ETSI TR 129 909 V8.1.2 (2009-01)

Technical Report

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
Diameter-based protocols usage and
recommendations in 3GPP
(3GPP TR 29.909 version 8.1.2 Release 8)**

Reference
DTR/TSGC-0329909v812

Keywords
GSM, LTE, UMTS

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

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

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

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

Contents

Foreword

This Technical Report 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.

Introduction

As a new generation AAA (Authentication, Authorization and Accounting) protocol, Diameter has been used widely and will be used more and more widely in 3GPP. Since several 3GPP WGs are developing Diameter based interfaces, e.g. CT3, CT4, etc, so in order to ensure correctness and consistency of using Diameter within all 3GPP WGs, a common set of principles, rules and recommendations across 3GPP WGs are necessary to be given clearly and followed. The present is to describe existing status of Diameter usage within 3GPP, find existing inconsistency of rules used for Diameter based interfaces which were specified in 3GPP and propose common recommendations of using Diameter to all 3GPP WGs to follow.

With more and more Diameter deployment, an inter-operator Diameter signalling network infrastructure will become necessary, so the present document will also study Diameter inter-operator considerations with brief guidelines on how to deploy & realize the inter-operator Diameter-based roaming infrastructure.

1 Scope

The present document contains a common set of principles, rules and recommendations across 3GPP WGs to ensure Diameter-based interfaces have the same treatment for release control and generating new applications-id. Also to address in a unified manner the use/re-use of AVPs, and other Diameter BASE (see IETF RFC 3588 [x]) related decisions.

The present document covers all aspects of Diameter usage within 3GPP, including description of the current situation of Diameter usage in different 3GPP WGs (CT3, CT4, SA5) in Release 6/7, describe recommendations and conditions to re-use existing Diameter applications (3GPP or IETF application-id), commands, AVPs and/or AVP values, describe recommendations and conditions to define new Diameter applications, commands, AVPs and/or AVP values, and any other related issues, e.g. the cross-release issue, whether to apply proposed guideline back to existing Diameter applications or not, or only new SAE Diameter interfaces, etc.

To achieve maximum benefit from this work it is strongly recommended that all 3GPP Diameter-based protocols follow the recommendations in the present document.

The present document also serves a placeholder for Diameter inter-operator considerations with brief guidelines on how to deploy & realize the inter-operator Diameter-based roaming infrastructure.

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] IETF RFC 3588 (September 2003): "Diameter Base Protocol".

[3] IETF RFC 4005 (August 2005): "Diameter Network Access Server Application".

[4] IETF RFC 4006 (August 2005): "Diameter Credit-Control Application".

[5] 3GPP TS 29.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3".

[6] IETF RFC 4072 (August 2005): "Diameter Extensible Authentication Protocol (EAP) Application".

[7] 3GPP TS 32.299: "Diameter charging applications ".

[8] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; Protocol details".

[9] 3GPP TS 29.230: "Diameter applications; 3GPP specific codes and identifiers".

[10] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)"

[11] IETF Draft, "Diameter Base Protocol", draft-ietf-dime-rfc3588bis-08.txt, working in progress.

[12] IETF Draft, "Diameter Applications Design Guidelines", draft-ietf-dime-app-design-guide-03.txt, working in progress.

[13] GSMA PRD IR.34 v4.1, "Inter-Service Provider IP Backbone Guidelines"

[14] GSMA PRD IR.67 v2.1.0, "DNS Guidelines for Operators"

[15] GSMA PRD IR.40 v4.0, "Guidelines for IPv4 Addressing and AS Numbering for GPRS Network Infrastructure and Mobile Terminals"

[16] Void

[17] 3GPP TS 23.003: "Numbering, addressing and identification; Stage 3"

[18] IETF RFC 4282, "The Network Access Identifier"

[19] 3GPP TS 24.234: "3GPP System to WLAN Interworking; UE to Network protocols; Stage 3"

[20] IETF Draft, "Diameter User-Name and Realm Based Request Routing Clarifications", draft-korhonen-dime-nai-routing-02.txt, Work in progress.

3 Definitions, symbols 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].

(none)

3.2 Symbols

For the purposes of the present document, the following symbols apply:

(none)

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].

SAE System Architecture Evolution
SDO Standard Development Organization

4 The status of Diameter in 3GPP

4.1 General

This subclause describes current status of Diameter usage before Release 8 and summarizes some problems of using Diameter protocol to satisfy 3GPP-specific requirements in the past. This subclause is a basis for further discussion to give proposed rules in subclause 5.

4.2 Diameter-based applications before Release 8

Diameter Base Protocol (see IETF RFC 3588 [2]) provides a set of messages and parameters to support AAA-related functionality with built-in protocol management mechanism, e.g. peer discovery, message routing, error handling, etc. Based on Diameter Base Protocol, IETF also defines many Diameter applications to support more specific requirements

in different scenarios, e.g. NASREQ (see IETF RFC 4284 [3]), Diameter Credit Control (see IETF RFC 4006 [4]), etc. Another important feature of Diameter Base Protocol [2] is that it also provides a set of principles and rules for extensibility to support more functionality in the future. That allows other SDOs like 3GPP to define more specific applications, messages, parameters (AVPs) and values to fulfil SDO-specific requirements.

Because of powerful functions and good extensibility, since Release 5, Diameter has been used widely in 3GPP systems, e.g. IMS, GBA, Interworking WLAN, Charging systems, PCC, etc.

The Diameter protocol is designed to be extensible, using several mechanisms, including defining new AVP values, creating new AVPs, creating new Diameter applications, in addition to reuse of existing AVP values, AVPs and Diameter applications (see IETF RFC 3588 [2] for more details).

Based on different principles and requirements, 3GPP WGs, i.e. CT3, CT4 and SA5, develop their Diameter-based interfaces with different approach. Some interfaces are based on existing IETF-defined Diameter applications, for example Wa interface (see 3GPP TS 29.234 [5]) is based on Diameter base protocol (IETF RFC 3588 [2]), NASREQ (IETF RFC 4005 [3]) and Diameter EAP application (IETF RFC 4072 [6]). Some interfaces are based on existing IETF-defined Diameter applications with 3PPP-specific AVPs/Values, for example Ro interfaces (see 3GPP TS 32.299 [7]) is based on Diameter Credit-Control Application (IETF RFC 4006 [4]) with some new 3GPP-specific AVPs. And some interfaces are new 3GPP-specific Diameter applications, e.g. Cx interface specified in 3GPP TS 29.229 [8] which includes 3GPP-specific commands, AVP codes and results codes. 3GPP TS 29.230 [9] serves as a placeholder for all 3GPP-specific Diameter applications, commands, AVP codes and result codes.

4.3 Problem description

During developing Diameter based interfaces, some inconsistent rules are found about how to using Diameter protocol to satisfy 3GPP-specific requirements in different 3GPP WGs. This subclause describes some examples of this issue.

Wx interface, between a 3GPP AAA Server and a HSS, is specified in 3GPP TS 29.234 [5] by CT4. A new application ID is allocated to it as some new AVPs with "M" bit set are added to existing commands, e.g. 3GPP-AAA-Server-Name AVP, WLAN-User-Data AVP, etc.

Wm interface, between a PDG and a 3GPP AAA Server/Proxy, is specified in 3GPP TS 29.234 [5] by CT4. For example, the 3GPP-WLAN-APN-Id AVP, with "M" bit set (see table 10.1.1 in section 10.1, 3GPP TS 29.234 [5]), is a 3GPP-defined AVP and added to AAR command for authorization purpose, but no new application is applied for Wm interface.

Gmb interface, between a GGSN and a BM-SC, is specified in 3GPP TS 29.061 [10] by CT3. A new application ID is allocated to it as some new AVPs with "M" bit set are added to existing commands, e.g. TMGI AVP, Required-MBMS-Bearer-Capabilities AVP, etc.

So it is seen that cross CT WGs there are some inconsistent principles or rules of usage of application IDs and 3GPP-speific AVPs with "M" bit set.

There is another 3GPP-specific issue when Diameter is used in 3GPP, i.e. so-called cross-release issue. New AVPs may be added to the same interface (Diameter Application) in different Releases. If all these AVPs are "M" bit set and added to the same Diameter Application (the same Application ID), inter-operability may occur when equipments following different releases are connected. For the issue, different principles are applied to different interfaces.

One case is AVPs which are added to new release are "M" bit clear. For example, for Release 7 Wm interface, QoS-Auth-Resources AVP is added with "M" bit clear to avoid inter-operability problems. This is similar with Gmb interface. For Gmb interface, a new application ID is allocated to it in Release 6. In Release 7, no new application ID is applied with some new AVPs with "M" bit set, e.g. MBMS-User-Data-Mode-Indication AVP, MBMS-GGSN-Address AVP, etc. In this case the same Application-ID is kept cross releases.

In other cases different application IDs are applied to different releases if there are different AVPs with "M" bit set. For Gx interface, different Application IDs are applied to Release 6 and Release 7 variants due to some new commands and AVPs.

So it is seen that cross CT WGs there are some inconsistent principles or rules for cross-release Diameter applications. And no consensus about how to use "M" bit is reached in the past.

Different principles or rules of Diameter usage across 3GPP WGs may lead to unexpected inter-operability problems as well as confuse developers. From protocol level, Diameter Base protocol has a set of error check and handling

mechanism, that is useful to keep Diameter protocol and applications work correctly and consistently. However some cases above can not utilise these mechanisms, e.g. protocol level error check.

Inconsistent usage of Diameter across WGs may also cause some difficulties for developing a common Diameter software platform to support different applications from development point of view.

So it is necessary to have a common principles or rules of how to use Diameter within 3GPP WGs in CT/SA WGs to satisfy 3GP-specific requirements, including:

- Conditions to re-use existing Diameter applications, commands, AVPs and/or AVP values;
- Conditions to define new Diameter applications, commands, AVPs and/or AVP values;
- The way to resolve cross-release issue;
- Whether to apply proposed guideline back to existing Diameter applications or not, or only new SAE Diameter interfaces and afterwards.
- Etc.

4.4 Existing and ongoing effort

3GPP tried to define some principles of Diameter usage in the past when Cx interface was developed (see subclause 7 of 3GPP TS 29.229 [8]). This can be one input to work of the present technical report.

IETF is also aware of the current limitations of Diameter Base Protocol (see IETF RFC3588 [2]) and is working in a new version of Diameter based protocol (RFC 3588bis, IETF draft, draft-ietf-dime-rfc3588bis [11]). The DIME WG (Diameter Maintenance and Extensions) is working on Diameter application design guidelines [12]. The IETF draft discusses problems about Diameter application design, contradictions and ambiguity when Diameter applications were designed and some guidelines are proposed about reusing existing and/or defining new Diameter applications, commands, AVPs or AVP values.

The outputs of the present TR is expected to be inputs to IETF-related work to work out more accurate guidelines of Diameter usage. 3GPP may also develop more detailed 3GPP-specific rules for Diameter usage based on the guidelines, rules and principles from IETF if needed.

5 Proposed alternatives rules for identified problems

5.1 General

The alternative proposals given in this subclause takes several aspects into account:

- Ongoing work on Diameter application design guidelines in IETF DIME WG [12];
- Ongoing work on Diameter Base Protocol improvement – IETF RFC 3588bis [11];
- Solutions provided in 3GPP R6/R7 to the listed Items about Diameter usage as described in subclause 4.
- New proposals different from the above

In principle, when a proposal to address any of the listed Items is coming by IETF ongoing work it should be the preferred solution to be documented in the conclusion section 6.

NOTE: Any identified problem will have a corresponding sub-clause, which will be introduced as an "Item". For each Item all possible solutions identified will be documented. Therefore clause 5 only contains the list of all alternatives and proposed solutions during the elaboration of the present TR. The final agreed recommendation for 3GPP are listed in clause 6.

5.2 Item 1: Setting of "M" bit on 3GPP defined AVPs

5.2.0 General

This item is about how to set "M" bit in new 3GPP-defined AVPs.

5.2.1 Proposal 1 (IETF)

Follow IETF RFC 3588 procedures on the setting of the M-bit. The Diameter base RFC defines that M-bit shall be set only when it is required to be understood by the receiving peer Diameter node. A Diameter client, server, proxy or translation agent receiving such AVP shall behave according to clause 4.1 of IETF RFC 3588 [2].

NOTE: IETF does not preclude to define the M-bit in the "MAY use" column in the AVP definition.

5.2.2 Proposal 2

"M" bit shall be set in all 3GPP-specific AVPs unless there are necessary reasons to clear the "M" bit in some new defined 3GPP-specific AVPs and it is guaranteed that this will not cause interoperability problems.

NOTE: It is left to the application specification team to define in what kind of necessary reasons the "M" bit can be cleared in a 3GPP-specific AVP.

5.2.3 3GPP evaluation

"M" bit set means: "Support of this AVP is mandatory" (i.e. the entity which receives that AVP must be able to recognize it, parse it, have it defined in its own library of AVPs). "M" bit DOES NOT mean "the AVP is Mandatory in the command or Grouped AVP" (that a frequent mistake/misinterpretation). Adding an AVP to an application (at a command level or nested within a Grouped AVP) with the "M" bit set will create a backward compatibility problem.

This is a generic DIAMETER Rule, 3GPP or any SDO is NOT ALLOWED to change this rule, unless this is discussed at the IETF first.

5.3 Item 2: Re-use of AVPs

5.3.1 General

This item discusses how the already existing AVPs can be used in 3GPP applications. Three points are taken into account here: configuration of the M-bit and whether to use or not the original Vendor-Id and AVP code.

5.3.2 Proposal 1

New or existing Diameter applications incorporate AVPs defined in different Diameter applications. In such a case, the re-used AVPs shall not be modified and shall be configured with the original Vendor-Id, AVP code and M-bit status. In order to support the re-used AVP, during capability negotiation the Supported-Vendor-Id shall be configured to include the vendor-id of the re-used AVPs.

5.3.3 Proposal 2 (IETF)

Vendor-Id and AVP code shall not be modified and shall be used as defined in the AVP's original document. Whether the "M" bit is set or not is based on actual requirements, e.g. support for end-to-end applications capabilities exchange in Diameter application design guidelines [12]. M-bit use is defined by application.

The RFC 3588, Diameter Base Protocol, permits different 'M' bit settings for different situations. The 'M' bit setting is **not** tied to the AVP as such. The purpose of the 'M' bit is to ensure that the receiver must really understand the AVP. RFC 3588 also includes the possibility for the originator to resend the command with failing AVPs omitted if the receiver rejects any AVP with the M-bit set.

5.3.4 3GPP evaluation

Proposal 2 is recommended.

Vendor-Id and AVP code shall not be modified and shall be the same as defined in the original AVP's Application specification. The 'M' bit setting is not tied to the AVP but can be defined on a per-application and per-command basis.

For a re-used AVP, the "M" bit setting in the current application and command shall be considered the same as in the AVP's original specification document, as a default, if there is no specific specification for this shown in the re-used AVP table. For those re-used AVPs which have different "M" bit settings against the originally defined AVPs, a description shall be added in the re-used AVP table to specify the new "M" bit settings.

5.4 Item 3: Version handling

5.4.0 General

This item evaluates the different proposals that 3GPP applications can take in order to use a 3GPP defined protocol (e.g. Gx or Cx protocols) in more than one release. In those cross-Release scenarios, a version handling mechanisms is normally needed.

5.4.1 Proposal 1

Use a new application id for each release as a fixed rule.

For cross-release Diameter applications, at most one new Diameter application id for each 3GPP release may be defined.

5.4.2 Proposal 2

If one or more conditions listed in subclause 5.5.2 about the creation of new applications are true, a new application id shall be defined for an interface in a new release. All of the application identifiers allocated to different releases of the same interface shall be contained in the Vendor-Specific-Application-Id AVP in the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

5.4.3 Proposal 3 - IETF

Follow IETF extensibility rules to assign a new Application Id. (See subclause 5.5.1)

5.4.4 Proposal 4

A proposal that has been followed so far in CT4 based on the definition of a new AVP called Supported-Features AVP (see Cx and Sh applications, subclause 7.2 in 3GPP TS 29.229 [8]). This AVP is complementary to the CER/CEA process and avoids the definition of a new Application Id per release. This AVP was added with the M bit set to Release 6, without changing the Application Id for Cx or Sh, however the handling of the corresponding error (DIAMETER_AVP_UNSUPPORTED) is specified and does not cause interoperability issues.

NOTE: IETF RFC3588 [2] and the current revised version in IETF DRAFT draft-ietf-dime-rfc3588bis [11] do not preclude this possibility. It is true that adding an AVP with the M bit set is indicated as one of the reasons that may lead to change the Diameter Application Id in this paragraph: "*Should a new Diameter usage scenario find itself unable to fit within an existing application without requiring major changes to the specification, it* ***may be desirable*** *to create a new Diameter application. Major changes to an application include: - Adding new AVPs to the command, which have the "M" bit set.*", but the change of application id is only indicated as something that "may be desirable". The first sentence in those two IETF specifications on the other hand indicates that: "*Creation of a new application should be viewed as a last resort.*", and a similar handling of new AVPs with the M bit set within a Diameter application is considered later in the same documents: "*If a message is rejected because it contains a Mandatory AVP which is neither defined in the base Diameter standard nor in any of the Diameter Application specifications governing the message in which it appears, the implementation may resend the message without the AVP, possibly inserting additional standard AVPs instead.*".

5.4.5 Proposal 5

5.4.5.1 General

The AVP use in this proposal extends ideas from the CT4's current handling. It introduces a new Supported – Application-Variant AVP to be negotiated during the Diameter peer connection establishment procedure. The Supported-Application-Variant AVP can only be used for optional extra Releases; new mandatory features will have to be supported with an Application ID upgrade.

The following proposal solves the issue of identifying Application-Ids and releases supported on a hop-by-hop basis as CER/CEA is negotiated with the next hop. Therefore end-to-end negotiation is not covered by this proposal.

New functionality, i.e., functionality beyond the Rel-7 standard, shall be introduced by post-Rel-7 versions of this specification to the Diameter applications as follows:

1) If possible, the new functionality shall be defined optional.

2) If backwards incompatible changes can not be avoided, the new functionality should be introduced as with a new Supported-Application-Variant AVP.

3) If the change would be backwards incompatible, even as if it was defined as a feature, a new version of the interface shall be created by changing the application identifier of the Diameter application per release.

5.4.5.2 Defining new functionality

5.4.5.2.1 General

An application will agree to a base functionality at a Standard level and a release extension will be an extension to that functionality. A new feature is a functional entity that has a significant meaning to the operation of a Diameter application, i.e., defining new optional capabilities. A new Supported-ApplicationVariant AVP will be defined for each version post the frozen versions of the specification.

5.4.5.2.2 Changing the version of the interface

The version of an interface shall be changed by a future release of this specification only if there is no technically feasible means to avoid backwards incompatible changes to the current release of the interface. The versioning of an interface shall be implemented by assigning a new application identifier for the interface. This procedure is in line with the Diameter base protocol (see IETF RFC 3588) which states that if an incompatible change is made to a Diameter application, a new application identifier shall be assigned for the Diameter application.

The following table shall apply to the PCC interfaces. The Application identifier column lists the current application identifiers assigned on 3GPP PCC.

Table 5.2.2.1: Application identifiers used

PCC Interface	Application identifier	First applied
Rx	16777236	3GPP Rel-7
Gx	16777238	3GPP Rel-7

5.4.5.2.3 Capabilities Exchange Request

```
Message Format

      <CER> ::= < Diameter Header : 257, REQ >
                { Origin-Host }
                { Origin-Realm }
```

```
            1* { Host-IP-Address }
               { Vendor-Id }
               { Product-Name }
               [ Origin-State-Id ]
             * [ Supported-Vendor-Id ]
             * [ Supported-Application-Variant]
             * [ Vendor-Specific-Application-Variant]
             * [ Auth-Application-Id ]
             * [ Inband-Security-Id ]
             * [ Acct-Application-Id ]
             * [ Vendor-Specific-Application-Id ]
               [ Firmware-Revision ]
             * [ AVP ]
```

5.4.5.2.4 Capabilities Exchange Answer

```
Message Format

      <CEA> ::= < Diameter Header: 257 >
                { Result-Code }
                { Origin-Host }
                { Origin-Realm }
               1* { Host-IP-Address }
                  { Vendor-Id }
                  { Product-Name }
                  [ Origin-State-Id ]
                  [ Error-Message ]
                * [ Failed-AVP ]
                * [ Supported-Vendor-Id ]
                * [ Supported-Application-Variant]
                * [ Vendor-Specific-Application-Variant]
                * [ Auth-Application-Id ]
                * [ Inband-Security-Id ]
                * [ Acct-Application-Id ]
                * [ Vendor-Specific-Application-Id ]
                  [ Firmware-Revision ]
                * [ AVP ]
```

5.4.5.2.5 AVPs

Table 5.2.5.1.1: Diameter Application AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
Supported-Application-Variant	**XXX**	**5.4.5**	**Unsigned32**	**V**			**M**	**No**
Vendor-Specific-Application-Variant	**XXX**	**5.4.5**	**Grouped**	**V**			**M**	**No**

5.4.5.2.5.1 Supported-Application-Variant AVP

The Vendor-ID header of the AVPs defined in this specification shall be set to 3GPP (10415).

The Supported-Application-Variant AVP is of type Unsigned32. If this AVP is present it may inform the destination host about the releases that the origin host supports.

Where a Supported-Application-Variant AVP is used to identify variant that have been defined by 3GPP, the Vendor-Id AVP shall contain the vendor ID of 3GPP. Vendors may define proprietary variant, but it is strongly recommended that the possibility is used only as the last resort. Where the Supported-Aplication-Variant AVP is used to identify variant that have been defined by a vendor other than 3GPP, it shall contain the vendor ID of the specific vendor in question.

Following values are defined:

- Rx interface –R8 (0)
- Gxa interface – R8 (1)

- Gxb interface – R8 (2)
- Gxc interface – R8 (3)

5.4.5.2.5.2 Vendor-Specific-Application-Variant AVP

The Vendor-Specific-Application-Variant is of type Grouped. This AVP provides a list of features supported on a per vendor basis allowing for the vendors to define vendor specific features.

Vendor-Specifc-Application-Variant::= Grouped <AVP header: XXX>

[Vendor ID]

1 *[Supported-Application-Variant]

5.4.6 3GPP evaluation

The decision to change or not change Diameter application id in each release or even within the same release should be left for the 3GPP WG defining the application. Diameter protocol requirements in the corresponding IETF RFCs shall be followed when taking this decisions and IETF guidance in the corresponding IETF RFCs should be considered as well.

There are two aspects of version handling covered in the proposals to address this item:

- Hop-by-hop version handling: Communicating the supported version to a directly connected Diameter peer at connection time in a CER/CEA exchange.
- End-to-end version handling: Communicating the supported version to a Diameter peer through one or more Diameter agents during an application message exchange.

Proposals 1, 2, 3 and 5 address hop-by-hop version handling and proposal 4 addresses end-to-end version handling.

With respect to hop-by-hop version handling:

- Proposal 1 is discarded, since it creates an unnecessary restriction for new applications and releases.
- Proposal 2 creates unnecessary restriction for new application and releases which shall not be considered as strict requirements for the definition of new applications but left to application specification team to evaluate on different situations. However, the part about including all supported applications in the CER/CEA exchanged in proposal 2 shall be followed.
- Proposal 3 is recommended to be considered as guidelines which provide more flexibility and it is left to the application specification team to evaluate the need of defining new Application Id or creating alternative means to avoid interoperability problems when changes are performed across 3GPP Releases.
- Proposal 5 is useful for application version negotiation on a hop by hop basis in the CER/CEA message exchange.

With respect to end-to-end version handling:

- Proposal 4 is also highly recommended for ease of extensibility of a Diameter Application. Note that the Supported-Feature AVP should be included into every new application where a need for end-to-end version handling has been identified. This method avoids continual updating of the application ID from 3GPP Release to Release. However its drawback is that the features supported are only discovered on the first command pair exchange and not at connection time during the CER/CEA exchange.

5.5 Item 4: Setting of a new Application-Id

5.5.0 General

This item covers the conditions under which a new application-id shall be assigned to an existing protocol.

5.5.1 Proposal 1 - IETF

Follow IETF RFC 3588 guidelines on defining new application id.

According to the IETF draft in [11] defining a new Application Id MAY be desirable when :

- Adding new AVPs to the command which have the "M" bit set
- Requiring a command that has a different number of round trips to satisfy the request
- Adding support for an authentication method requiring definition of new AVPs for use with the application

Additionally a new Application Id MUST be created when

- New commands are added to an existing application

The related excerpts from [11] follow for further reference:

a) Excerpt from section 1.2.4.

> Every Diameter application specification MUST have an IANA assigned Application Id (see Section 2.4 and Section 11.3).Should a new Diameter usage scenario find itself unable to fit withinan existing application without requiring major changes to the specification, it **may be desirable** to create a new Diameter application. Major changes to an application include:
>
> o Adding new AVPs to the command, which have the "M" bit set.
>
> o Requiring a command that has a different number of round trips to satisfy a request (e.g., application foo has a command that requires one round trip, but new application bar has a command that requires two round trips to complete).
>
> o Adding support for an authentication method requiring definition of new AVPs for use with the application. Since a new EAP authentication method can be supported within Diameter without requiring new AVPs, addition of EAP methods does not require the creation of a new authentication application.
>
> Creation of a new application should be viewed as a last resort. An implementation MAY add arbitrary non-mandatory AVPs to a command defined in an application, including vendor-specific AVPs without needing to define a new application. This can be done if the commands ABNF allows for it. Please refer to Section 11.1.1 for details.

b) Excerpt from section 1.2.3.

> A new command should only be created when no suitable command can be reused from an existing application. A new command MUST result in the definition of a new application.

5.5.2 Proposal 2

A new Application-Id shall be defined when one or more of the conditions below are true:

- New AVPs with "M" bit set are defined in a Diameter application;
- New commands are used;
- Existing AVPs are re-used with "M" bit set in a Diameter application;
- New values are added to an existing AVP with "M" bit set in a Diameter application;

NOTE: It is left to the application specification team to define that in the case of no confusion or inter-operability problems caused, whether creation of a new application identifier can be avoided when one or more conditions above are true.

5.5.3 Proposal 3

This proposal mandates the change of the application id whenever any of the bullets in Proposal 1 (IETF one) are fulfilled. I.e. a new Application Id SHALL be created when one or more of the following conditions occur:

- Adding new AVPs to the command which have the "M" bit set
- Requiring a command that has a different number of round trips to satisfy the request
- Adding support for an authentication method requiring definition of new AVPs for use with the application
- New commands are added to an existing application

5.5.4 3GPP evaluation

The decision to change or not change Diameter application id in each release or even within the same release should be left for the 3GPP WG defining the application. Diameter protocol requirements in the corresponding IETF RFCs shall be followed when taking this decisions and IETF guidance in the corresponding IETF RFCs should be considered as well.

Proposal 1 shows some cases where new Application Id might be desirable and just put the requirement to change the Application Id whenever new commands are needed.

Proposal 2 is stricter and additionally requires a change of application whenever any change is made that implies anything with the "M" bit set

Proposal 3 is the "stricter edition" of proposal 1 which shows all cases appeared in proposal 1 and requires changing of Application-Id whenever one or more of those cases happen.

Proposal 1 is preferred and it is left to the application specification team to evaluate the need of defining new Application Id or creating alternative means to avoid interoperability problems when these changes are performed across 3GPP Releases. Additionally cases shown in proposal 2 but not mentioned in proposal 1 should be considered as conditions that new Application-Id might be desirable as well.

NOTE: Hop by hop version negotiation needs further study. There are ongoing disussions in DIME group on this subject.

5.6 Item 5: New Values to an existing enumerated AVP

5.6.1 Proposal 1

Adding new values to an existing AVP with "M" bit set shall lead to creation of a new application identifier.

5.6.2 Proposal 2

If a Diameter peer receives a supported enumerated AVP with some values unknown, the Diameter peer could ignore these unknown values. If the "M" bit is set for the AVP, this might be to indicate that some existing values need to be understood. If some new values are added, a new application identifier is only required if all receivers shall understand them. .

5.6.3 Proposal 3

If a Diameter peer receives a supported enumerated AVP with some values unknown, the Diameter peer could ignore these unknown values. If the "M" bit is set for the AVP, this might be to indicate that some existing values need to be understood. A new application identifier and new AVP code are required only if all receivers shall understand the values that are added.

5.6.4 Proposal 4

New values can be added to an existing AVP that is defined with the M-bit set to "MUST" in earlier releases without having to change the application Id.

If a Diameter node supporting a specific application receives an AVP with the M-bit set with a value that it cannot recognize, the receiving node shall reject the command since it cannot understand a mandatory-to-understand AVP. Moreover the specification where this AVP is used with the new value(s) shall specify the behaviour for the originator when this situation occurs, e.g. by specifying that the originator shall issue the command again but according to an earlier release of the application.

NOTE: It is left to the application specification team to define What happens when the AVP is received in the answer instead of the request. However, in that case the receiver shall find a way to inform the sender.

5.6.5 Proposal 5

If a new value is added to an AVP such that it changes the semantics of the application using it, the application specification team shall increase the application version using the appropriate version handling procedure described in section 5.4.6 (Item 3: Version Handling). For example, a new AVP value can be considered to have changed the semantics if the application specification has normative statements that refer to the new value.

5.6.6 3GPP evaluation

The RFC 3588, Diameter Base Protocol, does not preclude adding new enumerated values to be defined for an AVP that has the "M" bit set if it is justified in certain specific situations (see e.g. Data-Reference AVP in 3GPP TS 29.328).

Proposal 1 and proposal 2 are discarded, since proposal 1 creates an unnecessary restriction for adding new values to an existing AVP with "M" bit set and proposal 2 is covered by proposal 3

Proposal 3 and proposal 4 document the preferred methods for how the receiving node deals with the unknown values in the AVPs with "M" bit set and flexibility is left to the protocol specification team to evaluate these. Proposal 3 is a restricted proposal and proposal 4 is more flexible but needs more handling at application level to specify the behaviours in the case of unknown values.

Proposal 5 is the recommended method for evaluating the impact of the new AVP value on the application version.

5.7 Item 6: Re-use of commands in new applications

5.7.0 General

This item is to discuss how to use the application identifier AVPs (Auth-Application-Id AVP, Vendor-Specific-Application-Id AVP, Acct-Application-Id AVP) in commands from pre-existing applications that are re-used in new 3GPP-specific applications.

5.7.1 Proposal 1

When a new 3GPP specific application has been allocated with a new application id and it also reuses existing commands with or without modifications, it shall use the newly allocated application id in the message header and in all relevant application id AVPs (Auth-Application-Id, Acct-Application-Id or Vendor-Specific-Application-Id AVP) present in the message body of the re-used command.

5.7.2 3GPP evaluation

Proposal 1 is recommended.

6 Conclusion

This TR has studied alternative solutions for some inconsistant rules used by different 3GPP WGs during development of Diameter based interfaces and has proposed a common set of principles, rules and recommendations across 3GPP WGs to ensure Diameter-based interfaces have the similar treatment for release control and generation of new application Ids. It also addresses common ways for the use/reuse of AVPs and other Diameter BASE related decisions.

The setting of the 'M' bit in new 3GPP-defined AVPs shall follow the generic Diameter Rule described in the 3GPP evaluation (see clause 5.2.3).

Three points are taken into account on how to reuse the existing AVPs in 3GPP applications for the configuration of the M-bit and whether to use or not, the original Vendor-Id and AVP code. The IETF proposal is adopted that Vendor-Id and AVP code shall not be modified and shall be the same as defined in the AVP's Application specification. The 'M' bit setting is not tied to the AVP but can be defined on a per-application and per-command basis (see clause 5.3.4).

For the version handling issue, the decision to change or not to change Diameter application id in each release or even within the same release is finally agreed to be left for the 3GPP WGs, defining the application, in order to be flexible. However, to ensure the decisions made by different 3GPP WGs are consistent, Diameter protocol requirements and IETF guidance in the corresponding IETF RFCs shall be followed when making these decisions. (Details see clause 5.4.6).

The consideration of conditions under which a new Application Id shall be assigned to an existing protocol provides an agreement to follow the mechanism that IETF uses (see clause 5.5.1).

For the item of New Values being applied to an existing enumerated AVP, The IETF does not preclude adding new enumerated values for an AVP that has the 'M' bit set. Hence, proposals are made on how the Diameter nodes should deal with the unknown value in a received pre-existing enumerated AVP with 'M' bit set. The recommendation is made by balancing flexibility and inter-operability (see clause 5.6.6).

For re-use of commands in new applications, it is agreed to use the newly allocated Application-Id in the message header and all the relevant Application-Id AVPs present in the message body of the re-used command no matter if the command is re-used, with or without modification.

To achieve maximum benefit from this work, this report recommends all 3GPP Diameter-based protocols to apply the evaluated guidelines for new Diameter interfaces and future releases. It also serves as a placeholder for Diameter multi-vendor considerations with brief guidelines on how to deploy and realize the inter-operator Diameter-based roaming infrastructure.

Annex A (Informative): Roaming Infrastructure

A.0 General

The subclause proposes brief guidelines on how to deploy & realize the inter-operator Diameter-based roaming infrastructure.

A.1 Deployment of S6a-Diameter Relay Pools

This annex provides an example of a deployment of S6a-Diameter relay pools to be used between a visited and home operator. This deployment may also be applied to the intra-operator scenario as well.

At a high level, the Diameter infrastructure needed for a multi-operator scenario comprises the intra-operator infrastructure of each involved network operator, and an inter-operator infrastructure shared by the involved network operators. The inter-operator infrastructure could be the evolution of the existing GPRS Roaming Exchange i.e. the IPX [13]. This is depicted below.

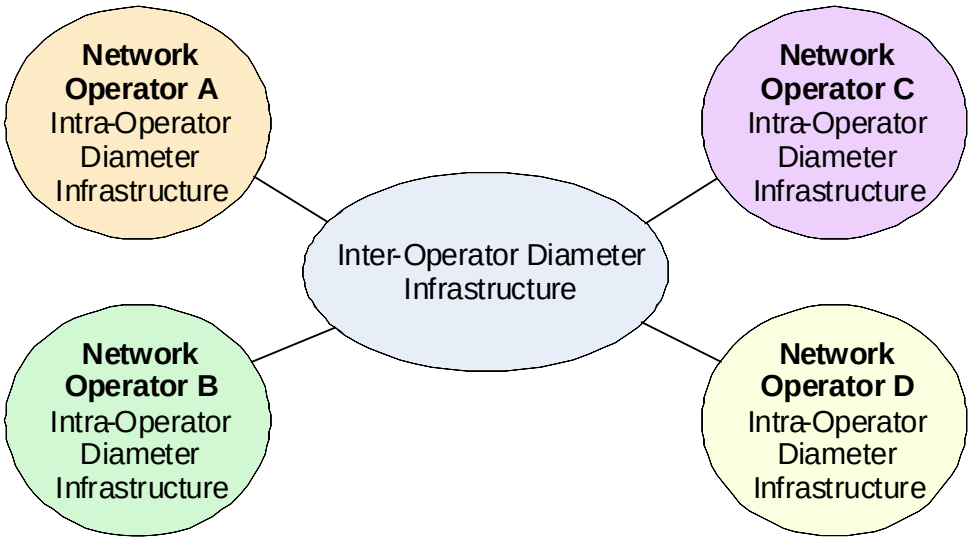

Figure A.1.1: High-level Diameter Infrastructure

For the intra-operator infrastructure it is suggested to make use of:

- An inner pool of relay agents to provide service within the operator network: The inner pool of relay agents has Diameter connections to HSS. A plain pool where each relay has a connection to HSS is possible. Alternatively, a hierarchical pool is also possible, with a first level of relays that have connections to the MMEs and a second level of relays with connection to HSS, where each relay in the second level groups connections from the first level relays, so that the number of connections to HSS can be reduced. The inner pool of relay agents has Diameter connections to a border pool of relay agents.

- A border pool of relay agents to interface with the inter-operator Diameter infrastructure: The border pool of relay agents has Diameter connections to an inner pool of relay agents. The border pool of relay agents has Diameter connections to the inter-operator Diameter infrastructure.

This is exemplified in the following figure A.1.2.

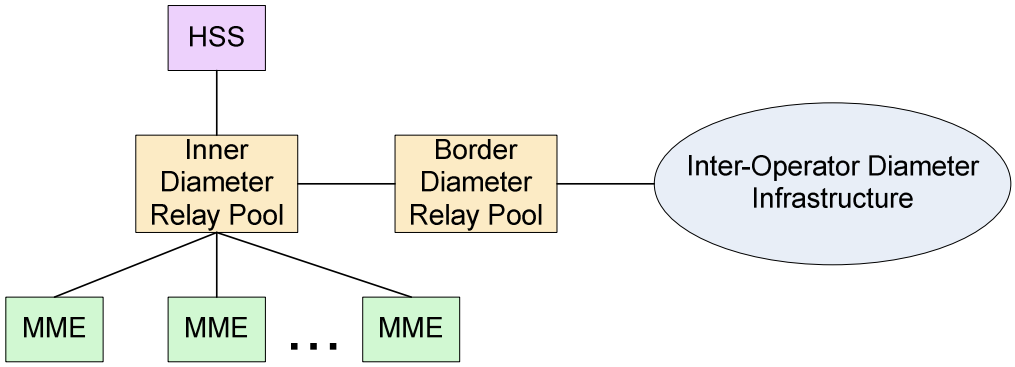

Figure A.1.2: Example Intra-Operator Diameter Infrastructure and its connectivity to inter-operator Diameter roaming infrastructure

Observe that several variations over the example presented here are possible. For example, the functions of the inner and the border pools of relay agents could be combined in a single pool, or different relay pools could be used for separate geographical areas.

For the inter-operator infrastructure it is proposed to use a hierarchical deployment of relay pools, so that:

- First level relay pools have Diameter connections to the different intra-operator infrastructures. Each first level relay pool provides service to a number of intra-operator infrastructures, e.g. based on geographical location.
- Each intra-operator infrastructure obtains service from at least one relay pool, and at least two separate relay agents.
- Groups of interconnected first level relay pools are possible.
- When a first level relay pool receives a request:
    - If the destination realm corresponds to a network operator for which the pool has a Diameter connection, then the request can be directly forwarded to the corresponding intra-operator infrastructure.
    - If not, then if the destination realm corresponds to a network operator for which an interconnected first level relay pool has a Diameter connection, the request can be forwarded to that interconnected first level relay pool.
    - Otherwise, the request is forwarded to a higher order relay pool.
- As many hierarchical levels as needed are possible.
- Similar principles to the ones described above are applied at all levels of the hierarchy, in order to find the optimum route to the destination intra-operator infrastructure.

This is exemplified in the following figure A.1.3.

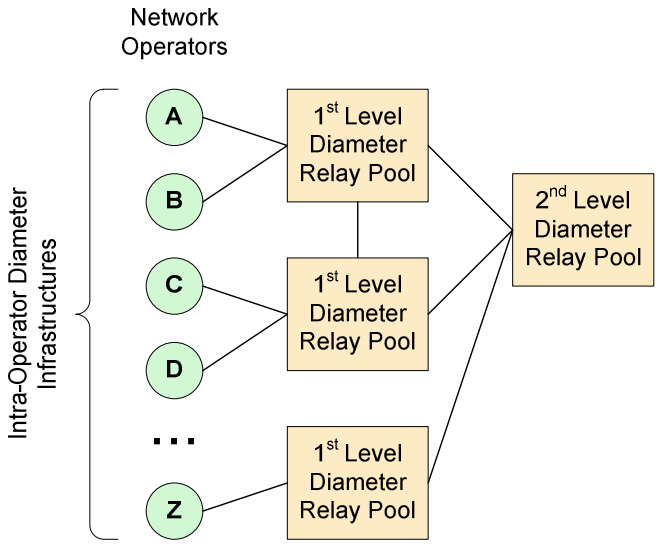

Figure A.1.3: Example Inter-Operator Diameter Infrastructure for S6a, S9 and Wd* interfaces

A.2 Deployment of S9 and Wd*-Diameter Relay Pools

This annex provides a short description of a deployment of S9 and Wd*-Diameter relay pools to be used between a visited and home operator. S9 (for PCC) and Wd* (for I-WLAN) interfaces can reuse the Diameter infrastructure deployed for S6a purposes.

S9 and Wd* Diameter usage differs from S6a usage only on two aspects. First both S9 and Wd* Diameter interfaces are only used for inter-operator roaming purposes. Second within the operator internal Diameter infrastructure peer nodes are different than the HSS. In case of S9 Diameter infrastructure connects to a PCRF and in case of Wd* to a 3GPP AAA Server/Proxy. However, the Diameter infrastructure needed for S9 and Wd* intra- and especially inter-operator purposes can be exactly the same than described in sub-clause A.1 for S6a. An example deployment is shown below.

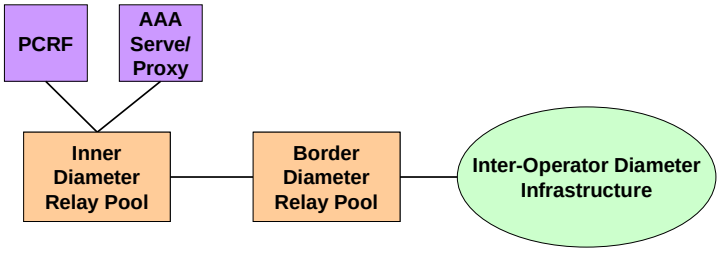

Figure A.2.1: Example of PCRF and AAA Server/Proxy connecting to inter-operator Diameter roaming infrastructure

A.3 Guidelines for connecting to the inter-operator Diameter infrastructure

This annex provides guidelines on connecting operator's internal Diameter infrastructure to the inter-operator Diameter infrastructure.

Past work on Diameter and various identities in 3GPP assume that the inter-operator IP backbone for roaming is the evolution of GPRS Roaming Exchange i.e. the IPX [3]. When connecting to the inter-operator IP backbone the rules defined in IR.34 [13], IR.67 [14] and IR.40 [15] shall be followed. From Diameter point of view this concerns addressing of the border relay agents and DNS naming of Diameter agents.

A.4 Void

Annex B (Normative): Diameter routing extensions

B.0 General

This sub-clause gives additional guidance to the Diameter Base Protocol [11] on the Diameter request routing.

B.1 Realm-based routing

The use of the Destination-realm AVP is specified in RFC 3588 as the valid realm the message is to be routed to. The realm field is used as primary key in lookups in the realm-based routing table. Diameter peers shall make use of the realm field in order to route Diameter requests. A Diameter peer obtains the valid realm to send requests to from the realm field in the User-Name AVP if this is a NAI.

B.2 NAI decoration

The User-Name AVP is a Diameter request message may contain a decorated NAI. The NAI decoration mechanism is defined in IETF RFC 4282 [18], further clarified in IETF Draft draft-korhonen-dime-nai-routing [20] and in 3GPP scope defined in 3GPP TS 23.003 [17]. All Diameter agents that participate in the message request routing should support decorated NAIs in the User-Name AVP and modifications to the Destination-Realm AVP as described in IETF Draft draft-korhonen-dime-nai-routing [20]. However, the decorated NAI routing mechanism may be overruled by local configuration/policy.

B.3 Explicit routing

If the network architecture requires a deployment of stateful Diameter agents, then the actual network deployment shall ensure that all Diameter messages belonging to the same user session traverse through the same stateful agents. Such explicit routing requirement may, for example, be satisfied by a network configuration.

B.4 Preserving the User-Name AVP

It is strongly recommended that the User-Name AVP is present in every request message for 3GPP applications, for example, due to possible request routing related reasons as described in sub-clauses B.1 and B.2. Unless there is a strong reason otherwise, for example, due to identity hiding, the User-Name AVP should also be used as the primary information element for the subscriber look-ups by the Diameter agents.

In specific cases, Diameter agents perform subscriber look-ups based on AVPs other than the User-Name AVP, such as the Subscription-Id AVP for instance. However in these scenarios it may be desirable to keep the User-Name AVP when the request is likely to traverse basic Diameter agents that make realm-based routing decisions based on User-Name AVP.

Annex C:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2007-09					The initial draft v0.0.0		0.0.0
2007-10					Contents of subclause introduction, 1, 2, 3, and 4 are incorporated based on e-mail discussion.	0.0.0	0.1.0
2007-11					The approved tdoc C3-070963, C3-071001, C3-071159 at CT3 #46 are incorporated into v0.1.0.	0.1.0	0.2.0
2008-01					The approved tdoc C3-080167, C3-080215, C3-080216 at CT3 #47 are incorporated into v0.2.0.	0.2.0	1.0.0
2008-04					The approved tdoc C3-080390, C3-080394, C3-080400, C3-080401, C3-080402, C3-080456, C3-080457 at CT3 #47bis are incorporated into v1.0.0.	1.0.0	1.1.0
2008-05					The approved tdoc C3-080829 at CT3#48 are incorporated into v1.1.0	1.1.0	1.2.0
2008-06					The approved tdoc C3-081189(C4-081971), C3-081190(C4-081972), C3-081191(C4-081993), C3-081243(C4-081970) at CT#48bis are incorporated into v1.2.0	1.2.0	1.3.0
2008-08					The agreed tdoc C3-081325, C3-081552 at CT3#49 are incorporated into v1.3.0	1.3.0	1.4.0
2008-09					Version 2.0.0 created for presentation to TSG by MCC	1.4.0	2.0.0
2008-09	TSG#41				Version 8.0.0 created by MCC	2.0.0	8.0.0
2008-12	TSG#42	CP-080755	001	2	Clean up of TR 29.909	8.0.0	8.1.0
2008-12	TSG#42	CP-080755	002	1	Routing and preserving the User-Name	8.0.0	8.1.0
2008-12	TSG#42	CP-080755	003		Principle for the "M" bit setting in re-used AVP tables	8.0.0	8.1.0
2009-01					Verson 8.1.1 created by MCC due to editorial correction	8.1.0	8.1.1
2009-01					Minor cosmetic corrections	8.1.1	8.1.2

History

Document history		
V8.1.2	January 2009	Publication