-Deregister request). In this case the S-CSCF shall remove all the information stored for that user.

The HSS shall send in the Deregistration-Reason AVP the reason for the de-registration, composed by a textual message (if available) aimed for the user and a reason code that determines the action the S-CSCF has to perform. The possible reason codes are:

- ~~PERMANENT_TERMINATION: the HSS indicates to the S-CSCF that the S-CSCF will no longer be assigned to the Public User Identity and associated implicitly registered Public User Identities for a given user (e.g. due IMS subscription cancellation). In this case, the S-CSCF initiates the de-registration of the user's Public User Identities.~~

- ~~NEW_SERVER_ASSIGNED: The HSS indicates to the S-CSCF that a new S-CSCF has been allocated to the user e.g. because the previous assigned S-CSCF was unavailable during a registration procedure. In this case, the S-CSCF initiates the de-registration of the Public User Identity and the associated implicitly registered Public User Identities for that user..~~

- ~~SERVER_CHANGE: The HSS indicates to the S-CSCF that the de-registration is requested to force the selection of new S-CSCF to assign to the user (e.g. when the user's S-CSCF capabilities are changed in the HSS or when the S-CSCF indicates that it has not enough memory for the updated User Profile). In this case, the S-CSCF initiates the de-registration of the registered Public User Identity and the associated implicitly registered Public User Identities.~~

- ~~REMOVE_S-CSCF: The HSS indicates to the S-CSCF that the S-CSCF will no longer be assigned to a user with the Public User Identity (and the associated Public User Identities) in the registration state set to unregistered. .In this case, the S-CSCF initiates the de-registration of the Public User Identity and the associated Public User Identities in the unregistered state..~~

~~The detailed de-registration procedures performed by the S-CSCF for each reason code are described in the 3GPP TS 24.229 [8].~~

- PERMANENT_TERMINATION: The IMS subscription or service profile(s) has been permanently terminated. The S-CSCF should start the network initiated de-registration towards the user.

- NEW_SERVER_ASSIGNED: new S-CSCF has been allocated to the user due to some reason, e.g. an error case, where the SIP registration is terminated in a new S-CSCF. The S-CSCF shall not start the network initiated de-registration towards the user but only clears its registration state and information regarding the user, i.e. all service profiles are cleared.

- SERVER_CHANGE: A new S-CSCF shall be allocated to the user when the user's S-CSCF capabilities are changed in the HSS or when the S-CSCF indicates that it has not enough memory for the updated User Profile. The S-CSCF should start the network initiated de-registration towards the user, i.e. all registrations are de-registered and the user is asked to re-register to all existing registrations.

- REMOVE_S-CSCF: The HSS indicates to the S-CSCF that the S-CSCF should no longer be used for a given user. The S-CSCF shall not start the network initiated de-registration towards the user when the user is not currently registered but clears all information regarding the user and responds to the HSS. The HSS then removes the S-CSCF for that user.

*** END OF MODIFICATION ***

3GPP TSG-CN WG4 Meeting #26 **N4-050334**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.228**	**CR**	**167**	⌘**rev**	**1**	⌘	Current version:	**5.10.0** ⌘

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 authentication procedures in not registered case			
Source:	⌘	CN4			
Work item code:	⌘	IMS-CCR	***Date:***	⌘	17/02/2005
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.** The detailed behaviour of authentication procedures doesn’t take into account that even though the registration status of the public identity received in the request is not registered, the user may have another public identity(ies) that belongs to another implicitly registered id set and has registration status registered and in that case the S-CSCF name is already stored in the HSS. As a reminder, comparison of S-CSCF addresses in HSS is already done for the cases when the public-id is registered or unregistered. It is not a new procedure. This CR only adds the comparison for the not registered case. The reason for the comparison is the same as for the other cases: it is possible that the I-CSCF has allocated a new S-CSCF for the user. This can happen when for example the connection between I-CSCF and the old S-CSCF is broken.
Summary of change:	⌘	When the HSS has received MAR command, the S-CSCF name received in the request must be compared to the S-CSCF name stored in the HSS also when the registration status of the public identity received in the request is not registered.
Consequences if not approved:	⌘	The received S-CSCF name is not compared to the S-CSCF name possibly stored earlier.

Clauses affected:	⌘	6.3.1
		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 request.

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.
    - ~~If it is not registered, 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.~~

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.

3GPP TSG-CN WG4 Meeting #26 **N4-050335**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.228**	**CR**	**168**	⌘**rev**	**1**	⌘	Current version:	**6.5.0**	⌘

*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 authentication procedures in not registered case		
Source:	⌘	CN4		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	17/02/2005
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:	⌘	The detailed behaviour of authentication procedures doesn't take into account that even though the registration status of the public identity received in the request is not registered, the user may have another public identity(ies) that belongs to another implicitly registered id set and has registration status registered and in that case the S-CSCF name is already stored in the HSS. As a reminder, comparison of S-CSCF addresses in HSS is already done for the cases when the public-id is registered or unregistered. It is not a new procedure. This CR only adds the comparison for the not registered case. The reason for the comparison is the same as for the other cases: it is possible that the I-CSCF has allocated a new S-CSCF for the user. This can happen when for example the connection between I-CSCF and the old S-CSCF is broken.
Summary of change:	⌘	When the HSS has received MAR command, the S-CSCF name received in the request must be compared to the S-CSCF name stored in the HSS also when the registration status of the public identity received in the request is not registered.
Consequences if not approved:	⌘	The received S-CSCF name is not compared to the S-CSCF name possibly stored earlier.

Clauses affected:	⌘	6.3.1				
		Y	N			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		

	□ ☒	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.

6.3.1 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.

    - ~~If it is not registered, 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 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.

3GPP TSG-CN WG4 Meeting #26 **N4-050336**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.229**	**CR**	**81**	⌘ **rev**	**1**	⌘	Current version:	**5.9.0**	⌘

*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:	⌘	Introduction of Failed-AVP		
Source:	⌘	CN4		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	31/01/2005
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. 29.228 Release 5 CR160 and Release 6 CR159 introduced the handling of data elements marked Mandatory, Conditional and Optional. Correct handling was defined when one of the information elements is missing. Handling for missing Information Elements which are tagged as Mandatroy or Conditional state that the missing AVP shall be returned in the Failed-AVP AVP. However, the Failed-AVP AVP is not defined in the ABNF.
Summary of change:	⌘	Modify the ABNF to include the Failed-AVP AVP in the UAA, SAA, LIA, MAA, RTA, PPA messages.
Consequences if not approved:	⌘	Inconsistencies between specifications and the Diameter Base Protocol RFC3588. Reference is made to an undefined AVP. Unclear behaviour for the handling of missing Information Elements that have been tagged as Mandatory or Conditional.

Clauses affected:	⌘	6.1.2, 6.1.4, 6.1.6, 6.1.8, 6.1.10, 6.1.12				
		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 Modification ***

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 }
                                        [ Server-Name ]
                                        [ Server-Capabilities ]
                                        *[ AVP ]
                                        *[ Failed-AVP ]
                                        *[ Proxy-Info ]
                                        *[ Route-Record ]
```

*** Second Modification ***

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 ]
                                    [ User-Data ]
                                    [ Charging-Information ]
                                    *[ AVP ]
                                    *[ Failed-AVP ]
                                    *[ Proxy-Info ]
                                    *[ Route-Record ]
```

*** Third Modification ***

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 }
[Server-Name]
[Server-Capabilities]
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

*** Fourth Modification ***

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]
[Public-Identity]
[SIP-Number-Auth-Items]
*** [SIP-Auth-Data-Item]**
* [AVP]
*[Failed-AVP]
* [Proxy-Info]
* [Route-Record]

*** Fifth Modification ***

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 }
                                     *[ AVP ]
                                     *[ Failed-AVP ]
                                     *[ Proxy-Info ]
                                     *[ Route-Record ]
```

*** Sixth Modification ***

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 }
                                     *[ AVP ]
                                     *[ Failed-AVP ]
                                     *[ Proxy-Info ]
                                     *[ Route-Record ]
```

3GPP TSG-CN WG4 Meeting #26 **N4-050337**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.229 CR 82** ⌘**rev** **1** ⌘ Current version: **6.3.0** ⌘

*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:	⌘	Introduction of Failed AVP			
Source:	⌘	CN4			
Work item code:	⌘	IMS-CCR	***Date:***	⌘	31/01/2005
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:	⌘	29.228 Release 5 CR160 and Release 6 CR159 introduced the handling of data elements marked Mandatory, Conditional and Optional. Correct handling was defined when one of the information elements is missing. Handling for missing Information Elements which are tagged as Mandatroy or Conditional state that the missing AVP shall be returned in the Failed-AVP AVP. However, the Failed-AVP AVP is not defined in the ABNF.
Summary of change:	⌘	Modify the ABNF to include the Failed-AVP AVP in the UAA, SAA, LIA, MAA, RTA, PPA messages.
Consequences if not approved:	⌘	Inconsistencies between specifications and the Diameter Base Protocol RFC3588. Reference is made to an undefined AVP. Unclear behaviour for the handling of missing Information Elements that have been tagged as Mandatory or Conditional.

Clauses affected:	⌘	6.1.2, 6.1.4, 6.1.6, 6.1.8, 6.1.10, 6.1.12				
		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 Modification ***

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 ]
```

*** Second Modification ***

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 ]
```

*** Third Modification ***

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]

*** Fourth Modification ***

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]

*** Fifth Modification ***

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 ]
```

*** Sixth Modification ***

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 ]
```

3GPP TSG-CN WG4 Meeting #26 **N4-050456**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.229 CR 077** ⌘ **rev 2** ⌘ Current version: **5.9.0** ⌘

*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 authentication-related AVPs
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	02/02/2005
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: ⌘ The current text in section 6.3.11 requires the SIP-Authorisation AVP to contain the data portion of the Authorization SIP headers suitable for inclusion in a SIP request. This wording could be interpreted as a request to include the Authorisation Request Header parameters as defined in IETF RFCs 3310 and 2617 in this AVP. However, this is not in line with 29.228, which requires the SIP-Authorisation AVP to contain the binary representation of either XRES or the concatenation of 'nonce' and 'auts'.

Similarly, section 6.3.10 could be misinterpreted, i.e. that it requires the SIP-Authenticate AVP to contain the parameters of the WWW-Authenticate header as defined in IETF RFCs 3310 and 2716.

It is proposed to align the text in sections 6.3.10 and 6.3.11 with 29.228.

This is an essential correction

Summary of change: ⌘ Content and encoding of SIP-Authenticate AVP and SIP-Authorisation AVP are detailed in sections 6.3.10 and 6.3.11.

Consequences if not approved: ⌘ Misalignment between 29.228 and 29.229 may result in incompatible parameter encoding in HSS and S-CSCF of different manufacturers. The consequence of this is a frequent failure of the IMS AKA and thus results in a frequent refusal of subscribers' access to IMS services.

Clauses affected: ⌘ 6.3.10, 6.3.11

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.

1st modified section

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].~~.~~

2nd modified section

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].~~.~~

End of modification

3GPP TSG-CN WG4 Meeting #26 **N4-050457**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.229**	**CR**	**078**	⌘**rev**	**2**	⌘	Current version:	**6.3.0** ⌘

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 authentication-related AVPs			
Source:	⌘	CN4			
Work item code:	⌘	IMS-CCR	***Date:***	⌘	02/02/2005
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:	⌘	The current text in section 6.3.11 requires the SIP-Authorisation AVP to contain the data portion of the Authorization SIP headers suitable for inclusion in a SIP request. This wording could be interpreted as a request to include the Authorisation Request Header parameters as defined in IETF RFCs 3310 and 2617 in this AVP. However, this is not in line with 29.228, which requires the SIP-Authorisation AVP to contain the binary representation of either XRES or the concatenation of 'nonce' and 'auts'. Similarly, section 6.3.10 could be misinterpreted, i.e. that it requires the SIP-Authenticate AVP to contain the parameters of the WWW-Authenticate header as defined in IETF RFCs 3310 and 2716. It is proposed to align the text in sections 6.3.10 and 6.3.11 with 29.228. **This is an essential correction**
Summary of change:	⌘	Content and encoding of SIP-Authenticate AVP and SIP-Authorisation AVP are detailed in sections 6.3.10 and 6.3.11.
Consequences if not approved:	⌘	Misalignment between 29.228 and 29.229 may result in incompatible parameter encoding in HSS and S-CSCF of different manufacturers. The consequence of this is a frequent failure of the IMS AKA and thus results in a frequent refusal of subscribers' access to IMS services.

Clauses affected:	⌘	6.3.10, 6.3.11
		Y **N**

Other specs	⌘		X	Other core specifications	⌘	
Affected:			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.

1st modified section

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].~~.~~

2nd modified section

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].

End of modification