

ETSI TS 129 389 V17.0.0 (2022-04)



**LTE;
Inter-V2X Control Function Signalling aspects (V6);
Stage 3
(3GPP TS 29.389 version 17.0.0 Release 17)**



Reference

RTS/TSGC-0429389vh00

Keywords

LTE

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

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2022.
All rights reserved.

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 <http://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

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	5
1 Scope	7
2 References	7
3 Definitions and abbreviations.....	8
3.1 Definitions	8
3.3 Abbreviations	8
4 General Description.....	8
4.1 Introduction	8
5 Procedure Description	8
5.1 Introduction	8
5.2 V2X Service Authorization	8
5.2.1 General.....	8
5.2.2 Detailed behaviour of the V2X Control Function in the HPLMN	9
5.2.3 Detailed behaviour of the V2X Control Function in the VPLMN	10
6 Protocol Specification and Implementations.....	10
6.1 Introduction	10
6.1.1 Use of Diameter base protocol.....	10
6.1.2 Securing Diameter Messages	10
6.1.3 Accounting functionality	10
6.1.4 Use of sessions.....	10
6.1.5 Transport protocol	11
6.1.6 Routing considerations	11
6.1.7 Advertising Application Support	11
6.1.8 Diameter Application Identifier.....	11
6.1.9 Use of the Supported-Features AVP	11
6.2 Commands.....	12
6.2.1 Introduction.....	12
6.2.2 Command-Code values.....	12
6.2.3 ProSe-Authorization-Request (PAR) Command	12
6.2.4 ProSe-Authorization-Answer (PAA) Command.....	13
6.3 Information Elements	13
6.3.1 General.....	13
6.3.2 V2X-Authorization-Data	14
6.3.3 V2X-Permission-in-VPLMN.....	15
6.3.4 V2X-Application-Server.....	15
6.3.5 Application-Server.....	15
6.3.6 Geographical-Information	15
6.3.7 OC-Supported-Features	15
6.3.8 OC-OLR	16
6.3.9 DRMP	16
6.3.10 Load	16
6.3.11 PC5-RAT-Type.....	16
6.4 Result-Code AVP and Experimental-Result AVP Values	16
6.4.1 General.....	16
6.4.2 Success.....	16
6.4.3 Permanent Failures	16
6.4.3.1 General	16
6.4.3.2 DIAMETER_ERROR_USER_UNKNOWN (5001)	16
6.4.3.3 DIAMETER_ERROR_UNKNOWN_V2X_SUBSCRIPTION (5690)	16

6.4.3.4	DIAMETER_ERROR_V2X_NOT_ALLOWED (5691).....	17
Annex A (normative):	Diameter overload control mechanism	18
A.1	General	18
A.2	Responding V2X Control Function behaviour	18
A.3	Requesting V2X Control Function behaviour	18
Annex B (Informative):	Diameter overload node behaviour	18
B.1	Message prioritization	18
Annex C (normative):	Diameter message priority mechanism	19
C.1	General	19
C.2	V6 interfaces	19
C.2.1	General.....	19
C.2.2	V2X Control Function behaviour	19
D.1	General	19
D.2	Responding V2X Control Function behaviour	19
D.3	Requesting V2X Control Function behaviour	20
Annex E (informative):	Change history	21
History		22

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 interfaces between the V2X Control Function in the HPLMN and the V2X Control Function in the VPLMN (V6 interface).

This specification defines the Diameter application for V6 reference points between the V2X Control Functions. The interactions between the V2X Control Functions are specified.

The stage 2 description for V2X service features in EPS is specified in 3GPP TS 23.285 [2].

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 23.285: "Architecture enhancements for V2X services; Stage 2".
- [3] IETF RFC 6733: "Diameter Base Protocol".
- [4] 3GPP TS 33.210: "3G Security; Network Domain Security; IP Network Layer Security".
- [5] IETF RFC 4960: "Stream Control Transmission Protocol".
- [6] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol".
- [7] IETF RFC 5234: "Augmented BNF for Syntax Specifications: ABNF".
- [8] 3GPP TS 23.003: "Numbering, addressing and identification".
- [9] 3GPP TS 29.228: "IP multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and Message Elements".
- [10] 3GPP TS 29.272: "Evolved Packet System; MME and SGSN Related Interfaces Based on Diameter Protocol".
- [11] 3GPP TS 29.329: "Sh Interface based on the Diameter protocol".
- [12] IETF RFC 7683: "Diameter Overload Indication Conveyance".
- [13] 3GPP TS 29.336: "Home Subscriber Server (HSS) diameter interfaces for interworking with packet data networks and applications".
- [14] 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging applications".
- [15] IETF RFC 7944: "Diameter Routing Message Priority".
- [16] 3GPP TS 29.388: "V2X Control Function to V2X Control Function to Home Subscriber Server (HSS) aspects (V4)".
- [17] 3GPP TS 29.345: "Inter-Proximity-services (ProSe) Function signalling aspects".
- [18] IETF RFC 8583: "Diameter Load Information Conveyance".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP 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 3GPP TR 21.905 [1].

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

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

ProSe	Proximity-based Services
V2X	Vehicle-to-Everything

4 General Description

4.1 Introduction

The V6 reference point is defined between a V2X Control Function in the HPLMN and a V2X Control Function in the VPLMN.

The definition of the V6 reference points and related functionalities are given in 3GPP TS 23.285 [2].

As defined in 3GPP TS 23.285 [2], the V6 reference point is used for:

- HPLMN control of service authorization for V2X.

5 Procedure Description

5.1 Introduction

This clause describes the Diameter-based V6 interface related procedures and Information elements exchanged between functional entities.

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 29.228 [9].

5.2 V2X Service Authorization

5.2.1 General

The V2X Service Authorization Procedure shall be used between the V2X Control Function in the HPLMN and the V2X Control Function in the VPLMN to obtain service authorization information for V2X services. The procedure shall be invoked by the V2X Control Function in the HPLMN of the UE and is used:

- to request service authorization information for V2X related to the UE from the V2X Control Function in the VPLMN;
- to provide the V2X Control Function in the VPLMN with the UE identity (IMSI or MSISDN) in order to allow to perform charging;

This procedure is mapped to the commands ProSe-Authorization-Request/Answer (PAR/PAA) in the Diameter application specified in clause 6.

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: V2X Service Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
UE Identity (See 3GPP TS 29.336 [13])	User-Identifier	M	This information element shall contain either the user IMSI, formatted according to 3GPP TS 23.003 [8], clause 2.2, or the user MSISDN, formatted according to 3GPP TS 29.329 [11].
PLMN Id (See 3GPP TS 29.272 [10])	Visited-PLMN-Id	M	This IE shall contain the PLMN-Id (3GPP TS 23.003 [8]) of the network in which the V2X Control Function is located.
Supported Features (See 3GPP TS 29.229 [6])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

Table 5.2.1-2: V2X Service Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 6.4)	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used to indicate success / errors as defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for V6 errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. The following errors are applicable: - User Unknown - Unauthorized Service - Unauthorized Service in this PLMN
Supported Features (See 3GPP TS 29.229 [6])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
V2X Authorization Data (See 6.3.2)	V2X-Authorization-Data	C	This Information Element shall contain the V2X authorization information of the user. It shall be present if success is reported.

5.2.2 Detailed behaviour of the V2X Control Function in the HPLMN

The V2X Control Function in the HPLMN shall make use of this procedure to request service authorization information for V2X related to the UE from the V2X Control Function in the VPLMN. The V2X Control Function shall include in the request the UE identity (IMSI or MSISDN) and the PLMN-Id identifying the PLMN of the requesting V2X Control Function.

When receiving a V2X Service Authorization response from the V2X Control Function in the VPLMN, the V2X Control Function in the HPLMN shall check the result code. If it indicates SUCCESS, the V2X Control Function shall merge with its own policy.

5.2.3 Detailed behaviour of the V2X Control Function in the VPLMN

When receiving a V2X Service Authorization request, the V2X Control Function in the VPLMN shall, in the following order:

1. Check whether the UE Identity (IMSI or MSISDN) exists. If not, a Result Code of DIAMETER_ERROR_USER_UNKNOWN shall be returned.
2. Check whether V2X is authorized for this UE Identity. If not, a Result Code of DIAMETER_ERROR_UNAUTHORIZED_SERVICE shall be returned.

If there is an error in any of the above steps then the V2X Control Function shall stop processing the request and shall return the error code specified in the respective step.

If the V2X Control Function cannot fulfil the received request for reasons not stated in the above steps, e.g. due to a database error or any of the required actions cannot be performed, it shall stop processing the request and set the Result Code to "DIAMETER_UNABLE_TO_COMPLY".

Otherwise, when the UE is authorized to use V2X over PC5 or V2X over MBMS in this PLMN, the V2X Control Function shall include the V2X-Authorization-Data AVP in the response to return V2X permissions and the V2X Application Server information, and shall set the Result Code to "DIAMETER_SUCCESS".

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 Securing Diameter Messages

For secure transport of Diameter messages, see 3GPP TS 33.210 [4].

6.1.3 Accounting functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) shall not be used on the V6 interface.

6.1.4 Use of sessions

Between the V2X Control Functions, 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 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.

6.1.5 Transport protocol

Diameter messages over the V6 interface shall make use of SCTP IETF RFC 4960 [5].

6.1.6 Routing considerations

This clause specifies the use of the Diameter routing AVPs Destination-Realm and Destination-Host.

The Destination-Realm AVP shall contain the network domain name of the targeted V2X Control Function. The network domain name is either known by the sending V2X Control Function or derived from the PLMN-Id of the targeted V2X Control Function to construct the EPC Home Network Realm/Domain, as indicated in 3GPP TS 23.003 [8], clause 19.2.

If a V2X Control Function knows the address/name of the V2X Control Function in charge of a given UE, and the associated network domain name, both the Destination-Realm and Destination-Host AVPs shall be present in the request.

If a V2X Control Function knows only the network domain name, the Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node.

Consequently, the Destination-Realm AVP is declared as mandatory and the Destination-Host AVP is declared as optional in the ABNF for all requests initiated by a V2X Control Function.

If the Vendor-Specific-Application-Id AVP is received in any of the commands defined in this specification, it shall be ignored by the receiving node, and it shall not be used for routing purposes.

6.1.7 Advertising Application Support

The V2X Control Functions shall advertise support of the Diameter Inter V2X Control Functions Application by including the value of the application identifier in the Auth-Application-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

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

The Vendor-Id AVP included in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands that is not included in the Vendor-Specific-Application-Id AVPs as described above shall indicate the manufacturer of the Diameter node as per IETF RFC 6733 [3].

6.1.8 Diameter Application Identifier

The Diameter Inter V2X Control Functions Application 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 Diameter Inter V2X Control Functions application is 16777356 (allocated by IANA). The Diameter application identifier is used over the V6 interface.

6.1.9 Use of the Supported-Features AVP

When new functionality is introduced on the V6 interface, it should be defined as optional. If backwards incompatible changes cannot be avoided, the new functionality shall be introduced as a new feature and support advertised with the Supported-Features AVP. The usage of the Supported-Features AVP on the V6 interface is consistent with the procedures for the dynamic discovery of supported features as defined in clause 7.2 of 3GPP TS 29.229 [6].

When extending the application by adding new AVPs for a feature, the new AVPs shall have the M bit cleared and the AVP shall not be defined mandatory in the command ABNF.

As defined in 3GPP TS 29.229 [6], the Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. On the all reference points as specified in this specification, the Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, for features defined in this document, the Vendor-Id AVP shall contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined for the reference point, the Feature-List-ID AVP shall differentiate those lists from one another.

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

This subclause defines Command-Code values for the Diameter Inter V2X Control Functions application used over the V6 interface as allocated by IANA.

Every command is defined by means of the ABNF syntax IETF RFC 5234 [7], according to the rules in IETF RFC 6733 [3]. In the case, the definition and use of an AVP is not specified in this document, the guidelines in IETF RFC 6733 [3] shall apply.

The Vendor-Specific-Application-Id AVP shall not be included in any command sent by Diameter nodes supporting applications defined in this specification. If the Vendor-Specific-Application-Id AVP is received in any of the commands defined in this specification, it shall be ignored by the receiving node.

NOTE: The Vendor-Specific-Application-Id is included as an optional AVP in all Command Code Format specifications defined in this specification in order to overcome potential interoperability issues with intermediate Diameter agents non-compliant with IETF RFC 6733 [3].

The following Command Codes are defined in this specification:

Table 6.2.2-1: Command-Code values for Diameter V2X Inter Control Functions Application

Command-Name	Abbreviation	Code	Clause
ProSe-Authorization-Request	PAR	8388668	6.2.3
ProSe-Authorization-Answer	PAA	8388668	6.2.4

For these commands, the Application-ID field shall be set to 16777356 (application identifier of the Diameter Inter V2X Control Functions interface application, allocated by IANA).

6.2.3 ProSe-Authorization-Request (PAR) Command

The ProSe-Authorization-Request (PAR) Command, indicated by the Command-Code field set to 8388668 and the "R" bit set in the Command Flags field, is sent from the V2X Control Function in the HPLMN to the V2X Control Function in the VPLMN. The ProSe-Authorization-Request (PAR) is originally defined in 3GPP TS 29.345 [17].

Message Format when used over the V6 application:

```
< ProSe-Authorization-Request > ::= < Diameter Header: 8388668, REQ, PXY, 16777356 >
< Session-Id >
[ DRMP ]
[ Vendor-Specific-Application-Id ]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[ Destination-Host ]
{ Destination-Realm }
```

```
*[ Supported-Features ]
[ OC-Supported-Features ]
{ User-Identifier }
{ Visited-PLMN-Id }
*[ AVP ]
*[ Proxy-Info ]
*[ Route-Record ]
```

6.2.4 ProSe-Authorization-Answer (PAA) Command

The ProSe-Authorization-Answer (PAA) Command, indicated by the Command-Code field set to 8388668 and the "R" bit cleared in the Command Flags field, is sent from the V2X Control Function in the VPLMN to the V2X Control Function in the HPLMN. The ProSe-Authorization-Answer (PAA) is originally defined in 3GPP TS 29.345 [17].

Message Format when used over the V6 application:

```
< ProSe-Authorization-Answer > ::=
  < Diameter Header: 8388668, PXY, 16777356 >
  < Session-Id >
  [ DRMP ]
  [ Vendor-Specific-Application-Id ]
  [ Result-Code ]
  [ Experimental-Result ]
  { Auth-Session-State }
  { Origin-Host }
  { Origin-Realm }
  *[ Supported-Features ]
  [ OC-Supported-Features ]
  [ OC-OLR ]
  *[ Load ]
  [ V2X-Authorization-Data ]
  *[ AVP ]
  [ Failed-AVP ]
  *[ Proxy-Info ]
  *[ Route-Record ]
```

6.3 Information Elements

6.3.1 General

The following table (table 6.3.1-1) specifies the Diameter AVPs defined for the V6 interface, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-ID header of all AVPs defined in this specification shall be set to 3GPP (10415).

For all AVPs which contain bit masks and are of the type Unsigned32 e.g., PRR-Flags, bit 0 shall be the least significant bit. For example, to get the value of bit 0, a bit mask of 0x0001 shall be used.

Table 6.3.1-1: V6 specific Diameter AVPs

Attribute Name	AVP Code	Clause defined	Value Type	AVP Flag rules				
				Must	May	Should not	Must not	May Encr.
V2X-Authorization-Data	4700	6.3.2	Grouped					
V2X-Permission-in-VPLMN	4701	6.3.3	Unsigned32					
V2X-Application-Server	4702	6.3.4	Grouped					
NOTE 1: The AVP header bit denoted as "M", indicates whether support of the AVP is required. The AVP header bit denoted as "V" indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see IETF RFC 6733 [3].								
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.								

The following table (table 6.3.1-2) specifies the Diameter AVPs re-used by the V6 interface from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within V6 interface.

Any other AVPs from existing Diameter Applications, except for the AVPs from the Diameter base protocol, do not need to be supported. The AVPs from the Diameter base protocol are not included in table 6.3.1-2.

Table 6.3.1-2: V6 re-used Diameter AVPs

Attribute Name	Reference	Comments	M-bit
Application-Server	3GPP TS 32.299 [14]	See clause 6.3.5	
Geographical-Information	3GPP TS 29.272 [10]	See clause 6.3.6	
Visited-PLMN-Id	3GPP TS 29.272 [10]		
User-Identifier	3GPP TS 29.336 [13]		
User-Name	IETF RFC 6733 [3]		
MSISDN	3GPP TS 29.329 [11]		
Supported-Features	3GPP TS 29.229 [6]		
Feature-List-ID	3GPP TS 29.229 [6]		
Feature-List	3GPP TS 29.229 [6]		
OC-Supported-Features	IETF RFC 7683 [12]	See clause 6.3.7	Must set
OC-OLR	IETF RFC 7683 [12]	See clause 6.3.8	Must set
DRMP	IETF RFC 7944 [15]	See clause 6.3.9	Must not set
Load	IETF RFC 8583 [18]	See clause 6.3.10	Must not set
PC5-RAT-Type	3GPP TS 29.388 [16]	See clause 6.3.11	Must not set
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.			

6.3.2 V2X-Authorization-Data

The V2X-Authorization-Data AVP is of type Group. It shall contain the V2X related authorization data.

AVP format

V2X-Authorization-Data ::= <AVP header: 4700 10415>

[V2X-Permission-in-VPLMN]

*[PC5-RAT-Type]

*[V2X-Application-Server]

*[AVP]

If the V2X-Permission-in-VPLMN AVP indicates V2X communication over PC5 Allowed, the PC5-RAT-Type AVPs may be present to indicate allowed PC5 RAT types to perform communication over PC5 reference point.

If the V2X-Permission-in-VPLMN AVP indicates V2X communication over PC5 Allowed and PC5-RAT-Type AVP is absent, it indicates that all the PC5 RAT types (e.g. PC5 LTE, PC5 NR) are allowed to perform V2X communication over PC5 reference point.

6.3.3 V2X-Permission-in-VPLMN

The V2X-Permission-in-VPLMN AVP is of type Unsigned32 and it shall contain a bit mask that indicates the permissions for V2X service in the visited PLMN for a user. The meaning of the bits shall be as defined in table 6.3.3-1:

Table 6.3.3-1: V2X-Permission-in-VPLMN

Bit	Name	Description
0	V2X communication over PC5 Allowed	This bit, when set, indicates that the user is allowed to use V2X communication over PC5 in the visited PLMN.
1	V2X communication over MBMS Allowed	This bit, when set, indicates that the user is allowed to use V2X communication over MBMS in the visited PLMN.
NOTE: Bits not defined in this table shall be cleared by the V2X Control Function in the VPLMN and discarded by the V2X Control Function in the HPLMN.		

6.3.4 V2X-Application-Server

The V2X-Application-Server AVP is of type Group. It shall contain the identifier of V2X Application Server (e.g. FQDN or IP address), and may contain a list of served geographical area which are associated with the given V2X Application Server.

AVP format

V2X-Application-Server ::= <AVP header: 4702 10415>

{ Application-Server }

*[Geographical-Information]

*[AVP]

6.3.5 Application-Server

The Application-Server AVP is of type UTF8String which is originally defined in 3GPP TS 32.299 [14]. It shall contain the identifier of V2X Application Server (e.g. FQDN or IP address).

6.3.6 Geographical-Information

The Geographical-Information AVP is of type UTF8String which is originally defined in 3GPP TS 29.272 [10]. It shall contain the served geographical area which is associated with a V2X Application Server.

6.3.7 OC-Supported-Features

The OC-Supported-Features AVP is of type Grouped and it is defined in IETF RFC 7683 [12]. This AVP is used to support Diameter overload control mechanism, see Annex A for more information.

6.3.8 OC-OLR

The OC-OLR AVP is of type Grouped and it is defined in IETF RFC 7683 [12]. This AVP is used to support Diameter overload control mechanism, see Annex A for more information.

6.3.9 DRMP

The DRMP AVP is of type Enumerated and it is defined in IETF RFC 7944 [15]. This AVP allows the V2X Control Function to indicate the relative priority of Diameter messages.

6.3.10 Load

The Load AVP is of type Grouped and it is defined in IETF RFC 8583 [18]. This AVP is used to support Diameter load control mechanism, see Annex D for more information.

6.3.11 PC5-RAT-Type

The PC5-RAT-Type AVP (AVP code 4604) is of type Enumerated, it is used to indicate the PC5 radio technology to perform V2X communication over PC5 reference point.

It is defined in 3GPP TS 29.388 [16].

6.4 Result-Code AVP and Experimental-Result AVP Values

6.4.1 General

This clause defines result code values that shall be supported by all Diameter implementations that conform to this specification.

6.4.2 Success

Result codes that fall within the Success category shall be used to inform a peer that a request has been successfully completed. The Result-Code AVP values defined in the Diameter base protocol IETF RFC 6733 [3] shall be applied.

6.4.3 Permanent Failures

6.4.3.1 General

Errors that fall within the Permanent Failures category shall be used to inform the peer that the request has failed, and should not be attempted again. The Result-Code AVP values defined in the Diameter base protocol IETF RFC 6733 [3] shall be applied. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and the Result-Code AVP shall be absent.

6.4.3.2 DIAMETER_ERROR_USER_UNKNOWN (5001)

This result code shall be sent by the HSS to indicate that the user identified by the IMSI is unknown. This error code is defined in 3GPP TS 29.229 [6].

6.4.3.3 DIAMETER_ERROR_UNKNOWN_V2X_SUBSCRIPTION (5690)

This result code shall be sent by the HSS to indicate that no V2X subscription is associated with the IMSI. This error code is defined in 3GPP TS 29.388 [16].

6.4.3.4 DIAMETER_ERROR_V2X_NOT_ALLOWED (5691)

This result code shall be sent by the HSS to indicate that V2X is not allowed to be used in the specific PLMN where the UE is registered. This error code is defined in 3GPP TS 29.388 [16].

Annex A (normative): Diameter overload control mechanism

A.1 General

Diameter overload control mechanism is an optional feature.

IETF RFC 7683 [12] 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 [12] on the V6 interface where, when applied, the requesting V2X Control Function shall behave as a reacting node and the responding V2X Control Function as a reporting node.

A.2 Responding V2X Control Function behaviour

The responding V2X Control Function requests traffic reduction from requesting V2X Control Function when it is in an overload situation, including OC-OLR AVP in answer commands as described in IETF RFC 7683 [12].

The V2X Control Function identifies that it is in an overload situation by implementation specific means. For example, the V2X Control Function may take into account the traffic over the V6 interfaces or other interfaces, the level of usage of internal resources (CPU, memory), the access to external resources, etc.

The V2X Control Function determines the specific contents of OC-OLR AVP in overload reports and the V2X Control Function decides when to send OC-OLR AVPs by implementation specific means.

A.3 Requesting V2X Control Function behaviour

The requesting V2X Control Function applies required traffic reduction received in answer commands to subsequent applicable requests, as per IETF RFC 7683 [12].

Requested traffic reduction is achieved by the requesting V2X Control Function by implementation specific means. For example, it may implement message throttling with prioritization or a message retaining mechanism for operations that can be postponed.

Annex B (Informative): Diameter overload node behaviour

B.1 Message prioritization

This clause describes possible behaviours of the requesting V2X Control Function receiving an overload indication from the responding V2X Control Function, regarding message prioritisation in an informative purpose.

The message prioritization on V6 interface is not applicable in this release.

Annex C (normative): Diameter message priority mechanism

C.1 General

IETF RFC 7944 [15] specifies a Diameter routing 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 and also abatement decisions when overload control is applied.

C.2 V6 interfaces

C.2.1 General

The Diameter message priority mechanism is an optional feature.

It is recommended to make use of IETF RFC 7944 [15] over the V6 interface of an operator network when the overload control defined in Annex A is applied on the V6 interface.

C.2.2 V2X Control Function behaviour

When the V2X Control Function supports the Diameter message priority mechanism over the V6 interface, the V2X Control Function shall comply with IETF RFC 7944 [15]. In particular, when priority is required, the V2X Control Function shall include the DRMP AVP indicating a priority level in the requests it sends, and prioritise received requests according to the priority level received within the DRMP AVP. It shall prioritise received answers according to the priority level received within the DRMP AVP if present, otherwise according to the priority level of the corresponding request. It shall include the DRMP AVP in the answer to a received request if the required priority of the answer is different from the one of the request. The V2X Control Function decisions for a required priority and for the priority level value are implementation specific.

Diameter requests related to high priority traffic should contain a DRMP AVP with a high priority of which the level value is operator dependent.

D.1 General

Diameter load control mechanism is an optional feature.

IETF RFC 8583 [18] specifies a Diameter load control mechanism which includes the definition and the transfer of related AVPs between Diameter nodes.

It is recommended to make use of IETF RFC 8583 [18] on the V6 interface where, when applied, the requesting V2X Control Function shall behave as a reacting node and the responding V2X Control Function as a reporting node.

D.2 Responding V2X Control Function behaviour

The responding V2X Control Function may report its current load by including a Load AVP of type HOST in answer commands as described in IETF RFC 8583 [18].

The responding V2X Control Function calculates its current load by implementation specific means. For example, the responding V2X Control Function may take into account the traffic over the V6 interface or other interfaces, the level of usage of internal resources (e.g. CPU, memory), the access to external resources, etc.

The responding V2X Control Function determines when to send Load AVPs of type HOST by implementation specific means.

D.3 Requesting V2X Control Function behaviour

When performing next hop Diameter Agent selection for requests that are routed based on realm, the requesting V2X Control Function may take into account load values from Load AVPs of type PEER received from candidate next hop Diameter nodes, as per IETF RFC 8583 [18].

Annex E (informative): Change history

Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	New
2016-10	CT4#74bis				Skeleton, implementation of C4-165232, C4-165233	0.1.0
2016-10	CT4#74bis				Editorial correction to the numbering of clauses	0.1.1
2016-11	CT4#75				Implementation of C4-166240	0.2.0
2017-02	CT4#76				Implementation of C4-171300, C4-171302, C4-171304, C4-171036	0.3.0
2017-03	CT#75	CP-170015			Presented for information and approval	1.0.0
2017-03	CT#75				3GPP TS approved in CT#75	14.0.0
2017-06	CT#76	CP-171032	0001	1	Load Control	14.1.0
2017-06	CT#76	CP-171032	0002	1	Remove Editor's Note on V2X Charging	14.1.0
2018-06	CT#80	-	-	-	Update to Rel-15 version (MCC)	15.0.0
2019-09	CT#85	CP-192094	0004	1	draft-ietf-dime-load published as RFC 8583	15.1.0
2020-06	CT#88e	CP-201049	0005	-	Authorized PLMNs and RATs for V2X	16.0.0
2022-04	-	-	-	-	Update to Rel-17 version (MCC)	17.0.0

History

Document history		
V17.0.0	April 2022	Publication