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

<div align="right">

CP-050087

</div>

Source:	TSG CT WG4				
Title:	Corrections on IP-based multimedia services on Sh-interface				
Agenda item:	9.1				
Document for:	APPROVAL				

Doc-2nd-Level	Spec	CR #	Rev	Rel	Tdoc Title	CAT	C_Version
C4-050853	29.328	130	1	Rel-6	Sh procedures applicable to Public Service Identity	F	6.5.0
C4-050809	29.328	137	1	Rel-6	Editorial corrections	D	6.5.0
C4-050673	29.329	070		Rel-6	Correction of references	F	6.4.0
C4-050803	29.329	071	1	Rel-6	Corrections to message parameters	F	6.4.0
C4-050806	29.329	072	1	Rel-6	Miscellaneous Corrections	F	6.4.0

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

C4-050673

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **29.329** CR **070** | ⌘**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 **X**

Title: ⌘	Correction of references	
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 29.328 "IP Multimedia (IM) Subsystem Sh 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 2960 "Stream Control Transmission Protocol"

[4]   IETF RFC 3588 "Diameter Base Protocol"

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

[6]   3GPP TS 29.229 "Cx and Dx Interfaces based on the Diameter protocol; protocol details (Release 5) "

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

[8]   ITU-T Recommendation E.164: " The international public telecommunication numbering plan"

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.329** CR **071**	⌘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 **X**

Title: ⌘	Corrections to message parameters	
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: ⌘	There is confusion about some of the parameters of messages.
Summary of change: ⌘	1. In PUA message, the server can now include list of supported features 2. AVPs in PUR and PNR messages that are defined in this TS are made **bold**. 3. Note 2 in Table 6.3.1 is removed.
Consequences if not approved: ⌘	1. It would not be possible to introduce features on PUA message. 2. Confusion about the possible differences between non-bold AVPs and bold AVPs in message definition 3. Applicability of Note 2 is not clear

Clauses affected: ⌘	6.1.3, 6.1.4, 6.1.7, 6.3

	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 Diameter application for Sh interface

6.1 Command-Code values

[...]

6.1.3 Profile-Update-Request (PUR) Command

The Profile-Update-Request (PUR) command, indicated by the Command-Code field set to 307 and the 'R' bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to update user data in the server.

Message Format

```
< Profile-Update-Request > ::=    < Diameter Header: 307, REQ, PXY, 16777217 >
                                  < Session-Id >
                                  { Vendor-Specific-Application-Id }
                                  { Auth-Session-State }
                                  { Origin-Host }
                                  { Origin-Realm }
                                  { Destination-Host }
                                  { Destination-Realm }
                                  *[ Supported-Features ]
                                  { User-Identity }
                                  { Data-Reference }
                                  { User-Data }
                                  *[ AVP ]
                                  *[ Proxy-Info ]
                                  *[ Route-Record ]
```

6.1.4 Profile-Update-Answer (PUA) Command

The Profile-Update-Answer (PUA) command, indicated by the Command-Code field set to 307 and the 'R' bit cleared in the Command Flags field, is sent by a client in response to the Profile-Update-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 3GPP TS 29.229 [6].

Message Format

```
< Profile-Update-Answer > ::=< Diameter Header: 307, PXY, 16777217 >
                                  < 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 ]
```

[...]

6.1.7 Push-Notification-Request (PNR) Command

The Push-Notification-Request (PNR) command, indicated by the Command-Code field set to 309 and the 'R' bit set in the Command Flags field, is sent by a Diameter server to a Diameter client in order to notify changes in the user data in the server.

Message Format

```
< Push-Notification-Request > ::=        < Diameter Header:  309, REQ, PXY, 16777217 >
                                 < Session-Id >
                                 { Vendor-Specific-Application-Id }
                                 { Auth-Session-State }
                                 { Origin-Host }
                                 { Origin-Realm }
                                 { Destination-Host }
                                 { Destination-Realm }
                                 *[ Supported-Features ]
                                 { User-Identity }
                                 { User-Data }
                                 *[ AVP ]
                                 *[ Proxy-Info ]
                                 *[ Route-Record ]
```

[...]

6.3 AVPs

The following table describes the Diameter AVPs defined for the Sh interface protocol, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted.

Table 6.3.1: Diameter Multimedia Application AVPs

Attribute Name	AVP Code	Section defined	Value Type	AVP Flag rules				
				Must	May	Should not	Must not	May Encr.
User-Identity	700	6.3.1	Grouped	M, V				N
MSISDN	701	6.3.2	OctetString	M, V				N
User-Data	702	6.3.3	OctetString	M, V				N
Data-Reference	703	6.3.4	Enumerated	M, V				
Service-Indication	704	6.3.5	OctetString	M, V				N
Subs-Req-Type	705	6.3.6	Enumerated	M, V				N
Requested-Domain	706	6.3.7	Enumerated	M, V				N
Current-Location	707	6.3.8	Enumerated	M, V				N
Identity-Set	708	6.3.10	Enumerated	V			M	N
Server-Name	602	6.3.9	UTF8String	M, V				N
Supported-Features	628	6.3.11	Grouped	V	M			No

Feature-List-ID	629	6.3.12	Unsigned32	V			M	No
Feature-List	630	6.3.13	Unsigned32	V			M	No
Supported-Applications	631	6.3.14	Grouped	V			M	No
Public-Identity	601	6.3.15	UTF8String	M, V				N
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 3GPP TS 29.229 [6].								
NOTE 2: Depending on the concrete command.								

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.329** CR **072**	⌘**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 **X**

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 text duplicated elsewhere, removing of sentences not relevant, clarifying text to match the intent.

Summary of change: ⌘	See the details below.

Consequences if not approved: ⌘	Specification could be misinterpreted, resulting in incompatible implementations resulting in interoperability problems.

Clauses affected:	⌘	6.1, 6.1.2, 6.1.4, 6.1.6, 6.1.8, 6.2.1, 6.3, 6.3.3, 6.3.10, 7.1

		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

6 Diameter application for Sh interface

[...]

6.1 Command-Code values

This section defines Command-Code values for this Diameter application.

Every command is defined by means of the ABNF syntax (as defined in RFC 2234 [5]), according to the rules in IETF RFC 3588 [4]. Whenever the definition and use of an AVP is not specified in this document, what is stated in ~~IETF RFC 3588 [4] or~~ 3GPP TS 29.229 [6] shall apply.

The command codes for the Sh interface application are taken from the range allocated by IANA in IETF RFC 3589 [7] as assigned in this specification. For these commands, the Application-ID field shall be set to 16777217 (application identifier of the Sh interface application, allocated by IANA).

The following Command Codes are defined in this specification:

Table 6.1.1: Command-Code values

Command-Name	Abbreviation	Code	Section
User-Data-Request	UDR	306	6.1.1
User-Data-Answer	UDA	306	6.1.2
Profile-Update-Request	PUR	307	6.1.3
Profile-Update-Answer	PUA	307	6.1.4
Subscribe-Notifications-Request	SNR	308	6.1.5
Subscribe-Notifications-Answer	SNA	308	6.1.6
Push-Notification-Request	PNR	309	6.1.7
Push-Notification-Answer	PNA	309	6.1.8

[...]

6.1.2 User-Data-Answer (UDA) Command

The User-Data-Answer (UDA) command, indicated by the Command-Code field set to 306 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the User-Data-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~~ or in 3GPP TS 29.229 [6].

Message Format

```
< User-Data-Answer > ::=        < Diameter Header: 306, PXY, 16777217 >
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                [ Result-Code ]
                                [ Experimental-Result ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
```

         *[Supported-Features]
          [User-Data]
         *[AVP]
         *[Failed-AVP]
         *[Proxy-Info]
         *[Route-Record]

[…]

6.1.4 Profile-Update-Answer (PUA) Command

The Profile-Update-Answer (PUA) command, indicated by the Command-Code field set to 307 and the 'R' bit cleared in the Command Flags field, is sent by a ~~client~~ server in response to the Profile-Update-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 or~~ in 3GPP TS 29.229 [6].

Message Format

    < Profile-Update-Answer > ::=< Diameter Header: 307, PXY, 16777217 >
         < Session-Id >
         { Vendor-Specific-Application-Id }
         [Result-Code]
         [Experimental-Result]
         { Auth-Session-State }
         { Origin-Host }
         { Origin-Realm }
         *[AVP]
         *[Failed-AVP]
         *[Proxy-Info]
         *[Route-Record]

[…]

6.1.6 Subscribe-Notifications-Answer (SNA) Command

The Subscribe-Notifications-Answer command, indicated by the Command-Code field set to 308 and the 'R' bit cleared in the Command Flags field, is sent by a ~~client~~ server in response to the Subscribe-Notifications-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 or~~ in 3GPP TS 29.229 [6].

Message Format

    < Subscribe-Notifications-Answer > ::= < Diameter Header: 308, PXY, 16777217 >
         < Session-Id >
         { Vendor-Specific-Application-Id }
         { Auth-Session-State }
         [Result-Code]
         [Experimental-Result]
         { Origin-Host }
         { Origin-Realm }
         *[Supported-Features]
         *[AVP]
         *[Failed-AVP]
         *[Proxy-Info]
         *[Route-Record]

[...]

6.1.8   Push-Notifications-Answer (PNA) Command

The Push-Notifications-Answer (PNA) command, indicated by the Command-Code field set to 309 and the 'R' bit cleared in the Command Flags field, is sent by a client in response to the Push-Notification-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 or in 3GPP TS 29.229 [6].

Message Format

> < Push-Notification-Answer > ::=< Diameter Header: 309, PXY, 16777217 >
>   < 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

[...]

6.2.1   Success

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

No result codes errors within this category have been defined so far.

[...]

6.3 AVPs

The following table describes the Diameter AVPs defined for the Sh interface protocol, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted.

Table 6.3.1: Diameter Multimedia Application AVPs

Attribute Name	AVP Code	Section defined	Value Type	Must	May	Should not	Must not	May Encrypt.
User-Identity	700	6.3.1	Grouped	M, V				No
MSISDN	701	6.3.2	OctetString	M, V				No
User-Data	702	6.3.3	OctetString	M, V				No

Data-Reference	703	6.3.4	Enumerated	M, V				
Service-Indication	704	6.3.5	OctetString	M, V				No
Subs-Req-Type	705	6.3.6	Enumerated	M, V				No
Requested-Domain	706	6.3.7	Enumerated	M, V				No
Current-Location	707	6.3.8	Enumerated	M, V				No
Identity-Set	708	6.3.10	Enumerated	V			M	No
Server-Name	602	6.3.9	UTF8String	M, V				No
Supported-Features	628	6.3.11	Grouped	V	M			No
Feature-List-ID	629	6.3.12	Unsigned32	V			M	No
Feature-List	630	6.3.13	Unsigned32	V			M	No
Supported-Applications	631	6.3.14	Grouped	V			M	No
Public-Identity	601	6.3.15	UTF8String	M, V				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 3GPP TS 29.229 [6].								
NOTE 2: Depending on the concrete command.								

[...]

6.3.3 User-Data AVP

The User-Data AVP is of type OctetString. This AVP contains the user data requested in the UDR and SNR operations and the data to be modified in the PURUPR operation . The exact content and format of this AVP is described in 3GPP TS 29.328 [1].

[...]

6.3.10 Identity-Set AVP

The Identity-Set AVP (AVP code 108) is of type Enumerated and indicates the requested set of IMS Public Identities. The Ffollowing values are defined:

    ALL_IDENTITIES (0)

    REGISTERED_IDENTITIES (1)

    IMPLICIT_IDENTITIES (2)

[...]

7 Special Requirements

7.1 Version Control

The version control mechanisms specified in 3GPP TS 29.229 [6] clauses 7.1, 7.2 and 7.3 apply to this specification.

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

Table 7.1.x: Features of feature list 1 used in Sh

Feature bit	Feature	M/O	Description
			[Editor's note: until now, no features has been defined for the Sh.]
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 following table shall apply to the Sh interface:, the column Application identifier lists the used application identifiers on Sh and 3GPP.

Table 7.1.y: Application identifiers used in Sh

Application identifier	First applied
16777217	3GPP Rel-5

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **29.328** CR **137** | ⌘**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 **X**

Title:	⌘	Editorial corrections
Source:	⌘	Qualcomm Incorporated
Work item code:	⌘	IMS2-CCR	**Date:** ⌘	14/4/2005

Category:	⌘	**D**		**Release:** ⌘	Rel-6

Use <u>one</u> 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 <u>one</u> 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:	⌘	Many inconsistencies, spelling errors, missing references, wrong references, incorrect section numbering
Summary of change:	⌘	See the details below
Consequences if not approved:	⌘	These mistakes would remain, leading to more time for comprehension of the specification

Clauses affected:	⌘	

		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

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

[2] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP (Release 5)".

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

[4] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model"

[5] 3GPP TS 29.329: "Sh Interface based on Diameter – Protocol details"

[6] 3GPP TS 29.228: "IP multimedia (IM) Subsystem Cx Interface; Signalling flows and Message Elements".

[7] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol ; Protocol details"

[8] IETF RFC 3588 "Diameter Base Protocol"

[9] ITU-T recommendation Q.763: "Signalling System No. 7 - ISDN User Part formats and codes"

[10] 3GPP TS 23.018: "Basic Call Handling; Technical realization"

[11] 3GPP TS 23.003: "Numbering, Addressing and Identification"

[12] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)"

[13] 3GPP TS 29.002: "Mobile Application Part (MAP) specification"

[14] 3GPP TS 23.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 3 - Stage 2"

[15] RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies"

[16] RFC 3261: "SIP: Session Initiation Protocol"

[17] RFC 2806: "URLs for Telephone Calls"

[18] 3GPP TS 23.141: "Presence Service; Architecture and Functional Description"

[19] TS 23.012: "Location Management Procedures"

[...]

5 General Architecture

This clausesection further specifies the architectural assumptions associated with the Sh reference point, building on 3GPP TS 23.228 [1], 3GPP TS 23.218 [4] and also the Ph reference point building upon 3GPP TS 23.141 [18].

[...]

6 Procedure Descriptions

6.1 User data handling procedures

6.1.1 Data read (Sh-Pull)

This procedure is used between the AS and the HSS. The procedure is invoked by the AS and is used:

- To read transparent and/or non-transparent data for a specified user from the HSS.

This procedure is mapped to the commands User-Data-Request/Answer in the Diameter application specified in 3GPP TS 29.329 [5]. Tables 6.1.1.1 and 6.1.1.2 detail the involved information elements.

Table 6.1.1.1: Sh-Pull

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1)	User-Identity	M	IMS Public User Identity or MSISDN of the user for whom the data is required. See section 7.1 for the content of this AVP.
Requested data (See 7.3)	Data-Reference	M	This information element indicates the reference to the requested information. The set of valid reference values are defined in 7.6.
Requested Identity set (See 7.11)	Identity-Set	O	If Data-Reference indicates that IMS Public Identities is the requested data set to be downloaded, this information element should be included. When this information element takes the value IMPLICIT_IDENTITIES, the HSS shall provide all non-barred IMS Public Identities that are belong to the same implicit registration set as the IMS Public Identity included in the message in the User-Identity AVP. The MSISDN user identity is not applicable for this value. When this information element takes the value REGISTERED_IDENTITIES, the HSS shall provide all non-barred IMS Public Identities whose state is registered, belonging to all Private Identities that the IMS Public Identity or MSISDN in the User-Identity AVP is associated with. When this information element takes the value ALL_IDENTITIES, the HSS shall provide all non-barred IMS Public Identities, belonging to all Private Identities that the IMS Public Identity or MSISDN in the User-Identity AVP is associated with. If Data-Reference indicates that IMS Public Identities is the requested data set to be downloaded and this information element is not included, the HSS shall download the set of IMS Public Identities that would be downloaded if the value of this information element had been ALL_IDENTITIES.
Requested domain (See 7.2)	Requested-Domain	C	This information element indicates the domains to which the operation is applicable. Check table 7.6.1 to see when it is applicable.
Current Location (See 7.8)	Current-Location	C	This information element indicates whether an active location retrieval has to be initiated or not. It shall be present if Location Information is requested. If this information element takes the value InitiateActiveLocationRetrieval (1) the HSS shall indicate to the MSC/VLR and/or SGSN the need to initiate an active location retrieval. Check table 7.6.1 to see when it is applicable.
Service Indication (See 7.4)	Service-Indication	C	IE that identifies, together with the IMS Public User Identity included in the User-Identity AVP and Data-Reference, the set of service related transparent data that is being requested. Check table 7.6.1 to see when it is applicable.
Application Server Identity (See 7.9)	Origin-Host	M	IE that identifies the AS originator of the request and that is used to check the AS permission list.
Application Server Name (See 7.10)	Server-Name	C	IE that is used, together with the IMS Public User Identity included in the User-Identity AVP and Data-Reference, as key to identify the filter criteria. Check table 7.6.1 to see when it is applicable.

Table 6.1.1.2: Sh-Pull Resp

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.5)	Result-Code / Experimental_ Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Sh 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.
Data (See 7.6)	User-Data	O	Requested data.

6.1.1.1   Detailed behaviour

The conditions for the inclusion of Requested-Domain as an additional key to the requested data are described in table 7.6.1. If repository data is requested, Service-Indication shall be present in the request. If initial filter criteria are requested, the Server-Name AVP shall contain the SIP URL of the AS that initiates the request; requests for initial filter criteria are limited to those initial filter criteria which are relevant to the requesting AS.

Upon reception of the Sh-Pull request, the HSS shall, in the following order:

1. In the AS permission list (see section 6.2) check that the requested user data is allowed to be read (Sh-Pull) by this AS by checking the combination of the identity of the AS sending the request (identified by the Origin-Host AVP) and the supplied Data-Reference.

   If the data referenced in the request is not allowed to be read, Experimental-Result ~~Code~~ shall be set to DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ in the Sh-Pull Response.

2. Check that the user for whom data is asked exists in HSS. If not, Experimental-Result ~~Code~~ shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Sh-Pull Response.

3. Check whether or not the data that is requested to be downloaded by the AS is currently being updated by another entity. If there is an update of the data in progress, the HSS may delay the Sh-Pull-Resp message until the update has been completed and shall include in the Sh-Pull-Resp message the updated data requested. The HSS shall ensure that the data returned is not corrupted by this conflict.

If there is an error in any of the above steps then the HSS shall stop processing and shall return the error code specified in the respective step (see 3GPP TS 29.329 [5] and 3GPP TS 29.229 [7] for an explanation of the error codes).

If the HSS cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY.

Otherwise, the requested operation shall take place and the HSS shall return the Result-Code AVP set to DIAMETER_SUCCESS and the requested data identified by User-Identity and Data-Reference in the Sh-Pull Response message.

6.1.2   Data Update (Sh-Update)

[...]

6.1.2.1   Detailed behaviour

Within the Sh-Update Request, the keys to determine the updated data are part of the information element Data (See 7.6). When data in the repository is updated (i.e. added, modified or removed) Service-Indication and Sequence-Number are also sent as part of the information element Data.

Newly added transparent data shall be associated with a Sequence Number of 0 in the Sh-Update Request. Sequence Number value 0 is reserved exclusively for indication of newly added transparent data.

Modified and removed transparent data shall be associated within the Sh-Update Request with a Sequence Number of n+1 where n is the original Sequence Number associated with the transparent data before modification or removal. If n equals 65535, then the next modification or deletion of that transparent data shall be associated with a Sequence Number of 1.

Upon reception of the Sh-Update request, the HSS shall, in the following order:

1. In the AS permission list (see section 6.2) check that the user data that is requested to be updated (Sh-Update) by this AS, is allowed to be updated by checking the combination of the identity of the AS sending the request (identified by the Origin-Host AVP) and the supplied Data-Reference.

    - If the data is not allowed to be updated, Experimental-Result Code shall be set to DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED in the Sh-Update Response.

2. Check that the user for whom the data is asked to be updated exists in the HSS. If not, Experimental-Result Code shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Sh-Update Response.

3. Check whether or not the data that is requested to be updated by the AS, as identified by the Service-Indication, is currently being updated by another entity. If there is an update of the data in progress, Experimental-Result Code shall be set to DIAMETER_PRIOR_UPDATE_IN_PROGRESS in the Sh-Update Response.

4. Check whether or not there is any repository data stored at the HSS already for the specified Service-Indication and the associated user.

    - If repository data identified by the Service-Indication is stored at the HSS for the specified user, check the following premises:

        1. Sequence_Number_in_Sh_Update is not equal to 0

        2. (Sequence_Number_in_Sh_Update - 1) is equal to (Sequence_Number_In_HSS modulo 65535)

    - If either of the above premises is false then Experimental-Result Code shall be set to DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC in the Sh-Update Response.

    - If both of the above premises are true, then check whether or not Service Data is received within the Sh-Update Req.

        - If Service Data is included in the Sh-Update Req, check whether or not the size of the data is greater than that which the HSS is prepared to accept.

            - If there is more data than the HSS is prepared to accept then Experimental-Result Code shall be set to DIAMETER_ERROR_TOO_MUCH_DATA and the new data shall be discarded.

            - If the HSS is prepared to accept the data, then the repository data stored at the HSS shall be updated with the repository data sent in the Sh-Update Req and the Sequence Number associated with that repository data shall be updated with that sent in the Sh-Update Req. This triggers the sending of Sh-Notif messages to any other ASs that are subscribed to Notifications for updates to the service data for that user (see 6.1.4).

        - If Service Data is not received, the data stored in the repository at the HSS shall be removed, and as a consequence the Service Indication and the Sequence Number associated with the removed data shall also be removed. This triggers the sending of Sh-Notif messages to any other ASs that are subscribed to Notifications for updates to the service data for that user (see 6.1.4). After sending Sh-Notif messages, the subscriptions to Notifications for the removed Repository Data shall be deleted.

    - If repository data identified by the Service-Indication is not stored for the user i.e. the Sh-Update Req intends to create a new repository data, check whether or not the Sequence Number in the Sh-Update Req is 0.

        - If the sequence number is not set to 0, Experimental-Result Code shall be set to DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC

        - If the sequence number is set to 0 check whether Service Data is included within the Sh-Update Req.

- If Service Data is not included in the Sh-Update Req, then Experimental-Result Code shall be set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED and the operation shall be ignored by the HSS.

- If Service Data is included in the Sh-Update Req, check whether or not the size of the data is greater than that which the HSS is prepared to accept. If there is more data than the HSS is prepared to accept then Experimental-Result Code shall be set to DIAMETER_ERROR_TOO_MUCH_DATA and the new data shall be discarded.

- If the HSS is prepared to accept the data included in the Sh-Update Req, then the data shall be stored in~~within~~ the data repository in the HSS.

If there is an error in any of the above steps then the HSS shall stop processing and shall return the error code specified in the respective step (see 3GPP TS 29.329 [5] and 3GPP TS 29.229 [7] for an explanation of the error codes).

If the HSS cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY.

Otherwise, the requested operation shall take place and the HSS shall return the Result-Code AVP set to DIAMETER_SUCCESS.

NOTE: When an AS receives DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC the AS may attempt to resolve the inconsitency between the version of the repository data that it holds and that stored at the HSS. It may execute a Sh-Pull to retrieve the current version of the data from the HSS or it ~~t~~may wait to receive a subsequent Sh-Notif message from the HSS for the affected repository data.

6.1.3   Subscription to notifications (Sh-Subs-Notif)

This procedure is used between the AS and the HSS. The procedure is invoked by the AS and is used:

- To subscribe to Notifications for when particular transparent and/or non-transparent data for a specified user is updated, from the HSS.

This procedure is mapped to the commands Subscribe-Notifications-Request/Answer in the Diameter application specified in 3GPP TS 29.329 [5]. Tables 6.1.3.1 and 6.1.3.2 detail the information elements involved.

Table 6.1.3.1: Sh-Subs-Notif

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1)	User-Identity	M	IMS public identity of the user for whom notifications of data changes are requested. See section 7.1 for the content of this AVP.
Requested data (See 7.3)	Data-Reference	M	This information element includes the reference to the data on which notifications of change are required (valid reference values are defined in 7.6).
Subscription request type (See 7.7)	Subs-Req-Type	M	This information element indicates the action requested on subscription to notifications.
Service Indication (See 7.4)	Service-Indication	C	IE that identifies, together with the IMS Public User Identity and Data-Reference, the set of service related transparent data for which notifications of changes are requested. This element shall be present when the Data-Reference value is RepositoryData (0).
Application Server Identity (See 7.9)	Origin-Host	M	IE that identifies the AS originator of the request and that is used to check the AS permission list.
Application Server Name (See 7.10)	Server-Name	C	IE that is used, together with the IMS Public user Identity and Data-Reference, as key to identify the filter criteria. This element shall be present when the Data-Reference value is InitialFilterCriteria (13).

Table 6.1.3.2: Sh-Subs-Notif Resp

Information element name	Mapping to Diameter AVP	Cat.	Description
~~Data request~~ ~~r~~Result (See 7.5)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Sh 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 take note of the subscription request on the data identified by IMS Public User Identity and Data-Reference. If notifications on changes of repository data are requested, Service-Indication shall be present in the request. If notifications on changes of filter criteria are requested, the Server-Name AVP shall be used as key to the filter criteria. The Server-Name AVP shall contain the SIP URL of the AS sending the request.

Upon reception of the Sh-Subs-Notif request, 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 29.329 [5] and 3GPP TS 29.229 [7]):

1. In the AS permission list (see section 6.2) the HSS shall check that the AS is allowed to subscribe to notifications (Sh-Subs-Notif) for the requested user data by checking the combination of the identity of the AS sending the request (identified by the Origin-Host AVP) and the supplied Data-Reference.

   - If this AS does not have Sh-Subs-Notif permission for the data referenced, Experimental-Result ~~Code~~ shall be set to DIAMETER_ERROR_USER_DATA_CANNOT_BE_NOTIFIED in the Sh-Subs-Notif Response.

2. Check that the user for whom notifications are asked exists in HSS. If not, Experimental-Result ~~Code~~ shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Sh-Subs-Notif Response.

If the HSS cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY.

6.1.4 Notifications (Sh-Notif)

This procedure is used between the HSS and the AS. The procedure is invoked by the HSS and is used:

- To inform the AS of changes in transparent and/or non-transparent data to which the AS has previously subscribed to receive Notifications for, using Sh-Subs-Notif (see 6.1.3).

This procedure is mapped to the commands Push-Notification-Request/Answer in the Diameter application specified in 3GPP TS 29.329 [5]. Tables 6.1.4.1 and 6.1.4.2 detail the involved information elements.

Table 6.1.4.1: Sh-Notif

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1)	User-Identity	M	IMS Public User Identity of the user which data has changed. See section 7.1 for the content of this AVP.
Requested Data (See 7.6)	User-Data	M	Changed data.

Table 6.1.4.2: Sh-Notif Resp

Information element name	Mapping to Diameter AVP	Cat.	Description
~~Data request~~ ~~r~~Result (See 7.5)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Sh 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.

[...]

~~6.5 User identity to HSS resolution~~

~~The User identity to HSS resolution mechanism enables the AS to find the address of the HSS that holds the subscriber data for a given public user identity when multiple and separately addressable HSSs have been deployed by the network operator. The resolution mechanism is not required in networks that utilise a single HSS or when an AS is configured to use pre-defined HSS.~~

~~The resolution mechanism described in 3GPP TS 23.228 [8] is based on the Subscription Locator Function (SLF). The AS accesses the subscription locator via the Dh interface. The Dh interface is always used in conjunction with the Sh interface. The Dh interface is based on Diameter. Its functionality is implemented by means of the routing mechanism provided by an enhanced Diameter redirect agent, which is able to extract the public user identity from the received requests.~~

~~To get the HSS address the AS sends to the SLF the Sh requests aimed for the HSS. On receipt of the HSS address from the SLF, the AS shall send the Sh requests to the HSS. The AS may store the HSS address and use it in further requests associated to the same public user identity.~~

~~In networks where the use of the user identity to HSS resolution mechanism is required and the AS is not configured to use predefined HSS, each AS shall be configured with the address/name of the SLF implementing this resolution mechanism.~~

6.2   AS permissions list

In table 7.6.1, the contents of the Data-AVP are described. Some of the individual elements carried within Data-AVP may be requested by the AS from the HSS using the Sh-Pull command (see section 6.1.1) or may be updated at the HSS by the AS using the Sh-Update command (see section 6.1.2). The AS may also request that the HSS notifies the AS of changes to specific elements within the Data-AVP using the Sh-Subs-Notif command (see section 6.1.3). The HSS will only allow these operations to take place if the element of the Data-AVP is permitted to be included in the specific command requested by the AS, as indicated in table 7.6.1.

To manage whether an AS may request each element of Data-AVP with a specific command, the HSS shall maintain a list of AS permissions (the 'AS Permissions List'). AS permissions are identified by AS identity and Data Reference with the possible permissions associated with each Data Reference being Sh-Pull, Sh-Update, Sh-Subs-Notif or any combination of these permissions (see table 7.6.1 for details of which permissions are allowed for each Data Reference). The permissions apply to all users served by the HSS, they are not user specific. When an AS requests Sh-Pull, Sh-Update or Sh-Subs-Notif the HSS shall check permissions and return an error result if the AS does not have the required permission.

6.3   Void

6.4   Void

6.5   User identity to HSS resolution

The User identity to HSS resolution mechanism enables the AS to find the address of the HSS that holds the subscriber data for a given public user identity when multiple and separately addressable HSSs have been deployed by the network operator. The resolution mechanism is not required in networks that utilise a single HSS or when an AS is configured to use pre-defined HSS.

The resolution mechanism described in 3GPP TS 23.228 [18] is based on the Subscription Locator Function (SLF). The AS accesses the subscription locator via the Dh interface. The Dh interface is always used in conjunction with the Sh interface. The Dh interface is based on Diameter. Its functionality is implemented by means of the routing mechanism provided by an enhanced Diameter redirect agent, which is able to extract the public user identity from the received requests.

To get the HSS address the AS sends to the SLF the Sh requests aimed for the HSS. On receipt of the HSS address from the SLF, the AS shall send the Sh requests to the HSS. The AS may store the HSS address and use it in further requests associated to the same public user identity.

In networks where the use of the user identity to HSS resolution mechanism is required and the AS is not configured to use predefined HSS, each AS shall be configured with the address/name of the SLF implementing this resolution mechanism.

7   Information element contents

[...]

7.3   Requested Data

- Reference to the data that an AS is requesting from the HSS.

- Reference to the data which, an AS wants to be notified of, when changed.

- Reference to data for which subscription to notification of change is rejected.

See chaptersection -7.6.

[...]

7.6 Data

[...]

7.6.6 Location Information

This information element contains the location of the served subscriber in the MSC/VLR if the requested domain is CS, or the location of the served subscriber in the SGSN if the requested domain is PS. If the HSS has to communicate with the MSC/VLR and/or SGSN to retrieve location information, it shall make use of the service MAP-PROVIDE-SUBSCRIBER-INFO.

For both Location Information for CS and Location Information for GPRS, the considerations described in 3GPP TS 23.078 [14] apply.

7.6.6.1 Location information for CS

This information element consists of the following subordinate information elements:

- Location number: defined in ITU-T Recommendation Q.763 [9]. Considerations described in 3GPP TS 23.018 apply[10].

- Service area ID: defined in 3GPP TS 23.003 [11].

- Global Cell ID: defined in 3GPP TS 23.003 [11].

- Location area ID: defined in 3GPP TS 23.003 [11].

- Geographical Information: defined in 3GPP TS 23.032 [12]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.

- Geodetic Information: defined in ITU-T Recommendation Q.763 [9]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.

- VLR Number: defined in 3GPP TS 23.003 [11].

- MSC Number: defined in 3GPP TS 23.003 [11].

- Age of location information: defined in 3GPP TS 23.018 [10].

- Current Location Retrieved: shall be present when location information was obtained after a successful paging procedure for Active Location Retrieval.
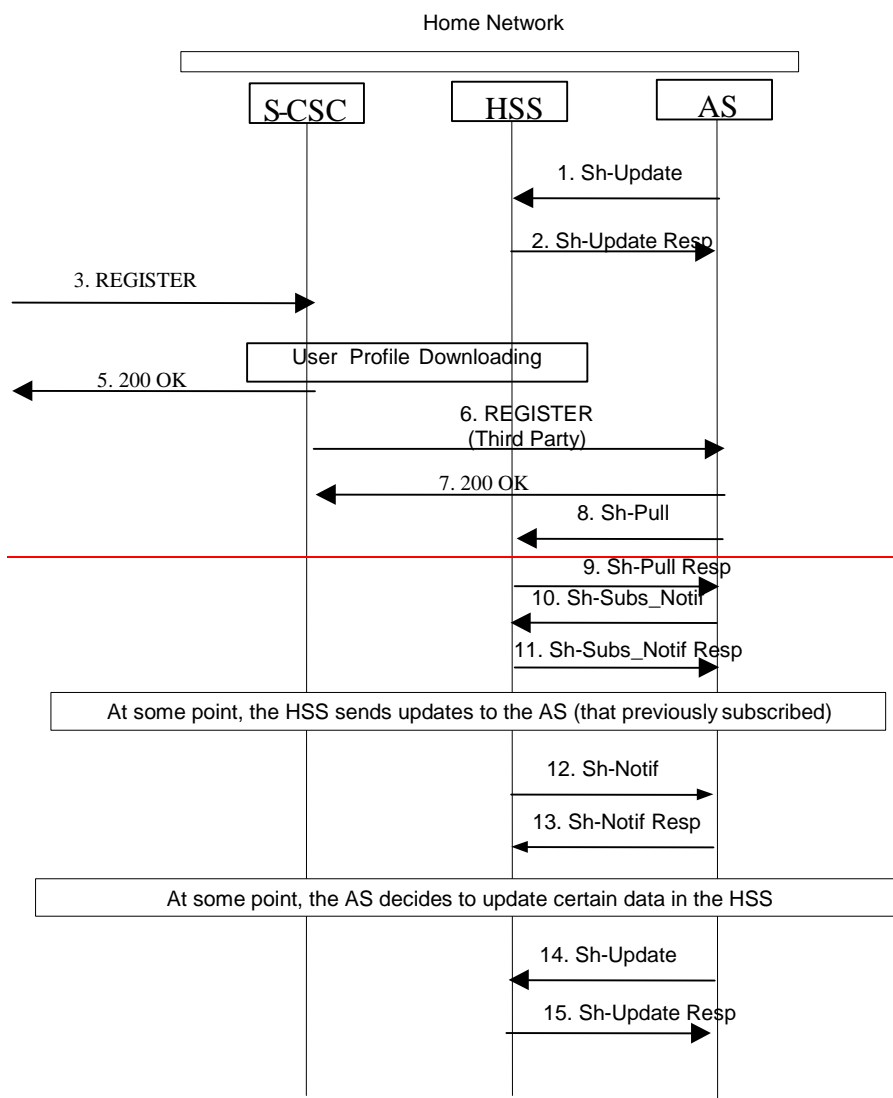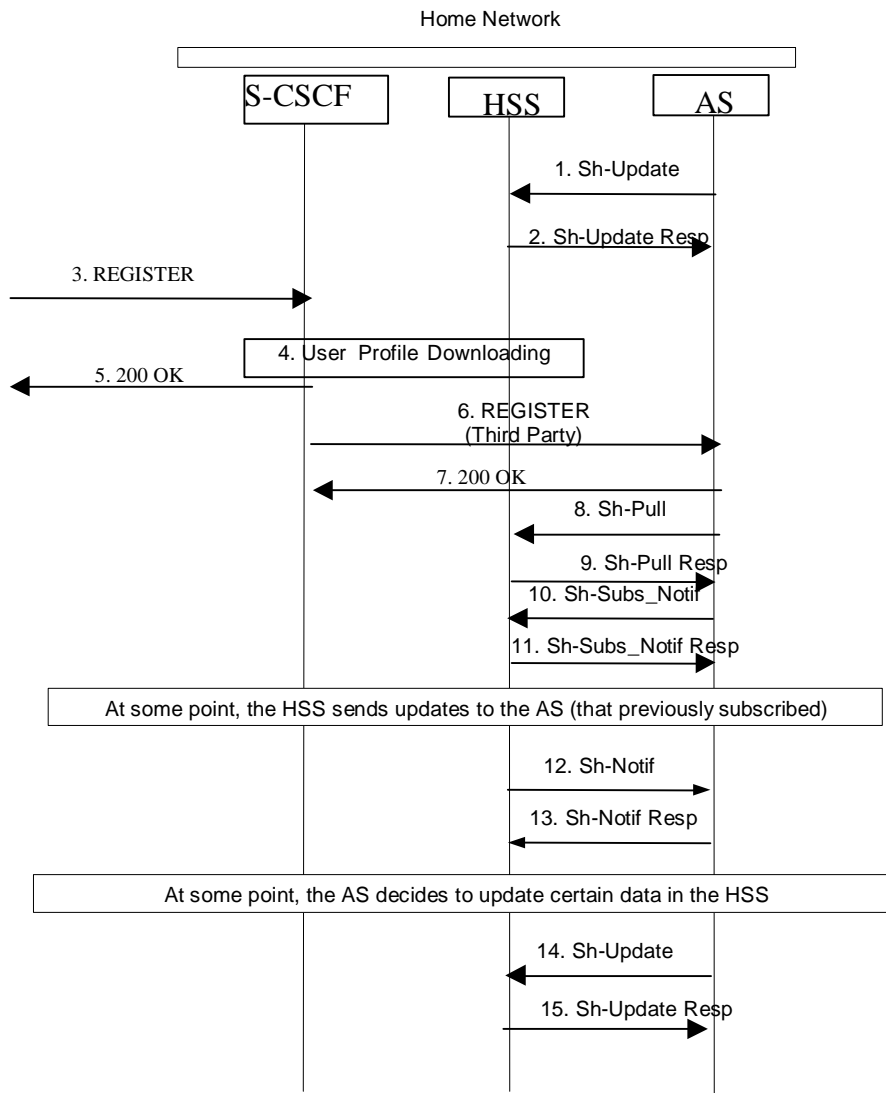
[...]

Annex B (informative): Message flow

B.1 Message flows

The following message flows give examples regarding which Diameter messages shall be sent in scenarios described in 3GPP TS 23.218 [4].

B.1.1 Data Update, Registration, Notification Subscription.

Home Network

S-CSC HSS AS

1. Sh-Update

2. Sh-Update Resp

3. REGISTER

User Profile Downloading

5. 200 OK

6. REGISTER
(Third Party)

7. 200 OK

8. Sh-Pull

9. Sh-Pull Resp

10. Sh-Subs_Notif

11. Sh-Subs_Notif Resp

At some point, the HSS sends updates to the AS (that previously subscribed)

12. Sh-Notif

13. Sh-Notif Resp

At some point, the AS decides to update certain data in the HSS

14. Sh-Update

15. Sh-Update Resp

Home Network

S-CSCF   HSS   AS

1. Sh-Update

2. Sh-Update Resp

3. REGISTER

4. User Profile Downloading

5. 200 OK

6. REGISTER
(Third Party)

7. 200 OK

8. Sh-Pull

9. Sh-Pull Resp

10. Sh-Subs_Notif

11. Sh-Subs_Notif Resp

At some point, the HSS sends updates to the AS (that previously subscribed)

12. Sh-Notif

13. Sh-Notif Resp

At some point, the AS decides to update certain data in the HSS

14. Sh-Update

15. Sh-Update Resp

Figure B.1.1: Data Update, Registration, Notification Subscription

1. A user subscribes to a new service. The operator provisions the service in an AS. The AS stores some service data for a user in the HSS, Sh-Update (user identity, updated data) e.g. repository data.

2. HSS confirms the data is updated

3. Some time later, user registers with the network

4. S-CSCF downloads the data from the HSS (during the procedure S-CSCF Registration Notification on Cx interface). Filter criteria specify that the AS wants to be notified that the end user is registered.

5. 200 OK

6. S-CSCF sends third party registration message to the application server to notify that user is registered.

7. 200 OK

8. The AS downloads data needed for providing service from HSS, by means of Sh-Pull (user identity, requested data, and service information).

9. HSS sends data to AS

10. The AS subscribes to notifications from the HSS of changes in data, by means of Sh-Subs-Notif (user identity, requested data, and/or service information).

11. The HSS confirms the subscription request.

12. At some moment, user data is updated in the HSS. As the AS subscribed to notifications (step 10), the HSS sends to the AS the requested updates, by means of Sh-Notif (user identity, updated data).

13. The AS acknowledges the notification.

14. At some moment, the AS decides to update user's service data e.g. repository data in the HSS, by means of Cx-Update (user identity, updated data).

15. The HSS confirms the service data is updated.

Annex C (informative): UML model of the data downloaded over Sh interface~~i/f~~

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

C.1 General description

The following picture gives an outline of the UML model of the user profile, which is exchanged between the HSS and an AS:
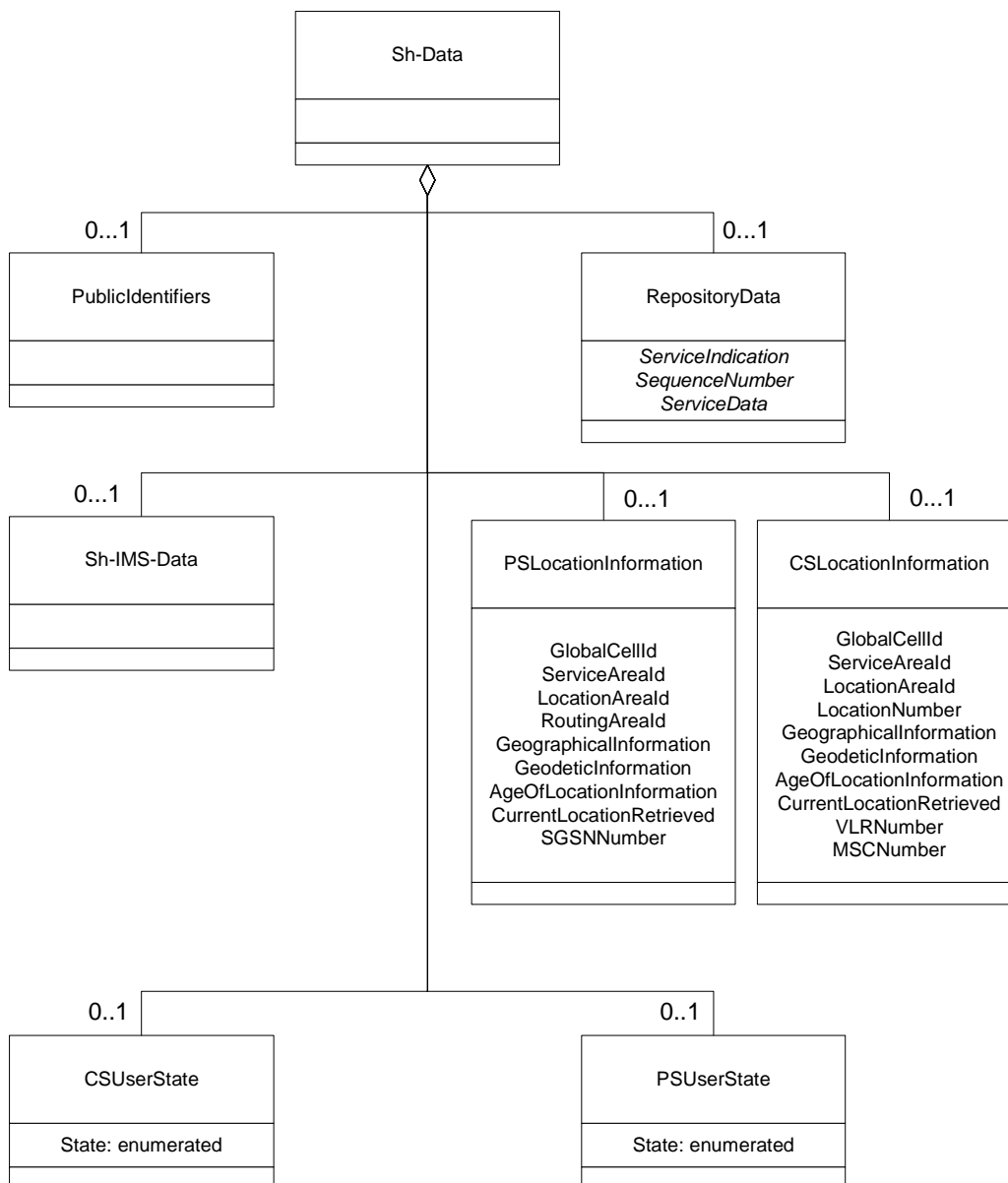
Figure C.1.1: Sh-Data

Each instance of the Sh-Data class contains 0 or 1 instance of the class PublicIdentifiers, 0 or 1 instance of the class RepositoryData, 0 or 1 instance of the class Sh-IMS-Data, 0 or 1 instance of the class CSUserState, 0 or 1 instance of

the class PSUserState ~~and/or~~ 0 or 1 instance of the class CSLocationInformation and~~or~~ 0 or 1 instance of the class PSLocationInformation.

Class RepositoryData contains repository data (transparent data) for a given service. It has attributes ServiceIndication, SequenceNumber and ServiceData.

Class CSUserState contains the state of a user in the CS domain. Its only attribute, State, is an enumeration whose possible values are defined in section ~~chapter~~ 7.6.7.

Class PSUserState contains the state of a user in the PS domain. Its only attribute, State, is an enumeration whose possible values are defined in section~~chapter~~ 7.6.7.

NOTE: the fact that attribute State is an enumeration is a difference from what can be carried in the MAP protocol.

Class CSLocationInformation has the attributes Location Number, Service Area ID, GlobalCellId, LocationAreaId, GeographicalInformation, GeodeticInformation, VLR Number, MSC Number, AgeOfLocationInformation and CurrentLocationRetrieved. They are defined in 7.6.

Class PSLocationInformation has the attributes ServiceAreaId, GlobalCellId, LocationAreaID, RoutingAreaID, GeographicalInformation, GeodeticInformation, SGSN Number, AgeOfLocationInformation and CurrentLocationRetrieved. They are defined in 7.6.

C.2 PublicIdentifiers

The following picture details the UML model of the class PublicIdentifiers:
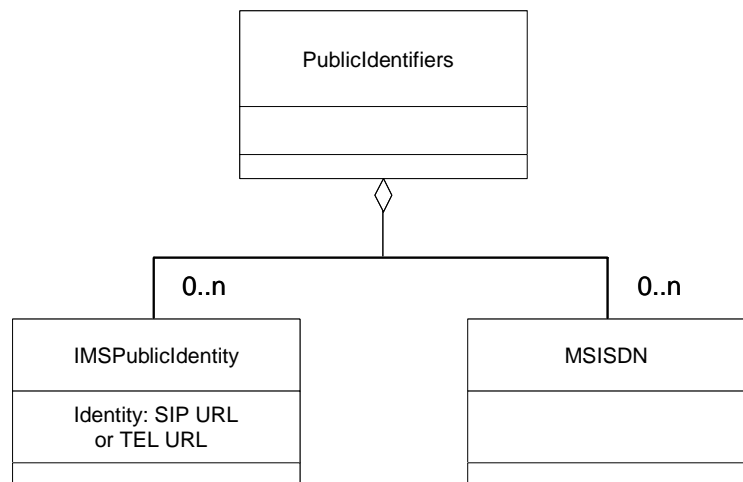
Figure C.2.1: The UML model of the class PublicIdentifiers

Class PublicIdentifiers contains 0 or more ~~to n user~~ public user identities which may be either of class IMSPublicIdentity or of class MSISDN. The identifiers are of format SIP URL, TEL URL or MSISDN.

C.3 Sh-IMS-Data

The following picture details the UML model of the class Sh-IMS-Data.
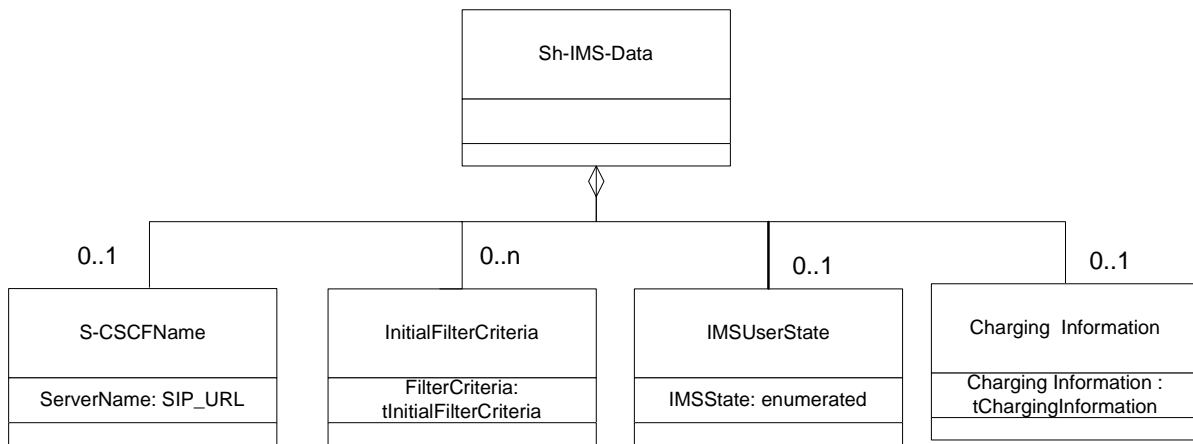
Figure C.3.1: Sh-IMS-Data

Each instance of the class Sh-IMS-Data contains 0 or 1 instance of the class S-CSCFName, 0 to n instances of the class InitialFilterCriteria, 0 or 1 instance of the class IMSUserState, and/or 0 or 1 instance of the class ChargingInformation.

Class S-CSCFName contains the SIP URL of the S-CSCF where the multimedia public identity that the AS included in the request is registered.

Class InitialFilterCriteria is defined in 3GPP TS 29.228 [6] and contains the initial filter criteria of the multimedia public identity that the AS included in the request.

Class IMSUserState contains the registration state of the identity given by the attribute of class Sh-IMS-Data. See section~~chapter~~ 7.6 for possible values.

Class Charging Information contains the online and offline charging function addresses. See section~~chapter~~ 7.6 for possible values.

Annex D (normative): XML schema for the Sh interface user profile

The file ShDataType.xsd, attached to this specification, contains the XML schema for the user profile that is sent over the Sh interface. The user profile XML schema defines the data types ~~types~~ 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.~~2~~329 [5]. The user profile XML schema file is intended to be used by an XML parser. The version of the Sh 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.

Tables D.1 and D.2 describe the data types and the dependencies among them that configure the user profile XML schema.

Table D.1: XML schema for the Sh user profile interface: simple data types

Data type	Tag	Base type	Comments
tPriority	Priority	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_SESSION 2 (TERMINATING_UNREGISTERED)
tIMSUserState	IMSUserState	Enumerated	Possible values: 0 (NOT_REGISTERED) 1 (REGISTERED) 2 (REGISTERED_UNREG_SERVICES) 3 (AUTHENTICATION_PENDING)
tCSUserState	CSUserState	Enumerated	Possible values (as defined in 3GPP TS 23.078 [14]): 0 (CAMELBusy) 1 (NetworkDeterminedNotReachable) 2 (AssumedIdle) 3 (NotProvidedfromVLR)
tPSUserState	PSUserState	Enumerated	Possible values (as defined in 3GPP TS 23.078 [14]): 0 (Detached) 1 (AttachedNotReachableForPaging) 2 (AttachedReachableForPaging)

			3 (ConnectedNotReachableForPaging)
			4 (ConnectedReachableForPaging)
			5 (NotProvidedFromSGSN)
tLocationNumber	LocationNumber	string	Syntax described in ITU-T Q.763 [9] (Base64 encoded according to RFC 2045 [15]). Lengh~~th~~ >=4 and <=16 (multiples of 4).
tCellGlobalId	CellGlobalId	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to RFC 2045 [15]). Length = 12.
tServiceAreaId	ServiceAreaId	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to RFC 2045 [15]). Length = 12.
tLocationAreaId	LocationAreaId	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to RFC 2045 [15]). Length = 8.
tRoutingAreaId	RoutingAreaId	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to RFC 2045 [15]). Length = 8.
tGeographicalInformation	GeographicalInformation	string	Syntax described in 3GPP TS 29.002 (base 64 encoded according to RFC 2045). Length = 12.
tGeodeticInformation	GeodeticInformation	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to RFC 2045 [15]). Length = 16.
tAgeOfLocationInformation	AgeOfLocationInformation	integer	>=0, <=32767
tAddressString	AddressString	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to RFC 2045 [15]). Length >= 4 and <=28 (multiples of 4).
tMSISDN	MSISDN	string	Syntax described in 3GPP TS 23.003 [11].
tSIP_URL	PublicIdentity	anyURI	Syntax described in RFC 3261 [16]
tTEL_URL	PublicIdentity	anyURI	Syntax described in RFC 2806 [17]
tDiameterURI	DiameterURI	string	Syntax of a Diameter URI as described in IETF RFC 3588 [8]
tIMSPublicIdentity	IMSPublicIdentity	(union)	Union of tSIP_URL and tTEL_URL

tServiceInfo	ServiceInfo	string	
tString	RequestURI, Method, Header, Content, Line	string	
tBool	ConditionTypeCNF, ConditionNegated	boolean	Possible values: 0 (false) 1 (true)
tSequenceNumber	SequenceNumber	integer	>=0, <=65535

Table D.2: XML schema for the Sh user profile interface: complex data types

Data type	Tag	Compound of		
		Tag	**Type**	**Cardinality**
tSh-Data	Sh-Data	PublicIdentifiers	tPublicIdentity	0 to 1
		RepositoryData	tTransparentData	0 to 1
		Sh-IMS-Data	tShIMSData	0 to 1
		CSLocationInformation	tCSLocationInformation	0 to 1
		PSLocationInformation	tPSLocationInformation	0 to 1
		CSUserState	tCSUserState	0 to 1
		PSUserState	tPSUserState	0 to 1
tTransparentData	RepositoryData	ServiceIndication	string	1
		SequenceNumber	tSequenceNumber	1
		ServiceData	tServiceData	0 to 1
tServiceData	any	any	any	1
tShIMSData	Sh-IMS-Data	SCSCFName	tSIP_URL	0 to 1
		InitialFilterCriteria	tInitialFilterCriteria	0 to n
		IMSUserState	tIMSUserState	0 to 1
		ChargingInformation	tChargingInformation	0 to 1
tCSLocationInformation	CSLocationInformation	LocationNumber	tLocationNumber	0 to 1
		CellGlobalId	tCellGlobalId	0 to 1
		ServiceAreaId	tServiceAreaId	0 to 1
		LocationAreaId	tLocationAreaId	0 to 1
		GeographicalInformation	tGeographicalInformation	0 to 1

		GeodeticInformation	tGeodeticInformation	0 to 1
		VLRNumber	tISDNAddress	0 to 1
		MSCNumber	tISDNAddress	0 to 1
		CurrentLocationRetrieved	tBool	0 to 1
		AgeOfLocationInformation	tAgeOfLocationInformation	0 to 1
tPSLocationInformation	PSLocationInformation	CellGlobalId	tCellGlobalId	0 to 1
		ServiceAreaId	tServiceAreaId	0 to 1
		LocationAreaId	tLocationAreaId	0 to 1
		RoutingAreaId	tRoutingAreaId	0 to 1
		GeographicalInformation	tGeographicalInformation	0 to 1
		GeodeticInformation	tGeodeticInformation	0 to 1
		SGSNNumber	tISDNAddress	0 to 1
		CurrentLocationRetrieved	tBool	0 to 1
		AgeOfLocationInformation	tAgeOfLocationInformation	0 to 1
tPublicIdentity	PublicIdentifiers	IMSPublicIdentity	tIMSPublicIdentity	0 to n
		MSISDN	tMSISDN	0 to n
tInitialFilterCriteria	InitialFilterCriteria	Priority	tPriority	1
		TriggerPoint	tTrigger	0 to 1
		ApplicationServer	tApplicationServer	1
tTrigger	TriggerPoint	ConditionTypeCNF	tBool	1

		SPT	tSePoTri	0 to n
tSePoTri	SPT	ConditionNegated	tBool	0 to 1
		Group	tGroupID	1 to n
		Choice / RequestURI	tString	1
		Choice / Method	tString	1
		Choice / SIPHeader	tHeader	1
		Choice / SessionCase	tDirectionOfRequest	1
		Choice / SessionDescription	tSessionDescription	1
		RegistrationType	tRegistrationType	(0 to 2)
tHeader	SIPHeader	Header	tString	1
		Content	tString	0 to 1
tSessionDescription	SessionDescription	Line	tString	1
		Content	tString	0 to 1
tApplicationServer	ApplicationServer	ServerName	tSIP_URL	1
		DefaultHandling	tDefaultHandling	0 to 1
		ServiceInfo	tServiceInfo	0 to 1
tChargingInformation	ChargingInformation	PrimaryEventChargingFunctionName	tDiameterURI	0 to 1
		SecondaryEventChargingFunctionName	tDiameterURI	0 to 1
		PrimaryChargingCollectionFunctionName	tDiameterURI	1
		SecondaryChargingCollectionFunctionName	tDiameterURI	0 to 1
NOTE: "n" shall be interpreted as non-bounded.				

3GPP TSG–CT4 Meeting #27   *Tdoc* ⌘**C4-050853**
Cancun, Mexico, 25th to 29th April 2005

	CR-Form-v7

CHANGE REQUEST

⌘	**29.328** CR **130**	⌘**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 **X**

Title: ⌘	Sh procedures applicable to Public Service Identity	
Source: ⌘	Orange, Ericsson	
Work item code:⌘	IMS2-CCR	***Date:*** ⌘ 30/03/2005
Category: ⌘ **F**		***Release:*** ⌘ REL-6

Use one of the following categories:	*Use one of the following releases:*
F (correction)	*2 (GSM Phase 2)*
A (corresponds to a correction in an earlier release)	*R96 (Release 1996)*
B (addition of feature),	*R97 (Release 1997)*
C (functional modification of feature)	*R98 (Release 1998)*
D (editorial modification)	*R99 (Release 1999)*
Detailed explanations of the above categories can	*Rel-4 (Release 4)*
be found in 3GPP TR 21.900.	*Rel-5 (Release 5)*
	Rel-6 (Release 6)

Reason for change:⌘	TS 23.228 section 5.4.12. 2 requires the following:
	Distinct PSIs can also be created and deleted by users using the Ut interface using the means described in sub-clause 5.4.12.3 for subdomain-based PSIs. The distinct PSI may then be created in the HSS by the AS using the Sh interface.
	Since data can be manipulated for PSI users via the Ut interface, it should be possible for the AS to update the corresponding transparent repository data in the HSS if any. More generally, it should be possible for the AS to interact with the HSS via the Sh interface for PSI users as well as for IMS subscribers.
Summary of change: ⌘	In section 6 about Sh procedures and in section 7 about IE content, the User Identity IE is extended to PSI users in addition to IMS subscribers. In addition this CR changes the word "user" for the corresponding IMS identity in some cases where the word "user" is not specific enough.
Consequences if not approved:	Incomplete specifications: Sh procedures are not applicable to PSI users.

Clauses affected: ⌘	6.1, 6.5, 7

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

Other comments: ⌘

*** FIRST MODIFICATION ***

6.1 User data handling procedures

6.1.1 Data read (Sh-Pull)

This procedure is used between the AS and the HSS. The procedure is invoked by the AS and is used:

- To read transparent and/or non-transparent data for a specified ~~user~~ IMS Subscription from the HSS.

This procedure is mapped to the commands User-Data-Request/Answer in the Diameter application specified in 3GPP TS 29.329 [5]. Tables 6.1.1.1 and 6.1.1.2 detail the involved information elements.

Table 6.1.1.1: Sh-Pull

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1)	User-Identity	M	IMS Public User Identity or Public Service Identity or MSISDN of the user for whom the data is required. See section 7.1 for the content of this AVP.
Requested data (See 7.3)	Data-Reference	M	This information element indicates the reference to the requested information. The set of valid reference values are defined in 7.6.
Requested Identity set (See 7.11)	Identity-Set	O	If Data-Reference indicates that IMS Public Identities is the requested data set to be downloaded, this information element should be included. When this information element takes the value IMPLICIT_IDENTITIES, the HSS shall provide all non-barred IMS Public Identities that are belong to the same implicit registration set as the IMS Public Identity included in the message in the User-Identity AVP. The MSISDN user identity is not applicable for this value. When this information element takes the value REGISTERED_IDENTITIES, the HSS shall provide all non-barred IMS Public Identities whose state is registered, belonging to all Private Identities that the IMS Public Identity or MSISDN in the User-Identity AVP is associated with. When this information element takes the value ALL_IDENTITIES, the HSS shall provide all non-barred IMS Public Identities, belonging to all Private Identities that the IMS Public Identity or MSISDN in the User-Identity AVP is associated with. If Data-Reference indicates that IMS Public Identities is the requested data set to be downloaded and this information element is not included, the HSS shall download the set of IMS Public Identities that would be downloaded if the value of this information element had been ALL_IDENTITIES.
Requested domain (See 7.2)	Requested-Domain	C	This information element indicates the domains to which the operation is applicable. Check table 7.6.1 to see when it is applicable.
Current Location (See 7.8)	Current-Location	C	This information element indicates whether an active location retrieval has to be initiated or not. It shall be present if Location Information is requested. If this information element takes the value InitiateActiveLocationRetrieval (1) the HSS shall indicate to the MSC/VLR and/or SGSN the need to initiate an active location retrieval. Check table 7.6.1 to see when it is applicable.
Service Indication (See 7. 4)	Service-Indication	C	IE that identifies, together with the IMS Public User Identity included in the User-Identity AVP and Data-Reference, the set of service related transparent data that is being requested. Check table 7.6.1 to see when it is applicable.
Application Server Identity (See 7.9)	Origin-Host	M	IE that identifies the AS originator of the request and that is used to check the AS permission list.
Application Server Name	Server-Name	C	IE that is used, together with the IMS Public User Identity included in the User-Identity AVP and Data-Reference, as key to identify the filter criteria. Check table 7.6.1 to see when it is applicable.

Table 6.1.1.2: Sh-Pull Resp

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.5)	Result-Code / Experimental_ Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Sh 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.
Data (See 7.6)	User-Data	O	Requested data.

6.1.1.1   Detailed behaviour

The conditions for the inclusion of Requested-Domain as an additional key to the requested data are described in table 7.6.1. If repository data is requested, Service-Indication shall be present in the request. If initial filter criteria are requested, the Server-Name AVP shall contain the SIP URL of the AS that initiates the request; requests for initial filter criteria are limited to those initial filter criteria which are relevant to the requesting AS.

Upon reception of the Sh-Pull request, the HSS shall, in the following order:

1. In the AS permission list (see section 6.2) check that the requested user data is allowed to be read (Sh-Pull) by this AS by checking the combination of the identity of the AS sending the request (identified by the Origin-Host AVP) and the supplied Data-Reference.

   If the data referenced in the request is not allowed to be read, Experimental-Result Code shall be set to DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ in the Sh-Pull Response.

2. Check that the user User Identity for whom data is asked exists in HSS. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Sh-Pull Response.

3. Check whether or not the data that is requested to be downloaded by the AS is currently being updated by another entity. If there is an update of the data in progress, the HSS may delay the Sh-Pull-Resp message until the update has been completed and shall include in the Sh-Pull-Resp message the updated data requested. The HSS shall ensure that the data returned is not corrupted by this conflict.

If there is an error in any of the above steps then the HSS shall stop processing and shall return the error code specified in the respective step (see 3GPP TS 29.329 [5] and 3GPP TS 29.229 [7] for an explanation of the error codes).

If the HSS cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY.

Otherwise, the requested operation shall take place and the HSS shall return the Result-Code AVP set to DIAMETER_SUCCESS and the requested data identified by User-Identity and Data-Reference in the Sh-Pull Response message.

6.1.2   Data Update (Sh-Update)

This procedure is used between the AS and the HSS. The procedure is invoked by the AS and is used:

- To allow the AS to update the transparent (repository) data stored at the HSS for a specified user each IMS Public User Identity or Public Service Identity.

This procedure is mapped to the commands Profile-Update-Request/Answer in the Diameter application specified in 3GPP TS 29.329 [5]. Tables 6.1.2.1 and 6.1.2.2 detail the involved information elements.

Table 6.1.2.1: Sh-Update

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1)	User-Identity	M	IMS Public User Identity or Public Service Identity ~~of the user~~ for which data is updated. See section 7.1 for the content of this AVP.
Requested data (See 7.3)	Data-Reference	M	This information element includes the reference to the data on which updates are required (possible values of the Data Reference are defined in Table 7.6.1).
Data (See 7.6)	User-Data	M	Updated data.
Application Server Identity (See 7.9)	Origin-Host	M	IE that identifies the AS originator of the request and that is used to check the AS permission list.

Table 6.1.2.2: Sh-Update Resp

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.5)	Result-Code / Experimental-Result	M	Result of the update of data in the HSS. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Sh 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.

6.1.2.1   Detailed behaviour

Within the Sh-Update Request, the keys to determine the updated data are part of the information element Data (See 7.6). When data in the repository is updated (i.e. added, modified or removed) Service-Indication and Sequence-Number are also sent as part of the information element Data.

Newly added transparent data shall be associated with a Sequence Number of 0 in the Sh-Update Request. Sequence Number value 0 is reserved exclusively for indication of newly added transparent data.
Modified and removed transparent data shall be associated within the Sh-Update Request with a Sequence Number of n+1 where n is the original Sequence Number associated with the transparent data before modification or removal. If n equals 65535, then the next modification or deletion of that transparent data shall be associated with a Sequence Number of 1.

Upon reception of the Sh-Update request, the HSS shall, in the following order:

1. In the AS permission list (see section 6.2) check that the ~~user~~ data that is requested to be updated (Sh-Update) by this AS, is allowed to be updated by checking the combination of the identity of the AS sending the request (identified by the Origin-Host AVP) and the supplied Data-Reference.

   - If the data is not allowed to be updated, Experimental-Result Code shall be set to DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED in the Sh-Update Response.

2. Check that the IMS Public User Identity or Public Service Identity in the request ~~user for whom the data is asked to be updated~~ exists in the HSS. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Sh-Update Response.

3. Check whether or not the data that is requested to be updated by the AS, as identified by the Service-Indication, is currently being updated by another entity. If there is an update of the data in progress, Experimental-Result Code shall be set to DIAMETER_PRIOR_UPDATE_IN_PROGRESS in the Sh-Update Response.

4. Check whether or not there is any repository data stored at the HSS already for the specified Service-Indication and the associated ~~user~~IMS Public User Identity or Public Service Identity.

   - If repository data identified by the Service-Indication is stored at the HSS for the specified IMS Public User Identity or Public Service Identity~~user~~, check the following premises:

1. Sequence_Number_in_Sh_Update is not equal to 0

2. (Sequence_Number_in_Sh_Update - 1) is equal to (Sequence_Number_In_HSS modulo 65535)

- If either of the above premises is false then Experimental-Result-Code shall be set to DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC in the Sh-Update Response.

- If both of the above premises are true, then check whether or not Service Data is received within the Sh-Update Req.

    - If Service Data is included in the Sh-Update Req, check whether or not the size of the data is greater than that which the HSS is prepared to accept.

        - If there is more data than the HSS is prepared to accept then Experimental-Result-Code shall be set to DIAMETER_ERROR_TOO_MUCH_DATA and the new data shall be discarded.

        - If the HSS is prepared to accept the data, then the repository data stored at the HSS shall be updated with the repository data sent in the Sh-Update Req and the Sequence Number associated with that repository data shall be updated with that sent in the Sh-Update Req. This triggers the sending of Sh-Notif messages to any other ASs that are subscribed to Notifications for updates to the service data for that IMS Public User Identity or Public Service Identity ~~user~~ (see 6.1.4).

    - If Service Data is not received, the data stored in the repository at the HSS shall be removed, and as a consequence the Service Indication and the Sequence Number associated with the removed data shall also be removed. This triggers the sending of Sh-Notif messages to any other ASs that are subscribed to Notifications for updates to the service data for that IMS Public User Identity or Public Service Identity ~~user~~ (see 6.1.4). After sending Sh-Notif messages, the subscriptions to Notifications for the removed Repository Data shall be deleted.

- If repository data identified by the Service-Indication is not stored for the IMS Public User Identity or Public Service Identity ~~user~~ i.e. the Sh-Update Req intends to create a new repository data, check whether or not the Sequence Number in the Sh-Update Req is 0.

    - If the sequence number is not set to 0, Experimental-Result Code shall be set to DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC

    - If the sequence number is set to 0 check whether Service Data is included within the Sh-Update Req.

        - If Service Data is not included in the Sh-Update Req, then Experimental-Result-Code shall be set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED and the operation shall be ignored by the HSS.

        - If Service Data is included in the Sh-Update Req, check whether or not the size of the data is greater than that which the HSS is prepared to accept. If there is more data than the HSS is prepared to accept then Experimental-Result-Code shall be set to DIAMETER_ERROR_TOO_MUCH_DATA and the new data shall be discarded.

        - If the HSS is prepared to accept the data included in the Sh-Update Req, then the data shall be stored inwithin the data repository in the HSS.

If there is an error in any of the above steps then the HSS shall stop processing and shall return the error code specified in the respective step (see 3GPP TS 29.329 [5] and 3GPP TS 29.229 [7] for an explanation of the error codes).

If the HSS cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY.

Otherwise, the requested operation shall take place and the HSS shall return the Result-Code AVP set to DIAMETER_SUCCESS.

NOTE: When an AS receives DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC the AS may attempt to resolve the inconsitency between the version of the repository data that it holds and that stored at the HSS. It may execute a Sh-Pull to retrieve the current version of the data from the HSS or it tmay wait to receive a subsequent Sh-Notif message from the HSS for the affected repository data.

6.1.3   Subscription to notifications (Sh-Subs-Notif)

This procedure is used between the AS and the HSS. The procedure is invoked by the AS and is used:

- To subscribe to Notifications for when particular transparent and/or non-transparent data for a specified IMS Public User Identity or Public Service Identity~~user~~ is updated, from the HSS.

This procedure is mapped to the commands Subscribe-Notifications-Request/Answer in the Diameter application specified in 3GPP TS 29.329 [5]. Tables 6.1.3.1 and 6.1.3.2 detail the information elements involved.

Table 6.1.3.1: Sh-Subs-Notif

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1)	User-Identity	M	IMS public identity or Public Service Identity ~~of the user for whom~~ for which notifications of data changes are requested. See section 7.1 for the content of this AVP.
Requested data (See 7.3)	Data-Reference	M	This information element includes the reference to the data on which notifications of change are required (valid reference values are defined in 7.6).
Subscription request type (See 7.7)	Subs-Req-Type	M	This information element indicates the action requested on subscription to notifications.
Service Indication (See 7.4)	Service-Indication	C	IE that identifies, together with the IMS Public User Identity and Data-Reference, the set of service related transparent data for which notifications of changes are requested. This element shall be present when the Data-Reference value is RepositoryData (0).
Application Server Identity (See 7.9)	Origin-Host	M	IE that identifies the AS originator of the request and that is used to check the AS permission list.
Application Server Name	Server-Name	C	IE that is used, together with the IMS Public user Identity and Data-Reference, as key to identify the filter criteria. This element shall be present when the Data-Reference value is InitialFilterCriteria (13).

Table 6.1.3.2: Sh-Subs-Notif Resp

Information element name	Mapping to Diameter AVP	Cat.	Description
Data request result (See 7.5)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Sh 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 take note of the subscription request on the data identified by IMS Public User Identity and Data-Reference. If notifications on changes of repository data are requested, Service-Indication shall be present in the request. If notifications on changes of filter criteria are requested, the Server-Name AVP shall be used as key to the filter criteria. The Server-Name AVP shall contain the SIP URL of the AS sending the request.

Upon reception of the Sh-Subs-Notif request, 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 29.329 [5] and 3GPP TS 29.229 [7]):

1. In the AS permission list (see section 6.2) the HSS shall check that the AS is allowed to subscribe to notifications (Sh-Subs-Notif) for the requested ~~user~~ data by checking the combination of the identity of the AS sending the request (identified by the Origin-Host AVP) and the supplied Data-Reference.

   - If this AS does not have Sh-Subs-Notif permission for the data referenced, Experimental-Result Code shall be set to DIAMETER_ERROR_USER_DATA_CANNOT_BE_NOTIFIED in the Sh-Subs-Notif Response.

2. Check that the <u>IMS Public User Identity or Public Service Identity in the request</u> ~~user for whom notifications are asked~~ exists in HSS. If not, Experimental-Result Code shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Sh-Subs-Notif Response.

If the HSS cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY.

6.1.4   Notifications (Sh-Notif)

This procedure is used between the HSS and the AS. The procedure is invoked by the HSS and is used:

- To inform the AS of changes in transparent and/or non-transparent data to which the AS has previously subscribed to receive Notifications for, using Sh-Subs-Notif (see 6.1.3).

This procedure is mapped to the commands Push-Notification-Request/Answer in the Diameter application specified in 3GPP TS 29.329 [5]. Tables 6.1.4.1 and 6.1.4.2 detail the involved information elements.

Table 6.1.4.1: Sh-Notif

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1)	User-Identity	M	IMS Public User Identity <u>or Public Service Identity</u> ~~of the user~~<u>for</u> which data has changed. See section 7.1 for the content of this AVP.
Requested Data (See 7.6)	User-Data	M	Changed data.

Table 6.1.4.2: Sh-Notif Resp

Information element name	Mapping to Diameter AVP	Cat.	Description
Data request result (See 7.5)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Sh 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.

6.1.4.1   Detailed behaviour

The keys to the updated data are part of the information element User-Data (See Annex C). When data repository is updated Service-Indication is also part of the information element User-Data.

Since authentication pending is a transient state of normally very short duration, notification of an IMS user's state change, to and from the authentication pending state shall not be sent to Application Servers, when the previous state before authentication pending and next state after authentication pending are the same. If the states are different before the authentication pending state is entered and after the authentication pending state is left then notification is sent to the AS of this new state.

*** NEXT MODIFICATION ***

6.5 User identity to HSS resolution

The User identity to HSS resolution mechanism enables the AS to find the address of the HSS that holds the subscriber data for a given IMS Public User Identity or Public Service Identity~~public user identity~~ when multiple and separately addressable HSSs have been deployed by the network operator. The resolution mechanism is not required in networks that utilise a single HSS or when an AS is configured to use pre-defined HSS.

The resolution mechanism described in 3GPP TS 23.228 [8] is based on the Subscription Locator Function (SLF). The AS accesses the subscription locator via the Dh interface. The Dh interface is always used in conjunction with the Sh interface. The Dh interface is based on Diameter. Its functionality is implemented by means of the routing mechanism provided by an enhanced Diameter redirect agent, which is able to extract the ~~public user identity~~IMS Public User Identity or Public Service Identity from the received requests.

To get the HSS address the AS sends to the SLF the Sh requests aimed for the HSS. On receipt of the HSS address from the SLF, the AS shall send the Sh requests to the HSS. The AS may store the HSS address and use it in further requests associated to the same ~~public user identity~~IMS Public User Identity or Public Service Identity.

In networks where the use of the user identity to HSS resolution mechanism is required and the AS is not configured to use predefined HSS, each AS shall be configured with the address/name of the SLF implementing this resolution mechanism.

*** NEXT MODIFICATION ***

7 Information element contents

7.1 User Identity

This information element contains a user identity according to the conditions described in table 7.1.1.

Table 7.1.1: User Identity content

Information element name	Mapping to Diameter AVP	Cat.	Description
IMS Public User Identity/Public Service Identity (See 7.1.1)	Public-Identity	C	IMS Public User Identity or Public Service Identity ~~of the user~~ for ~~whom~~ which the data is required. If the MSISDN is not included in the User-Identity AVP, the Public-Identity AVP shall be included in Sh messages only for allowed Data References as described in Table 7.6.1.
MSISDN (See 7.1.2)	MSISDN	C	MSISDN ~~of the user~~ for ~~whom~~ which the data is required. If the Public-Identity AVP is not included in the User-Identity AVP, the MSISDN AVP shall be included in the Sh-Pull message only for allowed Data References as described in Table 7.6.1.

7.1.1 IMS Public User Identity/Public Service Identity

This information element contains an IMS ~~public~~Public ~~user~~User ~~identity~~Identity/Public Service Identity (either SIP-URI or TEL-URL). See 3GPP 23.003 [11].

7.1.2 MSISDN

This information element contains a Basic MSISDN (see 3GPP TS 23.012 [19]).

7.2 Requested Domain

This information element details the access domains for which certain data (e.g. user state, location information) are requested. See 3GPP TS 29.329 [5] for the list of possible values.

7.3   Requested Data

-       Reference to the data that an AS is requesting from the HSS.

-       Reference to the data which, an AS wants to be notified of, when changed.

-       Reference to data for which subscription to notification of change is rejected.

See chapter 7.6.

7.4   Service Indication

Identifier of one set of service related transparent data, which is stored in an HSS in an operator network. It shall be unique within an operator network. Per IMS Public User Identity or Public Service Identity user and value of Service Indication the HSS may allocate memory space to implement a data repository to store transparent data.

7.5   Result

This information element contains the result code of the operation. See 3GPP TS 29.329 [5] for the list of possible values.

7.6   Data

This information element contains an XML document conformant to the XML schema defined in Annex D.

Annex C specifies the UML logical model of the data downloaded via the Sh interface.

Table 7.6.1 defines the data reference values and tags, access key and recommended AS permissions (as described in section 6.2) for the the operation(s) on data accessible via the Sh interface, i.e. the listed operation(s) in the Operations column are the only ones allowed to be used with this Data Ref value. It is a matter of operator policy to further restrict the AS permission rights defined in table 7.6.1.

Table 7.6.1: Data accessible via Sh interface

Data Ref.	XML tag	Defined in	Access key	Operations
0	RepositoryData	7.6.1	IMS Public User Identity or Public Service Identity + Data-Reference + Service-Indication	Sh-Pull, Sh-Update, Sh-Subs-Notif
10	IMSPublicIdentity	7.6.2	IMS Public User Identity or MSISDN + Data-Reference + Identity-Set	Sh-Pull
11	IMSUserState	7.6.3	IMS Public User Identity + Data-Reference	Sh-Pull, Sh-Subs-Notif
12	S-CSCFName	7.6.4	IMS Public User Identity or Public Service Identity + Data-Reference	Sh-Pull, Sh-Subs-Notif
13	InitialFilterCriteria	7.6.5	IMS Public User Identity or Public Service Identity + Data-Reference + Server-Name	Sh-Pull, Sh-Subs-Notif
14	LocationInformation	7.6.6	MSISDN + Data-Reference+ Requested-Domain	Sh-Pull
15	UserState	7.6.7		Sh-Pull
16	Charging information	7.6.8	IMS Public User Identity or Public Service Identity or MSISDN + Data-Reference	Sh-Pull
17	MSISDN	7.6.9	IMS Public User Identity or MSISDN + Data-Reference	Sh-Pull

7.6.1   Repository Data

This information element contains transparent data. A data repository may be shared by more than one AS implementing the same service.

7.6.2   IMSPublicIdentity

This information element contains an IMS Public User Identity or a Public Service Identity. If a wildcarded PSI is stored in the HSS for the Public Service Identity received, the HSS shall do the matching and return the wildcarded PSI.

An IMS Public User Identitythat would be either:

- associated with the Private Identity of the subscriber for whom the IMS User Public User Identity is included in the request or

- associated with the MSISDN present in the request.

Multiple instances of this information element may be included in the message.

7.6.3   IMS User State

This information element contains the IMS User State of the public identifier referenced. Its possible values are:

- REGISTERED,

- NOT_REGISTERED,

- AUTHENTICATION_PENDING,

- REGISTERED_UNREG_SERVICES.

If the <u>IMS</u> Public User Identity is shared between multiple Private User Identities, HSS shall indicate the most registered state of the shared Public User Identity to an AS. The most registered state of a shared <u>IMS</u> Public User Identity is defined as follows:

-   If the shared <u>IMS</u> Public User Identity is registered with any of the Private User Identities, the most registered state of the shared <u>IMS</u> Public User Identity is REGISTERED.

-   If the shared <u>IMS</u> Public User Identity is not currently registered with any of the Private User Identities, but it is in state REGISTERED_UNREG_SERVICES, then the most registered state of the shared <u>IMS</u> Public User Identity is REGISTERED_UNREG_SERVICES.

-   If the shared <u>IMS</u> Public User Identity is not currently registered with any of the Private User Identities, and it is not in state REGISTERED_UNREG_SERVICES, but it is in the process of being authenticated with any of the Private User Identities, then the most registered state of the shared <u>IMS</u> Public User Identity is AUTHENTICATION_PENDING.

-   If the shared <u>IMS</u> Public User Identity is not currently registered with any of the Private User Identities, and it is not in state REGISTERED_UNREG_SERVICES, and it is not in the process of being authenticated with any of the Private User Identities, then the most registered state of the shared <u>IMS</u> Public User Identity is NOT_REGISTERED.

7.6.4   S-CSCF Name

This information element contains the name of the S-CSCF where a multimedia public identity is registered.

7.6.5   Initial Filter Criteria

This information element contains the triggering information for a service.

For a more detailed description, refer to 3GPP TS 23.218 [4] and 3GPP TS 29.228 [6].

7.6.6   Location Information

This information elementcontains the location of the served subscriber in the MSC/VLR if the requested domain is CS, or the location of the served subscriber in the SGSN if the requested domain is PS. If the HSS has to communicate with the MSC/VLR and/or SGSN to retrieve location information, it shall make use of the service MAP-PROVIDE-SUBSCRIBER-INFO.

For both Location Information for CS and Location Information for GPRS, the considerations described in 3GPP TS 23.078 [14] apply.

7.6.6.1   Location information for CS

This information elementconsists of the following subordinate information elements:

-   Location number: defined in ITU-T Recommendation Q.763 [9]. Considerations described in 3GPP TS 23.018 apply[10].

-   Service area ID: defined in 3GPP TS 23.003 [11].

-   Global Cell ID: defined in 3GPP TS 23.003 [11].

-   Location area ID: defined in 3GPP TS 23.003 [11].

-   Geographical Information: defined in 3GPP TS 23.032 [12]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.

-   Geodetic Information: defined in ITU-T Recommendation Q.763 [9]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.

-   VLR Number: defined in 3GPP TS 23.003 [11].

-   MSC Number: defined in 3GPP TS 23.003 [11].

- Age of location information: defined in 3GPP TS 23.018 [10].

- Current Location Retrieved: shall be present when location information was obtained after a successful paging procedure for Active Location Retrieval.

7.6.6.2   Location information for GPRS

This information element consists of the following subordinate information elements:

- Service area ID: defined in 3GPP TS 23.003 [11].

- Global Cell ID: defined in 3GPP TS 23.003 [11].

- Location area ID: defined in 3GPP TS 23.003 [11].

- Geographical Information: defined in 3GPP TS 23.032 [12]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.

- Geodetic Information: defined in ITU-T Recommendation Q.763 [9]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.

- SGSN Number: defined in 3GPP TS 23.003 [11].

- Routing Area ID: defined in 3GPP TS 23.003 [11].

- Current Location Retrieved: shall be present when location information was obtained after a successful paging procedure for Active Location Retrieval.

7.6.7   User state

This information element indicates the state of the user in the domain indicated by the Requested-Domain (see 7.2), with the values specified in 3GPP TS 23.078 [14] for Subscriber State and PS Domain Subscriber State. The HSS shall make use of the operation MAP-PROVIDE-SUBSCRIBER-INFO towards the MSC/VLR and/or the SGSN to obtain this information.

7.6.8   Charging information

This information element contains the addresses of the charging functions (primary event charging function name, secondary event charging function name, primary charging collection function name, secondary charging collection function name). When a clash occurs between the charging function address(es) received over the ISC interface and those received over the Sh interface, the address(es) received over the ISC interface should take precedence.

NOTE: The use of the Sh interface to retrieve charging function addresses is not intended as a general-purpose alternative to receiving charging function addresses from the ISC interfaces. Rather, it is meant to address a special case where the AS needs to interact with the charging system before initiating a request to a user when the AS has not received the third party REGISTER for that user.

7.6.9   MSISDN

This information element contains a Basic MSISDN (see 3GPP TS 23.012 [19]) that is associated with the User Identity present in the request. All valid instances of this information element shall be included in the message.

7.7   Subscription request type

This information element indicates the action requested for subscription to notifications. See 3GPP TS 29.329 [5] for the list of valid values.

7.8   Current Location

This information element indicates whether an active location retrieval has to be initiated or not when an AS requested location information. See 3GPP TS 29.329 [5] for the list of possible values.

7.9 Application Server Identity

This information element contains the identity of the Application Server. It is used for the AS permission check (see 6.2).

7.10 Application Server Name

This information element indicates application server's SIP URI. See 3GPP TS 29.229 [7] for the detailed definition of the AVP.

7.11 Requested Identity Set

This information element indicates the set of IMS Public Identities that the AS wishes to download. See 3GPP TS 29.329 [5] for the detailed definition of the AVP.

*** END OF MODIFICATION ***