ETSI TS 129 330 V18.0.0 (2024-05)

5G;
IP Multimedia Subsystem (IMS);
Sc Interface based on the Diameter protocol;
(3GPP TS 29.330 version 18.0.0 Release 18)

Reference
RTS/TSGC-0429330vi00

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document describes the diameter-based Sc interface between Data Channel Signalling Function (DCSF) and Home Subscriber Server (HSS) and specifies:

1. The interactions between the Data Channel Signalling Function (DCSF) and Home Subscriber Server (HSS) at the Sc reference point, including the procedures and signalling flows.
2. The protocol specifications and implementations, including the diameter application, commands and message contents at the Sc reference point.

The IP Multimedia Subsystem (IMS) supporting DC architecture and procedures are specified in 3GPP TS 23.228 [2].

Whenever it is possible this document specifies the requirements for this protocol by reference to specifications produced by the IETF within the scope of Diameter base protocol as specified in IETF RFC 6733 [3]. Where this is not possible, extensions to the Diameter base protocol as specified in IETF RFC 6733 [3] are defined within this document.

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 TR 21.905: "Vocabulary for 3GPP Specifications".

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

[3] IETF RFC 6733: "Diameter Base Protocol".

[4] 3GPP TS 29.328: "IP Multimedia (IM) Subsystem Sh interface; signalling flows and message contents".

[5] IETF RFC 4960: "Stream Control Transmission Protocol".

[6] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol; protocol details".

[7] 3GPP TS 29.336: "Home Subscriber Server (HSS) diameter interfaces for interworking with packet data networks and applications".

[8] IETF RFC 7683: "Diameter Overload Indication Conveyance".

[9] IETF RFC 7944: "Diameter Routing Message Priority".

[10] 3GPP TS 22.153: "Multimedia Priority Service".

[11] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP" – stage 3.

[12] 3GPP TS 29.329: "Sh Interface based on the Diameter protocol; Protocol details".

[13] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[14] IETF RFC 8583: "Diameter Load Information Conveyance".

[15] 3GPP TS 29.364: "IMS Application Server Service Data Descriptions for AS interoperability".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Definition format (Normal)

<defined term>: *<definition>.*

example: text used to clarify abstract rules by applying them literally.

3.2 Symbols

For the purposes of the present document, the following symbols given in 3GPP TS 23.228 [2] apply:

Sc Reference Point between an DCSF and an HSS.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

DC Data Channel
DCSF Data Channel Signalling Function
IMS IP Multimedia Core Network Subsystem

4 General Description

This document describes the Sc interface related procedures, message parameters and protocol specifications.

The procedures, message parameters and protocol are identical as for the Sc. See clause 5 for details.

In the tables that describe the Information Elements transported by each Diameter command, each Information Element is marked as (M) Mandatory, (C) Conditional or (O) Optional in the "Cat." column. For the correct handling of the Information Element according to the category type, see the description detailed in clause 6 of the 3GPP TS 29.328 [4].

5 Diameter-based Sc Interface

5.1 Introduction

The Sc interface shall enable the Data Read and Data Update procedure between the DCSF and the HSS as described in the 3GPP TS 23.228 [2].

5.2 Procedure Descriptions

5.2.1 Data Read (Sc-Pull)

5.2.1.1 General

The Data Read Procedure shall be used between the DCSF and the HSS to read repository data for a specified user from the HSS. The procedure shall be invoked by the DCSF and is used:

- to read the transparent data for a specified user from the HSS, and the data is store by DCSF in the HSS to support its service logic.

This procedure is mapped to the commands User-Data-Request/Answer (UDR/UDA) in the Diameter application specified in clause 6.2.3 and clause 6.2.4.

Table 5.2.1-1 specifies the involved information elements for the request.

Table 5.2.1-2 specifies the involved information elements for the answer.

Table 5.2.1-1: Sc-Pull

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 3GPP TS 29.328 [4])	User-Identity	M	It shall contain the IMS Public User Identity (in the Public-Identity AVP) of the user for whom the data is required.
Requested data (See 3GPP TS 29.328 [4])	Data-Reference	M	This information element indicates the reference to the requested information.
Service Indication (See 3GPP TS 29.328 [4])	Service-Indication	M	IE that identifies, together with the Public User Identity included in the Public-Identity AVP and Data-Reference, the set of service related transparent data that is being requested.

Table 5.2.1-2: Sc-Pull Resp

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental_Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [3]). Experimental-Result AVP shall be used for Sc 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	User-Data	C	Requested data. This information element shall be present if the requested data exists in the HSS and the DCSF has permissions to read it.

5.2.1.2 Detailed behaviour

The DCSF shall invoke the data read procedure by sending the Sc-Pull request to HSS to read repository data for a specified user from the HSS. If repository data is requested, Service-Indication shall be present in the request.

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

1. In the DCSF permission list as specified in clause 6.1.7 check that the requested user data is allowed to be read (Sc-Pull) by this DCSF by checking the combination of the identity of the DCSF sending the request (identified by the Origin-Host AVP) and the supplied Data-Reference.

- If one or more Data References in the request are not allowed to be read, Experimental-Result shall be set to DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ in the Sc-Pull Response.

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

3. If the type of the User Identity (IMS Public User Identity) does not apply according to Table 6.3.4 as access key for the Data-Reference indicated in the request, Experimental-Result shall be set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED in the Sh-Pull Response.

4. Check whether or not the data that is requested to be downloaded by the DCSF is currently being updated by another entity. If there is an update of the data in progress, the HSS may delay the Sc-Pull-Resp message until the update has been completed. The HSS shall ensure that the data returned is not corrupted by this conflict. If HSS is not able to delay the Sc-Pull-Resp message e.g. due to timeout the Experimental-Result-Code shall be set to DIAMETER_PRIOR_UPDATE_IN_PROGRESS.

5. The HSS shall include the data pertinent to the requested Data Reference in the User-Data AVP. The HSS shall set the Result-Code to DIAMETER_SUCCESS. This includes cases where the data is not available to the HSS. The pertinent data included shall refer to the received IMS Public User Identity.

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 [12] and 3GPP TS 29.229 [6] 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 a database error or empty mandatory data elements, 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. Result-Code DIAMETER_SUCCESS is used also if the requested data does not exist in the HSS i.e. when the HSS is indicating valid empty data elements.

5.2.2 Data Update (Sc-Update)

5.2.2.1 General

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

- To allow the DCSF to update the transparent (repository) data stored at the HSS for each IMS Public User Identity.

This procedure is mapped to the commands Profile-Update-Request/Answer in the Diameter application specified in clause 6.2.3 and clause 6.2.4. Tables 5.2.1-1 and 5.2.1-2 detail the involved information elements.

Table 5.2.2-1: Sc-Update Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 3GPP TS 29.328 [4])	User-Identity	M	It shall contain the IMS Public User Identity (in the Public-Identity AVP) for which data is updated.
Requested data (See 3GPP TS 29.328 [4])	Data-Reference	M	This information element includes the reference to the data on which updates are required.
Data (See 3GPP TS 29.328 [4])	User-Data	M	Updated data.

Table 5.2.2-2: Sc-Update Response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 3GPP TS 29.328 [4])	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 (see IETF RFC 6733 [44]). Experimental-Result AVP shall be used for Sc 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.
Repository Data ID (See 3GPP TS 29.328 [4])	Repository-Data-ID	O	If a Sc-Update Request with multiple repository data fails, this information element shall include the service indication and the sequence number of the repository data instance that has generated the error.
Requested data (See 3GPP TS 29.328 [4])	Data-Reference	O	If Sc-Update Request with multiple data references fails, this information element shall include the Data reference for the data instance that has generated the error.

5.2.2.2 Detailed behaviour

As specified in 3GPP TS 23.228 [2], the DCSF can only update the repository data in HSS. When data in repository is dated is updated (i.e. added, modified or removed), the 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 Sc-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 Sc-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 Sc-Update request, the HSS shall, in the following order:

1. In the DCSF permission list check that the data that is requested to be updated (Sc-Update) by this DCSF, is allowed to be updated by checking the combination of the identity of the DCSF 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 shall be set to DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED in the Sc-Update Response.

2. Check that the User Identity in the request exists in the HSS. If not, Experimental-Result shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Sc-Update Response.

3. If the type of the User Identity does not use IMS Public User Identity as access key for the Data-Reference or the Data-Reference is not Repository Data (0) in the request, Experimental-Result shall be set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED in the Sc-Update Response.

4. If the Data-Reference indicates that repository data is present, and if the HSS and the DCSF supports the Update-Eff feature, check whether there are multiple repository data instances. If so, then repeat the steps 5 and 6 below for each instance of repository data ensuring that no repository data is changed until the checks done in the steps 5 and 6 have been successful for all the repository data instances.

5. Check whether or not the data that is requested to be updated by the DCSF, 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 shall be set to DIAMETER_PRIOR_UPDATE_IN_PROGRESS in the Sc-Update Response.

6. Check whether or not there is any repository data stored at the HSS already for the specified Service-Indication and the associated IMS Public User Identity (or group if the IMS Public User Identity is alias).

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

  1. Sequence_Number_in_Sc_Update is not equal to 0

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

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

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

    - If Service Data element is present in the Sc-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 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 Sc-Update Req and the Sequence Number associated with that repository data shall be updated with that sent in the Sc-Update Req.

    - If Service Data element is not present in the Sc-Update Req, 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.

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

  - If the sequence number is not set to 0, Experimental-Result 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 Sc-Update Req.

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

    - If Service Data element is present in the Sc-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 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 Sc-Update Req, then the data shall be stored in 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 clause 6.4 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.

If the HSS and the DCSF support the Update-Eff feature, the Sc Update is successful only if it is successful for the update of all the repository data instances in the request. Otherwise the HSS shall keep or restore all the stored repository data as they were before receiving the Sc Update request. If the error occurs during the steps 5 or 6 and if there were several repository data instances in the request, the Sc Update response shall contain a Repository Data ID indicating the service indication and the sequence number of (one of) the repository data instance(s) for which an error occurred.

If the HSS and the DCSF support the Update-Eff-Enhance feature, the Sc Update is successful only if it is successful for the update of all the data instances in the request. Otherwise the HSS shall keep or restore all the stored data as they were before receiving the Sc Update request. If an error occurs during the steps 5 or 6 with any of the data instance in the request, the Sc Update response shall contain the corresponding Data Reference indicating the first data instance for

which an error occurred. If there were several repository data instances in the request, the HSS shall behave the same as specified for Update-Eff feature.

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

NOTE: When an DCSF receives DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC the DCSF may attempt to resolve the inconsistency between the version of the repository data that it holds and that stored at the HSS. It may execute a Sc-Pull to retrieve the current version of the data from the HSS.

6 Protocol Specification and Implementations

6.1 Introduction

6.1.1 Use of Diameter base protocol

The Diameter base protocol as specified in IETF RFC 6733 [3] shall apply except as modified by the defined support of the methods and the defined support of the commands and AVPs, result and error codes as specified in this specification. Unless otherwise specified, the procedures (including error handling and unrecognised information handling) shall be used unmodified.

6.1.2 Accounting functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) shall not be used on the Sc interfaces.

6.1.3 Use of sessions

Between the DCSF and HSS, Diameter sessions shall be implicitly terminated. An implicitly terminated session is one for which the server does not maintain state information. The client shall not send any re-authorization or session termination requests to the server.

The Diameter base protocol specified in IETF RFC 6733 [3] includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in IETF RFC 6733 [3]. As a consequence, the server shall not maintain any state information about this session and the client shall not send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

6.1.4 Transport protocol

Diameter messages over the Sc interfaces shall make use of SCTP IETF RFC 4960 [5].

6.1.5 Routing consideration

The User identity to HSS resolution mechanism enables the DCSF to find the identity of the HSS that holds the subscriber data for a given IMS 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 a DCSF is configured to use pre-defined HSS.

The resolution mechanism described in 3GPP TS 23.228 [2] shall use a Diameter Proxy Agent.

The Diameter Proxy Agent shall be to determine the HSS identity.

To get the HSS identity the DCSF shall send the Sc request normally destined to the HSS to a pre-configured Diameter address/name.

- If this Sc Request is received by the Diameter Proxy Agent, the Diameter Proxy Agent shall determine the HSS identity based on the provided user identity and - if the Diameter load control mechanism is supported (see IETF RFC 8583 [14]) - optionally also based on previously received load values from Load AVPs of type HOST. The Diameter Proxy Agent shall then forward the Sc request directly to the determined HSS. The DCSF shall determine the HSS identity from the response to the Sc request received from the HSS.

The DCSF should store the HSS identity/name/Realm and shall use it in further Sc requests associated to the same IMS Public Identity.

In networks where the use of the user identity to HSS resolution mechanism is required and the DCSF is not configured to use a predefined HSS, each DCSF shall be configured with the pre-configured address/name of the Diameter Proxy Agent to enable use of these resolution mechanisms.

If a DCSF knows the address/name of the HSS for a certain user, and the associated home network domain name, both the Destination-Realm and Destination-Host AVPs shall be present in the request. Otherwise, only the Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node, e.g. the Diameter Proxy Agent (see 3GPP TS 29.228 [13]), based on the Diameter routing table in the client.

If the next Diameter node is a Diameter Proxy Agent, the Diameter Proxy Agent shall determine the destination HSS. The Diameter Proxy Agent, based on the result of this determination of the destination HSS, shall modify the Destination-Realm AVP and Destination-Host AVP of the request appropriately. The Diameter Proxy Agent shall then append a Route-Record AVP to the request and shall send the request to the destination HSS. Consequently, the Destination-Host AVP is declared as optional in the ABNF for all requests initiated by an DCSF.

If the response is routed back to a Diameter Proxy Agent, the Diameter Proxy Agent shall send the response back to the DCSF without modifying the Origin-Realm AVP and Origin-Host AVP. The response shall contain the Origin-Realm AVP set to the realm of the HSS together with the Origin-Host AVP set to the HSS that sent the response. The DCSF shall store the HSS realm and HSS address for each Public Identity, after the first request sent to the User Identity to HSS resolution function.

The Destination-Realm AVP is declared as mandatory in the ABNF for all requests.

6.1.6 Diameter Application Identifier

The Sc interface protocol shall be 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 Sc interface application is 16777363 (allocated by IANA).

6.1.7 DCSF permissions list

The contents of the Data-AVP are described in table 6.3.4-1. Some of the individual elements carried within Data-AVP may be requested by the DCSF from the HSS using the Sc-Pull command (see clause 6.2.3) or may be updated at the HSS by the DCSF using the Sc-Update command (see clause 6.2.5). 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 DCSF, as indicated in table 6.3.4-1.

To manage whether an DCSF may request each element of Data-AVP with a specific command, the HSS shall maintain a list of DCSF permissions (the 'DCSF Permissions List'). DCSF permissions are identified by DCSF identity and Data Reference with the possible permissions associated with each Data Reference being Sc-Pull, Sc-Update. The permissions apply to all users served by the HSS, they are not user specific. When an DCSF requests Sc-Pull, Sc-Update the HSS shall check permissions and return an error result if the DCSF does not have the required permission.

6.2 Commands

6.2.1 Introduction

This clause defines the command code values and related ABNF for each command described in this specification.

6.2.2 Command-code values

The messages in Sc interface use the same Command-Code value 306 as User-Data-Request/ User-Data-Answer and 307 as Profile-Update-Request/Profile-Update-Answer defined in 3GPP TS 29.328 [4].

The Vendor-Specific-Application-Id AVP shall not be listed in this specification since it has been deprecated in the new specification of the Diameter base protocol (IETF RFC 6733 [3]) even it is still listed as a required AVP (an AVP indicated as {AVP}) in the command code format specifications defined in 3GPP TS 29.328 [4].

The following Command Codes defined in 3GPP TS 29.328 [4] are reused in this specification:

Table 6.2.2: Command-Code values

Command-Name	Abbreviation	Code	Clause
User-Data-Request	UDR	306	6.2.3
User-Data-Answer	UDA	306	6.2.4
Profile-Update-Request	PUR	307	6.2.5
Profile-Update-Answer	PUA	307	6.2.6

6.2.3 User-Data-Request (UDR) Command

The User-Data-Request (UDR) command, indicated by the Command-Code field set to 306 and the 'R' bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to request repository data for a specified user.

Message Format

< User-Data -Request> ::= < Diameter Header: 306, REQ, PXY, 16777363 >
< Session-Id >
[DRMP]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Destination-Host]
{ Destination-Realm }
{ User-Identity }
***[Service-Indication]**
***{ Data-Reference }**
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.2.4 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 Experimental-Result AVP may contain one of the values defined in clause 6.2 or in 3GPP TS 29.229 [6].

Message Format

< User-Data-Answer > ::= < Diameter Header: 306, PXY, 16777363 >
< Session-Id >
[DRMP]
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[User-Data]
*[AVP]
[Failed-AVP]

*[Proxy-Info]
*[Route-Record]

6.2.5 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, 16777363 >
< Session-Id >
[DRMP]
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Destination-Host]
{ Destination-Realm }
{ User-Identity }
***{** Data-Reference **}**
{ User-Data }
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.2.6 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 server in response to the Profile-Update-Request command.

Message Format

< Profile-Update-Answer > ::=< Diameter Header: 307, PXY, 16777363 >
< Session-Id >
[DRMP]
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Repository-Data-ID]
*[AVP]
[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

6.3 Information Elements

6.3.1 General

This clause defines the command code values and related ABNF for each command described in this specification.

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

Table 6.3.1-1: Sc specific DiameterAVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**

The following table specifies the Diameter AVPs re-used by the Sc interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within Sc.

Any other AVPs from existing Diameter Applications, except for the AVPs from Diameter base protocol specified in IETF RFC 6733 [3], do not need to be supported. The AVPs from the Diameter base protocol specified in IETF RFC 6733 [3] are not included in table 6.3.1-2, but they may be re-used for the Sc protocol.

Table 6.3.1-2: Sc re-used Diameter AVPs

Attribute Name	Reference	Comments	M-bit
User-Identity	3GPP TS 29.329 [12]		Must set
Data-Reference	3GPP TS 29.329 [12]		Must set
User-Data	3GPP TS 29.329 [12]		Must set
Repository-Data-ID	3GPP TS 29.329 [12]		
Public-Identity	3GPP TS 29.229 [6]		Must set
Service-Indication	3GPP TS 29.329 [12]		Must set
Sequence-Number	3GPP TS 29.329 [12]		
MSISDN	3GPP TS 29.329 [12]		
External-Identifier	3GPP TS 29.336 [7]		
OC-Supported-Features	3GPP TS 29.229 [6]		
OC-OLR	3GPP TS 29.229 [6]		
Load	3GPP TS 29.229 [6]		
DRMP	3GPP TS 29.229 [6]		

NOTE 1: The M-bit settings for re-used AVPs override those of the defining specifications that are referenced. Values include: "Must set", "Must not set". If the M-bit setting is blank, then the defining specification applies.
NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.
NOTE 3: The value of these attributes is defined in IETF RFC 7683 [8].
NOTE 4: The value of this attribute is defined in IEFT RFC 8583 [14].
NOTE 5: The value of this attribute is defined in IETF RFC 7944 [9].

6.3.2 User-Identity AVP

The User-Identity AVP is of type Grouped. See 3GPP TS 29.329 [6] clause 6.3.1 for the definition of this AVP.

NOTE: Only the Public Identity applies to the Sc interface in this AVP in this release.

6.3.3 Data-Reference AVP

The Data-Reference AVP is of type Enumerated, and indicates the type of the requested user data in the operation UDR and PUR. See 3GPP TS 29.329 [6] clause 6.3.4.

The value of this AVP can only be set to 0 since DCSF can only get and update repository data.

6.3.4 User-Data AVP

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

Annex D specifies the UML logical model of the data downloaded via the Sc interface.

Table 6.3.4 defines the data reference values and tags, access key and recommended DCSF permissions for the operation(s) on data accessible via the Sc interface, i.e. the listed operation(s) in the Operations column are the only ones allowed to be used with this Data Ref value.

Table 6.3.4-1: Data accessible via Sc interface

Data Ref.	XML tag	Defined in	Access key	Operations
0	RepositoryData	6.3.5	Data Reference + (IMS Public User Identity) + Service Indication	Sc-Pull Sc-Update

The User-Data AVP is of type OctetString. This AVP contains the user data requested in the UDR/UDA operations and the data to be modified in the PUR/PUA operation. The exact content and format of this AVP is described in Annex C as Sc-Data.

6.3.5 Repository-Data-ID AVP

The Repository-Data-ID AVP is of type Grouped. This AVP shall contain a Service-Indication AVP and a Sequence-Number AVP. See 3GPP TS 29.329 [6] clause 6.3.24.

6.3.6 Public-Identity AVP

The Public-Identity AVP contains a Public User Identity. See 3GPP TS 29.229 [6] for the definition of this AVP.

6.3.7 Service-Indication AVP

The Service-Indication AVP is of type OctetString. This AVP contains the Service Indication that identifies the related repository data in the HSS. Standardized values of Service-Indication identifying standardized format of the related repository data are defined in 3GPP TS 29.364 [15].

6.3.8 Sequence-Number AVP

The Sequence-Number AVP is of type Unsigned32. This AVP contains a number associated to a repository data.

6.3.9 MSISDN AVP

The MSISDN AVP is of type OctetString. See 3GPP TS 29.329 [12] for the definition of this AVP.

NOTE: This MSISDN AVP does not apply to the Sc interface in this release.

6.3.10 External-Identifier AVP

See 3GPP TS 29.336 [7] for the definition of this AVP.

NOTE: This External-Identifier AVP does not apply to the Sc interface in this release.

6.3.11 OC-Supported-Features AVP

The OC-Supported-Features AVP is of type Grouped and it is defined in IETF RFC 7683 [8]. This AVP is used to support Diameter overload control mechanism.

6.3.12 OC-OLR AVP

The OC-OLR AVP is of type Grouped and it is defined in IETF RFC 7683 [8]. This AVP is used to support Diameter overload control mechanism.

6.3.13 Load AVP

The Load AVP is of type Grouped and it is defined in IETF RFC 8583[14]. This AVP is used to support the Diameter load control mechanism.

6.3.14 DRMP AVP

The DRMP AVP is of type Enumerated and it is defined in IETF RFC 7944 [26]. This AVP allows the HSS/SLF and the DCSF to indicate the relative priority of Diameter messages. The DRMP AVP may be used to set the DSCP marking for transport of the associated Diameter message.

6.4 Result Codes

6.4.1 General

This clause defines new result code values that must be supported by all Diameter implementations that conform to this specification. The result codes defined in 3GPP TS 29.329 [4] are also applicable. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and Result-Code AVP shall be absent.

6.4.2 Success

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

6.4.3 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.

6.4.3.1 DIAMETER_ERROR_USER_UNKNOWN (5001)

A message was received for a user identity that is unknown. This error code is defined in 3GPP TS 29.229 [6] clause 6.2.2.1.

6.4.3.2 DIAMETER_ERROR_OPERATION_NOT_ALLOWED (5101)

The requested operation is not allowed for the user. This error code is defined in 3GPP TS 29.329 [12] clause 6.2.2.2.

6.4.3.3 DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ (5102)

The requested user data is not allowed to be read. This error code is defined in 3GPP TS 29.329 [12] clause 6.2.2.3.

6.4.3.4 DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED (5103)

The requested user data is not allowed to be modified. This error code is defined in 3GPP TS 29.329 [12] clause 6.2.2.4.

6.4.3.5 DIAMETER_ERROR_TOO_MUCH_DATA (5008)

The size of the data pushed to the receiving entity exceeds its capacity. This error code is defined in 3GPP TS 29.229 [6] clause 6.2.2.8.

6.4.3.6 DIAMETER_ERROR_TRANSPARENT_DATA OUT_OF_SYNC (5105)

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. That is, the sequence number in the Sc-Update Request message, does not match with the immediate successor of the associated sequence number stored for that repository data at the HSS. It is

also used where an DCSF tries to create a new set of repository data when the identified repository data already exists in the HSS. This error code is defined in 3GPP TS 29.329 [12] clause 6.2.2.7.

6.4.3.7 DIAMETER_ERROR_FEATURE_UNSUPPORTED (5011)

A request application message was received indicating that the origin host requests that the command pair would be handled using a feature which is not supported by the destination host. The error code is defined in 3GPP TS 29.229 [6] clause 6.2.2.11.

6.4.4 Transient Failures

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

6.4.4.1 DIAMETER_USER_DATA_NOT_AVAILABLE (4100)

The requested user data is not available at this time to satisfy the requested operation. This error code is defined in 3GPP TS 29.329 [12] clause 6.2.3.1.

6.4.4.2 DIAMETER_PRIOR_UPDATE_IN_PROGRESS (4101)

The request on the updated or read repository data is currently being updated by another entity. This error code is defined in 3GPP TS 29.329 [12] clause 6.2.3.2.

Annex A (normative): Diameter overload control mechanism

A.1 General

Diameter overload control mechanism is an optional feature.

IETF RFC 7683 [8] specifies a Diameter overload control mechanism which includes the definition and the transfer of related AVPs between Diameter nodes.

It is recommended to make use of IETF RFC 7683 [8] on the Sc interface where, when applied, the DCSF shall behave as a reacting node and the HSS as a reporting node.

Depending on regional/national requirements and network operator policy, priority traffic (e.g. MPS as described in 3GPP TS 22.153 [10]) shall be exempted from throttling due to Diameter overload control up to the point where requested traffic reduction cannot be achieved without throttling the priority traffic.

A.2 HSS behaviour

The HSS requests traffic reduction from the DCSF when the HSS is in an overload situation, including OC-OLR AVP in answer commands as described in IETF RFC 7683 [8].

The HSS identifies that it is in an overload situation by implementation specific means. For example, the HSS may take into account the traffic over the Sc interfaces or other interfaces, the level of usage of internal resources (CPU, memory), the access to external resources, etc.

The HSS determines the specific contents of OC-OLR AVP in overload reports and the HSS decides when to send OC-OLR AVPs by implementation specific means.

A.3 DCSF behaviour

The DCSF applies required traffic reduction received in answer commands to subsequent applicable requests, as per IETF RFC 7683 [8].

The DCSF achieves requested traffic reduction by implementation specific means. For example, the DCSF may implement message throttling with prioritization or a message retaining mechanism for operations that can be postponed.

Diameter requests related to priority traffic (e.g. MPS) and emergency, detected via the presence of priority information (e.g., Resource-Priority header field for MPS) in SIP messages as described in 3GPP TS 24.229 [11], have the highest priority. Depending on regional/national regulatory and operator policies, these Diameter requests shall be the last to be throttled, when the DCSF has to apply traffic reduction. Relative priority amongst various priority traffic (e.g. MPS) and emergency traffic is subject to regional/national regulatory and operator policies.

Annex B (normative): Diameter message priority mechanism

B.1 General

IETF RFC 7944 [9] specifies a Diameter message priority mechanism that allows Diameter nodes to indicate the relative priority of Diameter messages. With this information, other Diameter nodes may leverage the relative priority of Diameter messages into routing, resource allocation, set the DSCP marking for transport of the associated Diameter message, and also abatement decisions when overload control is applied.

B.2 Sc interface

B.2.1 General

The Diameter message priority mechanism is an optional feature.

It is recommended to make use of IETF RFC 7944 [9] over the Sc interface of an operator network when the overload control defined in Annex A is applied on this Sc interface.

B.2.2 DCSF behaviour

When the DCSF supports the Diameter message priority mechanism, the DCSF shall comply with IETF RFC 7944 [9].

The DCSF sending a request shall determine the required priority according to its policies. When priority is required, the DCSF shall include the DRMP AVP indicating the required priority level in the request it sends, and shall prioritise the request according to priority level received.

When the DCSF receives the corresponding response, it shall prioritise the received response according to the priority level received within the DRMP AVP if present in the response, otherwise according to the priority level of the corresponding request.

If:

- the DCSF supports using the Diameter message priority mechanism for DSCP marking purposes,
- the transport network utilizes DSCP marking, and
- message-dependant DSCP marking is possible for the protocol stack transporting Diameter,

then the DCSF shall set the DSCP marking for transport of the request or response according to the required priority level.

Diameter requests related to priority traffic (e.g. MPS as identified by the AS through SIP procedures, emergency) shall contain a DRMP AVP with a high priority of which the level value is operator dependent.

When not-explicitly requested, the inclusion and priority value of the DRMP AVP in Diameter messages are implementation specific.

B.2.3 HSS behaviour

When the HSS supports the Diameter message priority mechanism, the HSS shall comply with IETF RFC 7944 [9].

The HSS sending a request shall determine the required priority according to its policies. When priority is required, the HSS shall include the DRMP AVP indicating the required priority level in the request it sends, and shall prioritise the request according to the required priority level.

When the HSS receives the corresponding response, it shall prioritise the received response according to the priority level received within the DRMP AVP if present in the response, otherwise according to the priority level of the corresponding request.

When the HSS receives a request, it shall handle the request according to the received DRMP AVP priority level. For the response, it may modify the priority level received in the DRMP AVP according to its policies and shall handle the response according to the required priority level. If the required priority level is different from the priority level received in the request, it shall include the DRMP AVP in the response.

If:

- the HSS supports using the Diameter message priority mechanism for DSCP marking purposes,
- the transport network utilizes DSCP marking, and
- message-dependant DSCP marking is possible for the protocol stack transporting Diameter,

then the HSS shall set the DSCP marking for transport of the request or response according to the required priority level.

When not-explicitly requested, the inclusion and priority value of the DRMP AVP in Diameter messages are implementation specific.

Annex C (normative): XML schema for the Sc interface user profile

The file ScDataType_Rel18.xsd, attached to this specification, contains the XML schema for the user profile that is sent over the Sc interface. The user profile XML schema defines the data 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. The user profile XML schema file is intended to be used by an XML parser.
The version of the Sc 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 C.1 and C.2 describe the data types and the dependencies among them that configure the user profile XML schema.

Table C.1: XML schema for the Sc user profile interface: simple data types

Data type	Tag	Base type	Comments
tSIP_URL	IMSPublicIdentity	anyURI	Syntax described in IETF RFC 3261 [16]. Wildcarded IMPU and Wildcarded PSI syntax described in 3GPP TS 23.003.
tTEL_URL	IMSPublicIdentity	anyURI	Syntax described in IETF RFC 3966 [17]. Wildcarded IMPU and Wildcarded PSI syntax described in 3GPP TS 23.003.
tIMSPublicIdentity	IMSPublicIdentity	(union)	Union of tSIP_URL and tTEL_URL
tSequenceNumber	SequenceNumber	integer	>=0, <=65535

Table C.2: XML schema for the Sc user profile interface: complex data types

Data type	Tag	Compound of		
		Tag	Type	Cardinality
tSc-Data	Sc-Data	PublicIdentifiers	tPublicIdentity	0 to 1
		RepositoryData	tTransparentData	0 to n
tTransparentData	RepositoryData	ServiceIndication	string	1
		SequenceNumber	tSequenceNumber	1
		ServiceData	tServiceData	0 to 1
tServiceData	any	any	any	1
tPublicIdentity	PublicIdentifiers	IMSPublicIdentity	tIMSPublicIdentity	0 to n

NOTE 1: "n" shall be interpreted as non-bounded.
NOTE 2: empty cells shall be interpreted as complex XML elements without defined content.

Annex D (informative): UML model of the data downloaded over Sc interface

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

The following picture gives an outline of the UML model of the user profile, which is exchanged between the HSS and an DCSF:

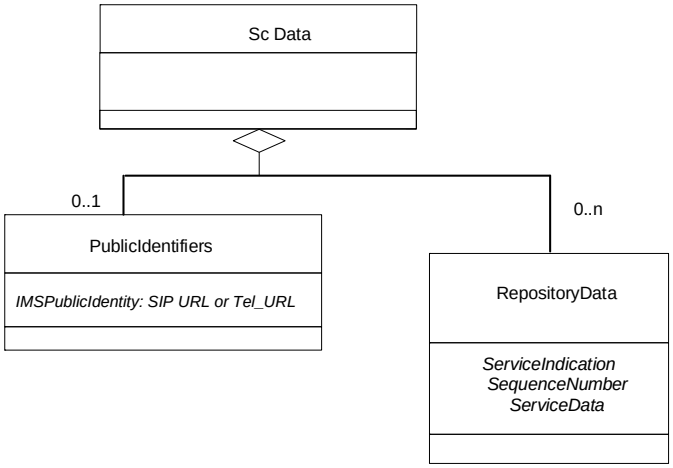

Figure D.1: Sc-Data

Each instance of the class Sc-Data contains an optional instance of the class PublicIdentifiers, zero or more instances of the class RepositoryData.

Class RepositoryData contains repository data (transparent data) for a given service that are associated to a Public user Identity or a group of alias Public User Identities. It has attributes ServiceIndication, SequenceNumber and ServiceData.

Class PublicIdentifiers contains zero or more instances of IMSPublicIdentity attribute. Each instance is a Public User Identity.

Annex E (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2023-10	CT4#118	C4-234651				TS skeleton	0.1.0
2023-11	CT4#119	C4-235662				Incorporated pCRs agreed from CT4#119 meeting, including: C4-235204, C4-235205, C4-235207, C4-235209, C4-235224, C4-235474, C4-235679, C4-235680	0.2.0
2024-03	CT4#121	C4-240853				Incorporated pCRs agreed from CT4#121 meeting, including: C4-240411, C4-240413, C4-240416, C4-240418, C4-240444, C4-240706, C4-240707, C4-240713, C4-240714, C4-240784, C4-240786, C4-240787	0.3.0
2024-03	CT#103					Application ID for Sc added by MCC	1.0.0
2024-03	CT#103	CP-240287				TS send for information and approval	1.0.0
2024-03	CT#103					TS approved	18.0.0

History

Document history		
V18.0.0	May 2024	Publication