

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Sh/Dh Interface

Contents

1	General Information.....	2
1.1	Revision history	2
1.2	Purpose	2
1.3	Scope.....	2
2	Protocol Binding	4
2.1	Diameter Application	5
2.2	AVPs	5
2.3	Command-Code values.....	6
3	General Error Handling	7
3.1	Result Codes	7
4	Sh interface.....	11
4.1	Overview	11
4.2	Usage Overview	11
4.3	Error Handling	12
4.4	Sh Interface Usage.....	13
5	Dh Interface	37
5.1	Overview	37
5.2	Usage Overview	37
5.3	Error Handling	38
5.4	Dh Interface Usage.....	38
6	Glossary.....	44
6.1	Abbreviations	44
7	References	46

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

1 General Information

1.1 Revision history

REVISION	RELEASE DATE	REVISED BY	REASON FOR REVISION
A	2013-04-19	ERAASJA	Approved
B	2013-05-31	EGERGMA	Minor change
C	2013-09-19	EGERGFT	<ul style="list-style-type: none">• New Pre-paging-Supported AVP and update Table 9 Data reference values used in UDR operations.• New AVP in UDR: Session-Priority
D	2014-09-16	EPTEBAR	<ul style="list-style-type: none">• The document is generalized (the body of the document is platform agnostic), should be stepped to a new main revision.
E	2014-12-03	EZOLTTH	<ul style="list-style-type: none">• Message error 5011• Supported-Features AVP
F	2015-04-29	ETXEHG	<ul style="list-style-type: none">• New AVPs: Wildcarded-Public-Identity and Wildcarded-IMPU
G	2016-08-18	ETASZAB	<ul style="list-style-type: none">• User-Name AVP is not sent in UDR for MSISDN.
H	2016-12-12	ETHTLO	<ul style="list-style-type: none">• Corrected PNR handling description.
J	2017-12-15	EGERGFT	<ul style="list-style-type: none">• Updated Table 9 with new Data Reference and Access Keys• Updated Table 9 with Access Keys used by MTAS
K	2018-04-05	ECHBHAV	<ul style="list-style-type: none">• Described CurrentLocationRetrieved information element in 4.4.1.4• Updated chapter 2 for SCTP

1.2 Purpose

This document describes the communication between the MTAS and the HSS. It also describes the communication between the MTAS and the SLF.

1.3 Scope

The communication with the HSS and the SLF uses a subset of the Sh application over the Diameter protocol as specified in [3] and [5], the details are explained in this document.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

MTAS uses the Ericsson Diameter protocol stack, provided by the underlying platform. Document [4] describes to what extent the Ericsson Diameter Base Protocol component conforms to the Diameter Base Protocol standard.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

2 Protocol Binding

Both the Sh and Dh interface described in this document are based on the Diameter protocol. The default Diameter port used is 3868. The transport used is either TCP or SCTP, both IPv4 and IPv6 can be used.

The support of the Sh and Dh interface must be announced during the Capability Exchange phase of the Diameter connection setup. The Diameter capability exchange is done according to the procedure described in section 5.6 of [1]. When there is more than one HSS in the network, the SLF acts as a re-direct agent, and the MTAS uses the SLF to determine which HSS to use for a given subscriber. See section 5

When there is only one HSS in the network, the MTAS directly contacts the HSS. See section 4

When an SLF is operating in the proxy mode, MTAS sends all Sh messages to the SLF. The messages are the same as those for the Sh interface for when there is only one HSS in the network. See section 4 and Figure 2.

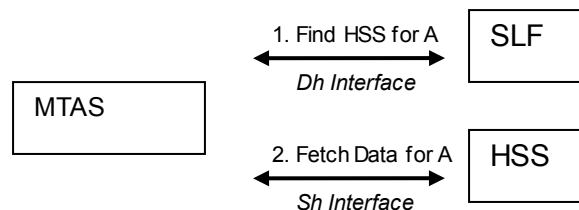


Figure 1 Usage of Sh and Dh interface

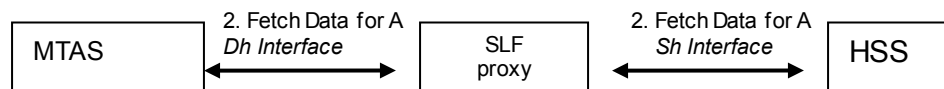


Figure 2 Usage of Sh and Dh interface SLF in proxy mode

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

2.1 Diameter Application

The Sh interface protocol is defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP (<http://www.iana.org/assignments/enterprise-numbers>) is 10415.

The Diameter application identifier assigned to the Sh interface application is 16777217 (allocated by IANA). The default Diameter port is 3868.

2.2 AVPs

The following table describes the Diameter AVPs defined for the Sh and Dh application, their AVP Code values and types. For more information about these AVP's see [5].

Attribute Name	AVP Code	Value Type
User-Identity	700	Grouped
MSISDN	701	OctetString
User-Data	702	OctetString
Data-Reference	703	Enumerated
Service-Indication	704	OctetString
Subs-Req-Type	705	Enumerated
Requested-Domain	706	Enumerated
Current-Location	707	Enumerated
Identity-Set	708	Enumerated
Supported-Features	628	Grouped
Feature-List-ID	629	Unsigned32
Feature-List	630	Unsigned32
Supported-Applications	631	Grouped
Public-Identity	601	UTF8String
Session-Priority	650	Enumerated

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Requested-Nodes	713	Unsigned32
Serving-Node-Indication	714	Enumerated
Pre-paging-Supported	717	Enumerated
Wildcarded-Public-Identity	634	UTF8String
Wildcarded-IMPU	636	UTF8String

Table 1 Diameter AVPs defined for the Sh and Dh application

2.3 Command-Code values

This section defines Command-Code values for the Dh and Sh application.

Command-Name	Abbreviation	Code
User-Data-Request	UDR	306
User-Data-Answer	UDA	306
Profile-Update-Request	PUR	307
Profile-Update-Answer	PUA	307
Subscribe-Notifications-Request	SNR	308
Subscribe-Notifications-Answer	SNA	308
Push-Notification-Request	PNR	309
Push-Notification-Answer	PNA	309

Table 2 Command-Code values for the Dh and Sh application

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

3 General Error Handling

The error codes from the Diameter Base Protocol [2] are listed under this chapter. They indicate whether a particular request was completed successfully or whether an error occurred. The error codes described in this chapter apply to both the Sh and Dh interface. Where the term server is used in this chapter it refers to either the SLF or HSS depending on context.

3.1 Result Codes

The Result-Code data field contains an IANA-managed 32-bit address space representing errors. Diameter provides the following classes of errors, all identified by the thousands digit:

- 1xxx (Informational)
- 2xxx (Success)
- 3xxx (Protocol Errors)
- 4xxx (Transient Failures)
- 5xxx (Permanent Failure)

A non-recognized class (one whose first digit is not defined in this section) **MUST** be handled as a permanent failure.

3.1.1 Informational

Errors that fall within this category are used to inform the requester that a request could not be satisfied, and additional action is required on its part before access is granted.

At this moment there are no errors that fall in this category for this application.

3.1.2 Success

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

Result condition	Result Code
Successful request	2001 DIAMETER_SUCCESS

Table 3 Result codes for success

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

3.1.3 Protocol Errors

Errors that fall within the Protocol Error category SHOULD be treated on a per-hop basis, and Diameter proxies MAY attempt to correct the error, if it is possible. Note that these and only these errors MUST only be used in answer messages whose 'E' bit is set.

Error condition	Result Code
The server received a command not included in the Sh Interface.	3001 DIAMETER_COMMAND_UNSUPPORTED
This error is given when Diameter cannot deliver the message to the destination, either because no host within the realm supporting the required application was available to process the request, or because Destination-Host AVP was given without the associated Destination-Realm AVP.	3002 DIAMETER_UNABLE_TO_DELIVER
The server sends this error when it cannot provide the requested service.	3004 DIAMETER_TOO_BUSY

Table 4 Result codes for errors

3.1.4 Transient Failures

Errors that fall within the transient failures category are used to inform a peer that the request could not be satisfied at the time it was received, but MAY be able to satisfy the request in the future.

At this moment there are no errors that fall in this category for this application.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

3.1.5 Permanent Failures

Errors that fall within the permanent failures category are used to inform the peer that the request failed, and should not be attempted again.

Error condition	Result Code
<p>The server received an authentication request with one or more mandatory AVPs, not recognized or supported.</p> <p>The Failed-AVP AVP MUST be included and contain a copy of the offending AVP.</p>	5001 DIAMETER_AVP_UNSUPPORTED
<p>The server received a request containing an AVP with an invalid value in its data portion.</p> <p>The Failed-AVP AVP MUST be included and contain a copy of the offending AVP.</p>	5004 DIAMETER_INVALID_AVP_VALUE
<p>The server received a request that does not contain an AVP that is required by the Command Code definition.</p> <p>The Failed-AVP AVP MUST be included and contain an example of the offending AVP.</p>	5005 DIAMETER_MISSING_AVP
<p>The server received a request containing AVPs that contradicted each other, and is not willing to provide service to the user.</p> <p>The Failed-AVP AVPs MUST be included, containing the AVPs that contradicted each other</p>	5007 DIAMETER_CONTRADICTING_AVPS

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

<p>The server received a request containing an AVP that MUST NOT be present.</p> <p>The Failed-AVP AVP MUST be included and contain a copy of the offending AVP.</p>	<p>5008 DIAMETER_AVP_NOT_ALLOWED</p>
<p>The server received a request containing an AVP that appeared more often than permitted in the message definition.</p> <p>The Failed-AVP AVP MUST be included and contain a copy of the first instance of the offending AVP that exceeded the maximum number of occurrences</p>	<p>5009 DIAMETER_AVP_OCCURS_TOO_MANY_TIMES</p>
<p>Any exception not covered before</p>	<p>5012 DIAMETER_UNABLE_TO_COMPLY</p>

Table 5 Result codes for permanent errors

3.1.6 Timeout

If a reply for a message is not received before a default timeout period the Diameter stack in MTAS will resend the message. The timeout and number of retries are configurable parameters in MTAS.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

4 Sh interface

4.1 Overview

The Sh application is defined as an application on the Diameter Base Protocol, see [2]. The relevant standards have been specified in 3GPP (see [3] and [5]).

The MTAS uses Sh functionality to access subscriber related information in the HSS.

Sh functionality used by MTAS:

- Access to transparent and non-transparent data for the IMS domain.
- Subscriptions to modifications of transparent data.
- Storage of transparent data for the default user.
- Update of transparent and non-transparent data

This interface has been standardized in 3GPP with the intention of providing the needed information and support for the AS's. The information that can be retrieved with this interface is related to the subscriber and refers to the state and permanent data in the IMS domain. The interface also allows updating and retrieval of transparent and non-transparent data in the HSS.

When the SLF acting as a proxy agent is utilized, the Dh interface is considered to be an Sh interface.

4.2 Usage Overview

In the table below the operations used by the MTAS are shown. The operations are further described in the following chapters.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Operation	Description
Data read (Sh-Pull)	To read transparent or non-transparent data for a specified subscriber from the HSS
Data Update (Sh-Update)	To update the transparent (repository) or non-transparent data stored at the HSS for a specified Public User Identity.
Subscription to Notifications (Sh-Subs-Notif)	To subscribe or unsubscribe to Notifications for when particular transparent or non-transparent data for a specified user is updated.
Notifications (Sh-Notif)	To inform the MTAS of changes in transparent or non-transparent data.

Table 6 Operations in Sh interface

4.3 Error Handling

4.3.1 Experimental Error Codes

The experimental error codes are included within the Experimental-Result-Code AVP in the answer messages. If the Experimental-Result-Code AVP is included in the message, then there will be no Result-Code AVP in the same message.

The experimental error codes indicate Sh specific errors and are vendor specific to MTAS

The experimental error codes supported are listed below and are defined in section 6.2 in [5].

Error condition	Experimental Result Code
The server received a request for a user not defined in its database.	5001 DIAMETER_ERROR_USER_UNKNOWN

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

The size of the data pushed to the receiving entity exceeds its capacity.	5008 DIAMETER_ERROR_TOO_MUCH_DATA
The requested operation is not allowed for the user.	5101 DIAMETER_ERROR_OPERATION_NOT_ALLOWED
The request repository data is not allowed to be read.	5102 DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ
The requested user data is not allowed to be notified on changes.	5104 DIAMETER_ERROR_USER_CANNOT_BE_NOTIFIED
The request to update the repository data at the HSS could not be completed because the requested update is based on an out-of-date version of the repository data.	5105 DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC
A request application message was received indicating that the origin host request that the command pair would be handled using a feature which is not supported by the destination host.	5011 DIAMETER_ERROR_FEATURE_UNSUPPORTED

Table 7 Experimental error codes Sh interface

4.4 Sh Interface Usage

4.4.1 Data Read (Sh-Pull)

The MTAS uses this operation in order to request subscriber related information, the transparent and non-transparent data from the HSS.

Data Read (Sh-Pull) is provided by means of the Diameter Sh Application User-Data-Request (UDR) command.

4.4.1.1 Prerequisites

Client and Server have a Diameter session established (CER/CEA messages already exchanged) and they both support the Sh Diameter Application.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

4.4.1.2 Procedure

This is the procedure for the Data Read operation.

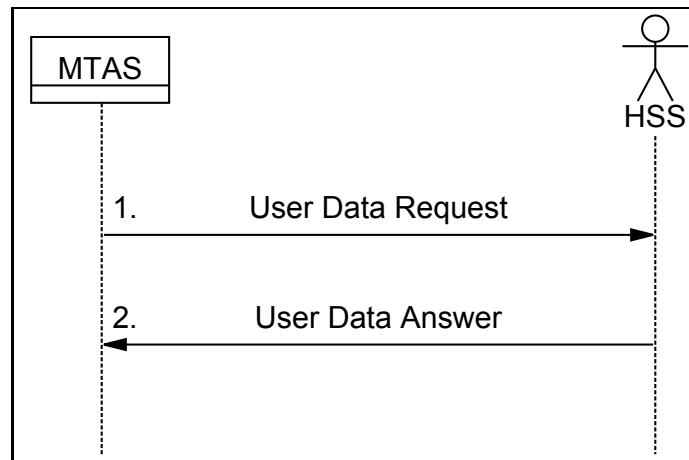


Figure 3 Procedure for Data Read operation

The description of the steps for this procedure is the following:

1. The MTAS generates a User Data Request according to the standard 3GPP format. For the supported data references and access keys, see Table 9.
2. The User Data Answer with the requested data and Result Code `DIAMETER_SUCCESS`, or an error code is returned to the MTAS.

4.4.1.3 Protocol Binding

4.4.1.3.1 User-Data-Request

The MTAS invokes UDR operation with the Command-Code field set to 306 and the 'R' bit set in the Command Flags field. The MTAS supports the AVPs in Table 8 in the User-Data-Request Diameter command. MTAS retrieves two types of data from the HSS, the repository data (Transparent data) and non-transparent data.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1 in [3])	User-Identity	M	IMS Public Identity or MSISDN of the user for whom the data is required.
Wildcarded PSI (See 7.1A in [3])	Wildcarded-Public-Identity	O	If the request refers to a Wildcarded PSI that is known to MTAS, the Wildcarded PSI will be present in this information element. If present it should be used by the HSS to identify the identity affected by the request. If this element is present it should be used by the HSS to identify the identity affected by this request.
Wildcarded Public User Identity (See 7.1B in [3])	Wildcarded-IMPU	O	If the request refers to a Wildcarded Public User Identity that is known by MTAS, the Wildcarded Public User Identity will be present in this information element. If present it should be used by the HSS to identify the identity affected by the request. If this element is present it should be used by the HSS to identify the identity affected by this request.
Requested data (See 7.3 in [3])	Data-Reference	M	This IE indicates the reference to the requested information. The set of valid data reference values are shown in Table 9.
Service Indication (See 7.4 in [3])	Service-Indication	C	IE that identifies, together with the User-Identity and Data-Reference, the set of service related transparent data that is being requested.
Application Server Identity (See 7.9 in [3])	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 user identity and Data-Reference, as key to identify the filter criteria. This element shall be present when the Data-Reference value is InitialFilterCriteria.
Requested Identity Set (See 7.11 in [3])	Identity-Set	O	If Data-Reference indicates IMSPublicIdentity, 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 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. If the User Identity is a Public Service Identity, the HSS shall return only the User Identity in the request. 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.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Private Identity (See 7.6.19 in [3])	User-Name	C	Private Identity of the user for whom the data is required. This element shall be present when fetching STN-SR by SCC AS if IMS Private Identity was available during user registration in the 3rd party registration body.
Requested domain (See 7.2 in [3])	Requested-Domain	C	This information element indicates the domain to which the operation is applicable. Check table 7.6.1 in [3] to see when it is applicable.
Current Location (See 7.8 in [3])	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 and/or MME the need to initiate an active location retrieval. Check table 7.6.1 in [3] to see when it is applicable.
Requested nodes (See 7.2A in [3])	Requested-Nodes	O	This information element indicates the Node Types to which the operation is applicable. Check table 7.6.1 in [3] to see when it is applicable.
Serving Node Indication (See 7.2B in [3])	Serving-Node-Indication	O	This information element shall indicate that only the serving node address/identity associated to the location data is required. Check table 7.6.1 in [3] to see when it is applicable.
Pre-paging Supported (See 7.18 in [3])	Pre-paging-Supported	C	This information element indicates whether Pre-paging is supported by the AS.
Session priority (See 7.15 in [3])	Session-Priority	O	This information element indicates the session's priority level to the HSS. If it is not included, the request shall be treated as normal.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Supported-Features (See 6.1.1 in [5])	Supported-Features	C	<p>If this AVP is present it may inform the destination host about the features that the origin host supports. The Feature-List AVP contains a list of supported features of the origin host. The Vendor-Id AVP and the Feature-List AVP shall together identify which feature list is carried in the Supported-Features AVP.</p> <p>Where a Supported-Features AVP is used to identify features that have been defined by 3GPP, the Vendor-Id AVP shall contain the vendor ID of 3GPP. Vendors may define proprietary features, but it is strongly recommended that the possibility is used only as the last resort. Where the Supported-Features AVP is used to identify features that have been defined by a vendor other than 3GPP, it shall contain the vendor ID of the specific vendor in question.</p> <p>If there are multiple feature lists defined by the same vendor, the Feature-List-ID AVP shall differentiate those lists from one another. The destination host shall use the value of the Feature-List-ID AVP to identify the feature list.</p>
--	--------------------	---	---

Table 8 AVPs for UDR operation

Table 9 details the data reference values and the associated access keys that are used to retrieve data for the user from the HSS. For the data references supported by the HSS, see 7.6 of [3].

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Data reference value	XML tag	Access key
0	RepositoryData	IMS Public User Identity or Public Service Identity + Data-Reference + Service-Indication
10	IMSPublicIdentity	(IMS Public User Identity OR MSISDN) + Data-Reference + Identity-Set = IMPLICIT_IDENTITIES
12	SCSCFName	IMS Public User Identity + Data-Reference
16	ChargingInformation	IMS Public User Identity + Data-Reference
17	MSISDN	IMS Public User Identity + [Private Identity] + Data-Reference
26	TADSInformation	MSISDN OR (IMS Public User Identity + Private Identity) + Data-Reference
27	STN-SR	IMS Public User Identity + Private Identity + Data-Reference
14	LocationInformation	MSISDN + Data-Reference + Requested-Domain + Current-Location + [Requested-Nodes] + [Serving-Node-Indication]
30	CSRN	MSISDN OR (IMS Public User Identity + Private Identity) + Data-Reference + Pre-paging-Supported
32	IMSI	IMS Public User Identity + Private Identity + Data-Reference

Table 9 Data reference values used in UDR operations

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Message Format:

```

< User-Data-Request >::= < Diameter Header: 306, REQ, PXY, 16777217 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    [ Destination-Host ]
    { User-Identity }
    [Wildcarded-Public-Identity]
    [Wildcarded-IMPU]
    [ Supported-Features ]
    *[ Service-Indication ]
    { Data-Reference }
    [ Identity-Set ]
    [ Requested-Domain ]
    [ Current-Location ]
    [ User-Name ]
    [ Requested-Nodes ]
    [ Serving-Node-Indication ]
    [ Pre-paging-Supported ]
    [ Session-Priority ]
    *[ AVP ]
    *[ Proxy-Info ]
    *[ Route-Record ]

```

4.4.1.3.2 User-Data-Answer

The HSS replies with the UDA Diameter command with Command-Code field set to 306 and the 'R' bit cleared in the Command Flags field.

The HSS will send the following parameters in the User-Data-Answer Diameter command:

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 3.1)	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(as specified in section 1.4) in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Wildcarded PSI (See 7.1A in [3])	Wildcarded-Public-Identity	O	If the request refers to a specific PSI matching a Wildcarded PSI and the Wildcarded-Public-Identity AVP was not included in the request and is not included in the User-Data AVP, the HSS must include the corresponding Wildcarded PSI in this information element.
Wildcarded Public User Identity (See 7.1B in [3])	Wildcarded-IMPU	O	If the request refers to a specific Public User Identity matching a Wildcarded Public User Identity and the Wildcarded-IMPU AVP was not included in the request and is not included in the User-Data AVP, the HSS must include the corresponding Wildcarded Public User Identity in this information element.
Data (See 7.6 in [3])	User-Data	O	Requested data.

Table 10 Parameters for UDA operation

Message Format:

```

< User-Data-Answer > ::= < Diameter Header: 306, PXY, 16777217 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    *[ Supported-Features ]
    [ Wildcarded-Public-Identity ]
    [ Wildcarded-IMPU ]
    [ Result-Code ]
    [ User-Data ]
    [ Experimental-Result ]
    *[ AVP ]
    *[ Failed-AVP ]
    *[ Proxy-Info ]
    *[ Route-Record ]

```

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

4.4.1.4 Results

If the request cannot be performed, the HSS will indicate one of the errors defined in section 3 or section 4.3

The MTAS will handle any return code except success (2xxx) as a failure to read the requested subscriber data.

The CurrentLocationRetrieved information element will be present when location information was obtained after a successful paging procedure for Active Location Retrieval.

4.4.2 Data Update (Sh-Update)

The MTAS uses this service operation in order to update the transparent repository data associated with a Public User Identity in the HSS.

Data Update (Sh-Update) is provided by means of the Diameter Sh Application Profile-Update-Request (PUR) command.

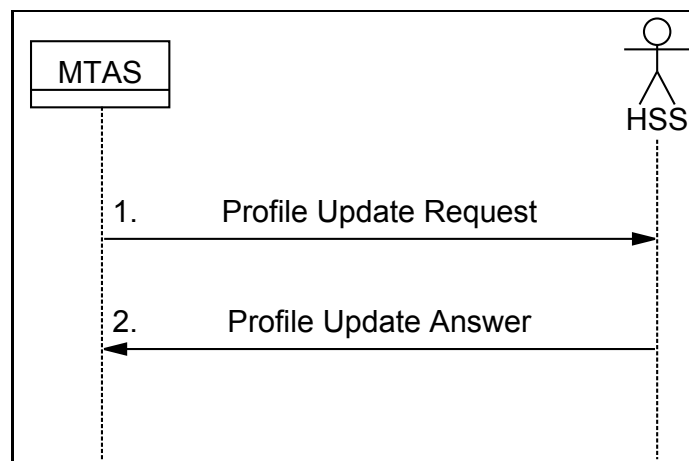
The SCC AS uses this service operation in order to update the non-transparent user data associated with STN-SR in the HSS.

4.4.2.1 Prerequisites

Client and Server have a Diameter session established (CER/CEA messages already exchanged) and they both support the Sh Diameter Application.

4.4.2.2 Procedure

This is the procedure for the Data Update operation



Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Figure 4 Procedure for Data Update operation

The description of the steps for this procedure is the following:

1. The MTAS generates a Profile Update Request according to the standard 3GPP format.
2. The Profile Update Answer with Result Code DIAMETER_SUCCESS or an error code is returned to the MTAS.

4.4.2.3 Protocol Binding

4.4.2.3.1 Profile-Update-Request

The MTAS invokes PUR operation with the Command-Code field set to 307 and the 'R' bit set in the Command Flags field. The following parameters will be set in the Profile-Update-Request Diameter command:

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1 in [3])	User-Identity	M	IMS public identity of the user which data is updated.
Data (See 7.6 in [3])	User-Data	M	Updated data.
Wildcarded PSI (See 7.1A in [3])	Wildcarded-Public-Identity	O	If the request refers to a Wildcarded PSI that is known by MTAS, this Wildcarded PSI will be included in this information element. If this element is present it should be used by the HSS to identify the identity affected by this request.
Wildcarded Public User Identity (See 7.1B in [3])	Wildcarded-IMPU	O	If the request refers to a Wildcarded Public User Identity that is known by MTAS, this Wildcarded Public User Identity will be included in this information element. If this element is present it should be used by the HSS to identify the identity affected by this request.
Application Server Identity (See 7.9 in [3])	Origin-Host	M	IE that identifies the AS originator of the request and that is used to check the AS permission list.
Requested data (See 7.3 in [3])	Data-Reference	M	This IE indicates the reference to the requested information. The set of valid data reference values are shown in Table 12.
Private Identity (See 7.6.19 in [3])	User-Name	C	Private Identity of the user for whom the data is required. This element shall be present when updating STN-SR by SCC AS if IMS Private Identity was available during user registration in the 3 rd party registration body.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Supported-Features (See 6.1.1 in [5])	Supported-Features	C	<p>If this AVP is present it may inform the destination host about the features that the origin host supports. The Feature-List AVP contains a list of supported features of the origin host. The Vendor-Id AVP and the Feature-List AVP shall together identify which feature list is carried in the Supported-Features AVP.</p> <p>Where a Supported-Features AVP is used to identify features that have been defined by 3GPP, the Vendor-Id AVP shall contain the vendor ID of 3GPP. Vendors may define proprietary features, but it is strongly recommended that the possibility is used only as the last resort. Where the Supported-Features AVP is used to identify features that have been defined by a vendor other than 3GPP, it shall contain the vendor ID of the specific vendor in question.</p> <p>If there are multiple feature lists defined by the same vendor, the Feature-List-ID AVP shall differentiate those lists from one another. The destination host shall use the value of the Feature-List-ID AVP to identify the feature list.</p>
--	--------------------	---	---

Table 11 Parameters for PUR operation

Table 12 details the data reference values and the associated access keys that are used to update data for the user in the HSS. They are all fully defined in 7.6 of [3].

Data reference value	XML tag	Access key
0	RepositoryData	IMS Public User Identity or Public Service Identity + Data-Reference + Service-Indication
27	STN-SR	IMS Public User Identity + [Private Identity] + Data-Reference

Table 12 Data reference values used in PUR operations

Message Format:

```
< Profile-Update-Request > ::= < Diameter Header: 307, REQ, PXY, 16777217 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
```


Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

{ Destination-Realm }
[Destination-Host]
{ User-Identity }
[Wildcarded-Public-Identity]
[Wildcarded-IMPU]
[User-Name]
[Supported-Features]
{ Data-Reference }
{ User-Data }
*[AVP]
*[Proxy-Info]
*[Route-Record]

4.4.2.3.2 Profile-Update-Answer

The HSS replies with the PUA Diameter command with Command-Code field set to 307 and the 'R' bit cleared in the Command Flags field.

The HSS will set the following parameters in the Profile-Update-Answer Diameter command:

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7. 5 in [3])	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.
Wildcarded PSI (See 7. 1A in [3])	Wildcarded -Public-Identity	O	If the request refers to a specific PSI matching a Wildcarded PSI and the Wildcarded-Public-Identity AVP was not included in the request, the HSS must include the corresponding Wildcarded PSI in this information element. This information will be used by the AS to identify the affected Wildcarded PSI.
Wildcarded Public User Identity (See 7. 1B in [3])	Wildcarded -IMPU	O	If the request refers to a specific Public User Identity matching a Wildcarded Public User Identity and the Wildcarded-IMPU AVP was not included in the request, the HSS must include the corresponding Wildcarded Public User Identity in this information element. This information will be used by the AS to identify the affected Wildcarded Public User Identity.

Table 13 Parameters for PUA command

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Message Format:

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

4.4.2.4 Results

If the request cannot be performed, the HSS will indicate one of the errors defined in section 3 or section 4.3.

The MTAS will handle any return code except DIAMETER_SUCCESS (2001) as a failure to update the requested subscriber data.

4.4.3 Subscription to Notifications (Sh-Subs-Notif)

The MTAS uses this operation in order to subscribe or to unsubscribe to notifications, for when a particular data associated with a Public User Identity is updated in the HSS.

Subscription to Notifications (Sh-Subs-Notif) is provided by means of the Diameter Sh Application Subscribe-Notifications-Request (SNR) command.

4.4.3.1 Prerequisites

Client and Server have a Diameter session established (CER/CEA messages already exchanged) and they both support the Sh Diameter Application.

4.4.3.2 Procedure

This is the procedure for the Subscription to Notifications operation.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

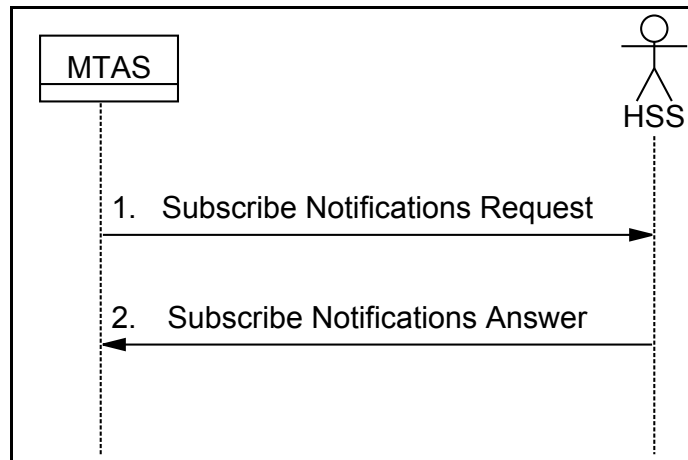


Figure 5 Procedure for Subscriptions to Notifications operation

The description of the steps for this procedure is the following:

1. The MTAS generates a Subscribe Notifications Request according to the standard 3GPP format.
2. The Subscribe Notifications Answer with Result Code DIAMETER_SUCCESS or an error code is returned to MTAS.

4.4.3.3 Protocol Binding

4.4.3.3.1 Subscribe-Notifications-Request

The client invokes SNR operation with the Command-Code field set to 308 and the 'R' bit set in the Command Flags field. The following parameters will be set in the Subscribe-Notification-Request Diameter command:

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1 in [3])	User-Identity	M	IMS public identity of the user for whom notifications of data changes are requested.
Wildcarded PSI (See 7.1A in [3])	Wildcarded-Public-Identity	O	If the request refers to a Wildcarded PSI that is known by MTAS, the Wildcarded PSI will be included in this information element. If this element is present, it should be used by the HSS to identify the identity affected by the request.
Wildcarded Public User Identity (See 7.1 B in [3])	Wildcarded-IMPU	O	If the request refers to a Wildcarded Public User Identity that is known by MTAS, the Wildcarded Public User Identity will be included in this information element. If this element is present, it should be used by HSS to identify the identity affected by the request.
Requested data (See 7.3 in [3])	Data-Reference	M	This information element includes the reference to the data on which notifications of change are required.
Subscription request type (See 7.7 In [3])	Subs-Req-Type	M	This information element indicates the action requested on subscription to notifications.
Service Indication (See 7.4 in [3])	Service-Indication	O	IE that identifies, together with the User-Identity and Data-Reference, the set of service related transparent data for which notifications of changes are requested..
Application Server Identity (See 7.9 in [3])	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 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).

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Supported-Features (See 6.1.1 in [5])	Supported-Features	C	<p>If this AVP is present it may inform the destination host about the features that the origin host supports. The Feature-List AVP contains a list of supported features of the origin host. The Vendor-Id AVP and the Feature-List AVP shall together identify which feature list is carried in the Supported-Features AVP.</p> <p>Where a Supported-Features AVP is used to identify features that have been defined by 3GPP, the Vendor-Id AVP shall contain the vendor ID of 3GPP. Vendors may define proprietary features, but it is strongly recommended that the possibility is used only as the last resort. Where the Supported-Features AVP is used to identify features that have been defined by a vendor other than 3GPP, it shall contain the vendor ID of the specific vendor in question.</p> <p>If there are multiple feature lists defined by the same vendor, the Feature-List-ID AVP shall differentiate those lists from one another. The destination host shall use the value of the Feature-List-ID AVP to identify the feature list.</p>
--	--------------------	---	---

Table 14 Parameters for SNR operation

Message Format:

< Subscribe-Notifications-Request > ::= < Diameter Header: 308, REQ, PXY, 16777217 >

< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
[Destination-Host]
{ User-Identity }
[Wildcarded-Public-Identity]
[Wildcarded-IMPU]
[Supported-Features]
[Service-Indication]
[Service-Name]
{ Subs-Req-Type }
{ Data-Reference }
*[AVP]
*[Proxy-Info]
*[Route-Record]

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

4.4.3.3.2 Subscribe-Notifications-Answer

The HSS replies with the SNA Diameter command with Command-Code field set to 308 and the 'R' bit cleared in the Command Flags field.

The HSS will indicate the following parameters in the Subscribe-Notifications-Answer Diameter command:

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7. 5 in [3])	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.
Wildcarded PSI (See 7. 1A in [3])	Wildcarded -Public-Identity	O	If the request refers to a specific PSI matching a Wildcarded Public User Identity and the Wildcarded-Public User Identity AVP was not included in the request, the HSS must include the corresponding Wildcarded PSI in this information element. This information will be used by the AS to identify the affected Wildcarded PSI.
Wildcarded PSI (See 7. 1B in [3])	Wildcarded -IMPU	O	If the request refers to a specific Public User Identity matching a Wildcarded Public User Identity and the Wildcarded-IMPU AVP was not included in the request, the HSS may include the corresponding Wildcarded Public User Identity in this information element. This information may be used by the AS to identify the affected Wildcarded Public User Identity.

Table 15 Parameters for SNA command

Message Format:

```
<Subscribe-Notifications-Answer>::= < Diameter Header: 308, PXY, 16777217 >  
    < Session-Id >  
    { Vendor-Specific-Application-Id }  
    { Auth-Session-State }  
    { Origin-Host }  
    { Origin-Realm }  
    [Wildcarded-Public-Identity]  
    [Wildcarded-IMPU]  
    [ Result-Code ]
```

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

[Experimental-Result]
 *[Supported-Features]
 *[AVP]
 *[Failed-AVP]
 *[Proxy-Info]
 *[Route-Record]

4.4.3.4 Results

If the request cannot be performed, the HSS will indicate one of the errors defined in section 3 or section 4.3.

The MTAS will handle any return code except success (2xxx) as a failure to subscribe the requested subscriber data.

4.4.4 Notifications (Sh-Notif)

The HSS uses this service operation in order to inform the MTAS of changes in data associated with a Public User Identity.

Notifications (Sh- Notif) is provided by means of the Diameter Sh Application Push-Notification-Request (PNR) command.

4.4.4.1 Prerequisites

Client and Server have a Diameter session established (CER/CEA messages already exchanged) and they both support the Sh Diameter Application.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

4.4.4.2 Procedure

This is the procedure for the push notification operation.

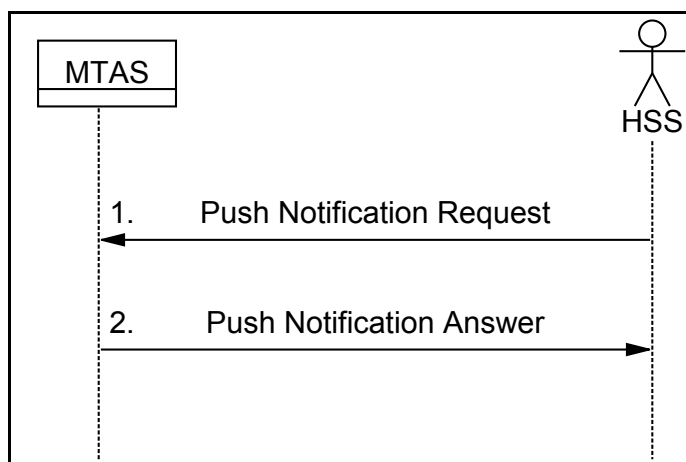


Figure 6 Procedure for Notifications operation

The description of the steps for this procedure is the following:

1. The HSS generates a Push-Notification-Request according to the standard 3GPP format. This message will be sent to the MTAS when the data has been updated by another entity and the MTAS has subscribed to data change notifications previously.

Note 1: MTAS uses two different diameter stacks towards the HSS in relation to the user data handling: “MTAS_SH” and “MTASXDMS”. Unique Origin-Host addresses are configured for the different stacks and the HSS can use the Origin-Host AVP to identify the individual entities. The “MTASXDMS” stack serves for provisioning purposes and it is not used to subscribe to data change notifications. The “MTAS_SH” diameter stack serves for traffic handling and it is used to subscribe to notifications of the user data changes.

Note 2: If the user data has been changed by the “MTAS_SH” entity – for example, due to a Supplementary Service Code activity – then no PNR will be sent since the actor entity is never notified. If the user data has been changed by the “MTASXDMS” entity of a node then the “MTAS_SH” entity of the same node will receive a PNR if the MTAS has subscribed to data change notifications.

2. On reception of the request, the MTAS updates the internal user cache with the new data content. The MTAS responds with a success answer if the cache update was successful, and with an error code otherwise.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

4.4.4.3 Protocol Binding

4.4.4.3.1 Push-Notification-Request

The HSS invokes PNR operation with the Command-Code field set to 309 and the 'R' bit set in the Command Flags field. The MTAS will receive the following parameters in the Push-Notification-Request Diameter command:

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1 in [3])	User-Identity	M	IMS public identity of the user which data has changed.
Wildcarded PSI (See 7.1A in [3])	Wildcarded-Public-Identity	O	If the request refers to a Wildcarded PSI, the Wildcarded PSI must be included in this information element. If this element is present, MTAS will use it to identify the identity affected by the request.
Wildcarded Public User Identity (See 7.1 B in [3])	Wildcarded-IMPU	O	If the request refers to a Wildcarded Public User Identity the Wildcarded Public User Identity must be included in this information element. If this element is present MTAS will use it to identify the identity affected by the request.
Requested Data (See 7.6 in [3])	User-Data	M	Changed data.
Supported-Features (See 6.1.1 in [5])	Supported-Features	C	If this AVP is present it may inform the destination host about the features that the origin host supports. The Feature-List AVP contains a list of supported features of the origin host. The Vendor-Id AVP and the Feature-List AVP shall together identify which feature list is carried in the Supported-Features AVP. Where a Supported-Features AVP is used to identify features that have been defined by 3GPP, the Vendor-Id AVP shall contain the vendor ID of 3GPP. Vendors may define proprietary features, but it is strongly recommended that the possibility is used only as the last resort. Where the Supported-Features AVP is used to identify features that have been defined by a vendor other than 3GPP, it shall contain the vendor ID of the specific vendor in question. If there are multiple feature lists defined by the same vendor, the Feature-List-ID AVP shall differentiate those lists from one another. The destination host shall use the value of the Feature-List-ID AVP to identify the feature list.

Table 16 Parameters for PNR operation

Message Format:

```
< Push-Notification-Request > ::= < Diameter Header: 309, REQ, PXY, 16777217 >
```

```
< Session-Id >
{ Vendor-Specific-Application-Id }
```

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
[Destination-Host]
{ User-Identity }
[Wildcarded-Public-Identity]
[Wildcarded-IMPU]
[Supported-Features]
{ User-Data }
*[AVP]
*[Proxy-Info]
*[Route-Record]

4.4.4.3.2 Push-Notification-Answer

The MTAS replies with the PNA Diameter command with Command-Code field set to 309 and the 'R' bit cleared in the Command Flags field.

The MTAS will set the following parameters in the Push-Notification-Answer Diameter command:

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.5 in [3])	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.

Table 17 Parameters in PNA command

Message Format:

```
< Push-Data-Answer > ::= < Diameter Header: 309, PXY, 16777217 >  
    < Session-Id >  
    { Vendor-Specific-Application-Id }  
    { Auth-Session-State }  
    { Origin-Host }  
    { Origin-Realm }  
    [ Result-Code ]  
    [ Experimental-Result ]
```

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

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

4.4.4.4 Results

If the MTAS detects an error at the protocol level, one of the errors in section 3.1 is sent. If MTAS fails to process the notification at the application level the MTAS sends error code DIAMETER_UNABLE_TO_COMPLY (5012)

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

5 Dh Interface

5.1 Overview

The MTAS uses the SLF to know which server a request should be sent to when there are several suitable HSSs deployed in the network. Based on configuration and provisioning information the name or address of the suitable target server is returned. If no suitable target server could be found an appropriate error response is returned.

Dh interface uses the Sh interface, defined as an application on the Diameter base protocol.

Sh functionalities are defined as an application on the Diameter Base Protocol to [2]. The relevant standards have been specified in 3GPP (see [5]).

5.2 Usage Overview

The table below shows the Service Operations that are used by the MTAS. The operations are further described in the following chapters.

Operation	Description
RedirectRequest()	This operation is used to redirect a request.

Table 18 Operations in Dh interface

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

5.3 Error Handling

5.3.1 Protocol Errors

The requests to the SLF using the Dh interface are the same as the requests to the HSS for the Sh interface. The difference is that a successful Dh request will result in the `DIAMETER_REDIRECT_INDICATION` answer which contain the address of the HSS to use for the corresponding request. Although this is an error message it indicates that the SLF successfully found a redirection host for the user specified in the request.

Successful Case	Result Code
The operation was performed correctly. The server name to which the request must be routed is returned to MTAS.	3006 <code>DIAMETER_REDIRECT_INDICATION</code>

Table 19 Protocol errors in Dh interface

5.4 Dh Interface Usage

5.4.1 RedirectRequest

The goal of the RedirectRequest operation is to obtain the destination server name corresponding to the request issued by MTAS.

5.4.1.1 Procedure

This is the procedure for the RedirectRequest operation.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

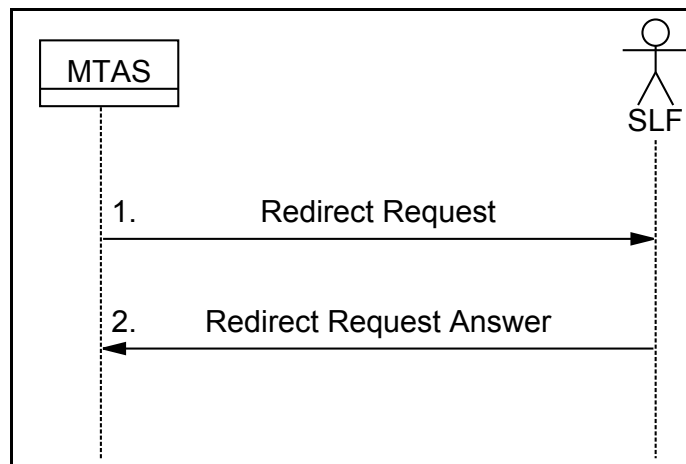


Figure 7 Procedure for RedirectRequest operation

The description of the steps for this procedure is the following:

1. MTAS sends a RedirectRequest to the SLF.
2. The SLF responds with RedirectRequest answer with result code DIAMETER_REDIRECT_INDICATION or an error code.

5.4.1.2 Protocol Binding

“RedirectRequest” and “RedirectRequest answer” can be one of the following (below each request row in the table there is its corresponding answer row):

Command-Name	Abbreviation	Code	Direction
User-Data-Request	UDR	306	AS->SLF
User-Data-Answer	UDA	306	SLF->AS
Profile-Update-Request	PUR	307	AS->SLF
Profile-Update-Answer	PUA	307	SLF->AS
Subscribe-Notify-Request	SNR	308	AS->SLF
Subscribe-Notify-Answer	SNA	308	SLF->AS

Table 20 Protocol binding of Dh interface

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

5.4.1.2.1 Pre-requisites

MTAS and the SLF hold an established Diameter session, i.e. a transport connection exists and a CER/CEA exchange has been performed between them. The SLF must have included the ApplicationId corresponding to the Sh/Dh application (16777217) in the CEA response to the MTAS.

The SLF is configured to act as a redirector for the requested operation.

The SLF's routing database has been provisioned with the key values that the requests received from MTAS include.

5.4.1.2.2 User-Data-Request (UDR)

The MTAS invokes UDR operation specified in the Dh interface. The SLF receives the following parameters in the User-Data-Request Diameter command. Only those AVPs used by the SLF routing service logic are shown in the table:

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 6.3 in [5])	User-Identity	M	IMS Public Identity or MSISDN of the user for whom the data is required.

Table 21 Parameters in UDR operation

For a description of the format of the UDR see section 4.4.1.3.1.

5.4.1.2.3 User-Data-Answer (UDA)

The SLF replies with the UDA Diameter command with Command-Code field set to 306 and the 'E' bit set in the Command Flags field.

The SLF will set the following parameters in the User-Data-Answer Diameter command:

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code	O	Result of the request. Result-Code to DIAMETER_REDIRECT_INDICATION is set when the request has been successfully performed.
Result	Experimental-Result	O	Experimental-Result AVP is used for service-specific errors.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Information element name	Mapping to Diameter AVP	Cat.	Description
Server-Name	Redirect-Host	C ¹	Server name of the server selected by the service to handle the request.
Redirect-Host-Usage	Redirect-Host-Usage	C ¹	Value must be set to All-user
Redirect-Max-Cache-Time	Redirect-Max-Cache-Time	C ¹	The value of the Redirect-Max-Cache-Time is ignored because the SLF can return the value 0 even though it is acceptable for the redirection details to be cached at least for the duration of this transaction

Table 22 Parameters in UDA command

Message format:

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

5.4.1.2.4 Profile-Update-Request (PUR)

MTAS invokes PUR specified in the Dh interface. The SLF receives the following parameters in the Profile-Update-Request Diameter command. Only those AVPs used by the SLF routing service logic are shown in the table:

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 6.3 in [5])	User-Identity	M	IMS public identity of the user which data is updated.

Table 23 Parameters in PUR operation

For a description of the format of the PUR see section 4.4.2.3.1.

¹ Must be present if Result-Code is present and takes the value DIAMETER_REDIRECT_INDICATION.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

5.4.1.2.5 Profile-Update-Answer (PUA)

The SLF replies with the PUA Diameter command with Command-Code field set to 307 and the 'E' bit set in the Command Flags field.

The SLF will set the following parameters in the Profile-Update-Answer Diameter command:

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code	M	Result of the request. Result-Code to DIAMETER_REDIRECT_INDICATION is set when the request has been successfully performed.
Result	Experimental-Result	O	Experimental-Result AVP is used for service-specific errors.
Server-Name	Redirect-Host	C ²	Server name of the server selected by the service to handle the request.
Redirect-Host-Usage	Redirect-Host-Usage	C ²	Value must be set to All-user
Redirect-Max-Cache-Time	Redirect-Max-Cache-Time	C ²	Value must be set to 0

Table 24 Parameters in PUA command

Message format:

```
< Profile-Update-Answer > ::= < Diameter Header: 307, 16777217, PXY, E >  
    < Session-Id >  
    { Vendor-Specific-Application-Id }  
    { Origin-Host }  
    { Origin-Realm }  
    { Auth-Session-State }  
    [ Result-Code ]  
    [ Experimental-Result ]  
    *{ Redirect-Host }  
    { Redirect-Host-Usage }  
    { Redirect-Max-Cache-Time }
```

² Must be present if Result-Code is present and takes the value DIAMETER_REDIRECT_INDICATION.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

5.4.1.2.6 Subscribe-Notifications-Request (SNR)

The MTAS invokes the SNR operation specified in the Dh interface. The SLF receives the following parameters in the Subscribe-Notification-Request Diameter command. Only those AVPs used by the SLF routing service logic are shown in the table:

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 6.3 in [5])	User-Identity	M	IMS public identity of the user for whom notifications of data changes are requested.

Table 25 Parameters in SNR operation

For a description of the format of the SNR see section 4.4.3.3.1.

5.4.1.2.7 Subscribe-Notifications-Answer (SNA)

The SLF replies with the SNA Diameter command with the Command-Code field set to 308 and the 'E' bit set in the Command Flags field.

The SLF will set the following parameters in the Subscribe-Notifications-Answer Diameter command. Only those AVPs used by the SLF routing service logic are shown in the table:

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code	M	Result of the request. Result-Code to DIAMETER_REDIRECT_INDICATION is set when the request has been successfully performed.
Result	Experimental-Result	O	Experimental-Result AVP is used for service-specific errors.
Server-Name	Redirect-Host	C ³	Server name of the server selected by the service to handle the request.
Redirect-Host-Usage	Redirect-Host-Usage	C ³	Value must be set to All-user
Redirect-Max-Cache-Time	Redirect-Max-Cache-Time	C ³	Value must be set to 0

Table 26 Parameters in SNR command

³ Must be present if Result-Code is present and takes the value DIAMETER_REDIRECT_INDICATION.

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

Message format:

```
<Subscribe-Notifications-Answer>::=<Diameter Header: 308,6777217, PXY, E >  
    < Session-Id >  
    { Vendor-Specific-Application-Id }  
    { Origin-Host }  
    { Origin-Realm }  
    { Auth-Session-State }  
    [ Result-Code ]  
    [Experimental-Result ]  
    *{ Redirect-Host }  
    { Redirect-Host-Usage }  
    { Redirect-Max-Cache-Time }
```

6 Glossary

6.1 Abbreviations

Abbreviation	Description
3GPP	3 rd Generation Partnership Project
ABNF	Augmented Backus-Naur Form
AS	Application Server
AVP	Attribute-Value Pair
CSRN	CS domain Routing Number
HSS	Home Subscriber Server
IETF	Internet Engineering Task Force
IM	IP Multimedia
IMS	IM Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPMM	IP Multimedia
IRS	Implicit Register Set

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

ISDN	Integrated Services Digital Network
MSISDN	Mobile Subscriber ISDN Number
PNA	Push-Notification-Answer
PNR	Push-Notification-Request
PUA	Profile-Update-Answer
PUR	Profile-Update-Request
RFC	Request For Comment
SCTP	Stream Control Transmission Protocol
SLF	Service Locator Function
SNA	Subscribe-Notifications-Answer
SNR	Subscribe-Notifications-Request
STN-SR	Session Transfer Number for SRVCC
T-ADS	Terminating Access Domain Selection
TCP	Transmission Control Protocol
UDA	User-Data-Answer
UDR	User-Data-Request
XML	Extensible Markup Language

Prepared (also subject responsible if other) ETASZAB Tamás Szabad		No. 9/155 19-AVA 901 18 Uen		
Approved BDGSEACC [Tamás Szabad]	Checked	Date 2018-04-05	Rev K	Reference

7 References

- [1] 3GPP TS 29.229 v6.7.0 Cx and Dx interfaces based on the Diameter protocol
- [2] RFC3588 Diameter Base Protocol
- [3] 3GPP TS 29.328 v10.3.0 and v12.14.0
IM Subsystem Sh interface; Signalling flows and message contents
- [4] TSP: 1/174 02-CRA 119 0019/2 Diameter Base Protocol, Statement of Compliance
CBA: 1/174 02-CXP 904 0375 Diameter Base Protocol, Statement of Compliance 1/174 02-CXP 904 0375
- [5] 3GPP TS 29.329 v10.4.0 Sh/Dh interface based on the Diameter protocol