



## **Implementation Agreement for the DB-0 Interface**

**MSF-IA-DIAMETER.002-FINAL**

# MultiService Forum Implementation Agreement

**Contribution Number:** msf2006.047.01

**Document Filename:** MSF-IA-DIAMETER.002-FINAL

**Working Group:** Protocol and Control

**Title:** Implementation Agreement for the DB-0 Interface

**Editor:** Dan Warren, Vodafone

**Contact Information:** Tel - +44 7795 300783

e-mail – dan.warren@vodafone.com

**Working Group Chairperson:** Chris Gallon, Fujitsu

**Date:** 19 May 2006

**Abstract:** As part of GMI 2006, MSF is defining network elements and interfaces that draw heavily on the definition of IMS as defined in Release 6 of 3GPP specifications. This part of the GMI 2006 architecture thus has considerable similarity to the 3GPP architecture itself and so the interfaces that 3GPP define can be greatly re-used and need only minor modifications to become applicable to their equivalent interfaces in GMI 2006. Amongst the interfaces in GMI 2006 IMS are a number that connect to the HSS and, where required, the SLF. Addressed in this IA are those reference points to the HSS and SLF that are similar to the Cx and Dx interfaces defined in 3GPP TS 29.228 [1] and 3GPP TS 29.229 [2] – specifically the DB-0 interface between the S-CSC and HSS (and SLS where required) and between the I-CSCF and HSS (and SLS where required).

The MultiService Forum (MSF) is responsible for developing Implementation Agreements, Product Specifications or Architectural Frameworks, which can be used by developers and network operators to ensure interoperability between components from different vendors. MSF Implementation Agreements, Product Specifications and Architectural Frameworks are formally ratified via a Straw Ballot and then a Principal Member Ballot. Draft MSF Implementation Agreements, Product Specifications and Architectural Frameworks may be published before formal ratification via Straw or Principal Member Ballot. In order for this to take place, the MSF Technical Committee must formally agree that a draft Implementation Agreement, Product Specifications or Architectural Framework should be progressed through the balloting process. A Draft MSF Implementation Agreement, Product Specification or Architectural Framework is given a document number in the same manner as an Implementation Agreement. Draft Implementation Agreements, Product Specifications or Architectural Frameworks may be revised before or during the full balloting process. The revised document is allocated a new major or minor number and is published. The original Draft Implementation Agreement, Product Specifications or Architectural Framework remains published until the Technical Committee votes to withdraw it. After being ratified by a Principal Member Ballot, the Draft Implementation Agreement, Product Specifications or Architectural Framework becomes final. Earlier Draft Implementation Agreements, Product Specifications or Architectural Frameworks remain published until the Technical Committee votes to withdraw them.

The goal of the MSF is to promote multi-vendor interoperability as part of a drive to accelerate the deployment of next generation networks. To this end the MSF looks to adopt pragmatic solutions in order to maximize the chances for early deployment in real world networks.

To date the MSF has defined a number of detailed Implementation Agreements and detailed Test Plans for the signaling protocols between network components and is developing additional Implementation Agreements and Test Plans addressing some of the other technical issues such as QoS and Security to assist vendors and operators in deploying interoperable solutions.

The MSF welcomes feedback and comment and would encourage interested parties to get involved in this work program. Information about the MSF and membership options can be found on the MSF website <http://www.msforum.org/>

**DISCLAIMER**

The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and the MultiService Forum is not responsible for any errors or omissions. The MultiService Forum does not assume any responsibility to update or correct any information in this publication. Notwithstanding anything to the contrary, neither the MultiService Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind whether based on theories of tort, contract, strict liability or otherwise, shall be assumed or incurred by the MultiService Forum, its member companies, or the publisher as a result of reliance or use by any party upon any information contained in this publication. All liability for any implied or express warranty of merchantability or fitness for a particular purpose is hereby disclaimed.

The receipt or any use of this document or its contents does not in any way create by implication or otherwise:

Any express or implied license or right to or under any MultiService Forum member company's patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

Any warranty or representation that any MultiService Forum member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor

Any commitment by a MultiService Forum company to purchase or otherwise procure any product(s) and/or service(s) that embody any or all of the ideas, technologies, or concepts contained herein; nor

Any form of relationship between any MultiService Forum member companies and the recipient or user of this document.

Implementation or use of specific MultiService Forum Implementation Agreements, Architectural Frameworks or recommendations and MultiService Forum specifications will be voluntary, and no company shall agree or be obliged to implement them by virtue of participation in the MultiService Forum.

**For addition information contact:**

MultiService Forum  
39355 California Street, Suite 307  
Fremont, CA 94538  
USA  
Phone: +1 510 608-5922  
Fax: +1 510 608-5917  
[info@msforum.org](mailto:info@msforum.org)  
<http://www.msforum.org>

## I. Introduction

Within the MSF Release 3 Architecture in MSF-ARCH-003.00-FINAL [3] for GMI 2006, a number of devices that can be seen to be either identical or very similar to those defined in 3GPP IMS architecture (see 3GPP TS 23.228 [4]) are identified. Within MSF-ARCH-003.00-FINAL [3], a number of new IA's are also identified and in some cases, these IA's refer closely to 3GPP reference points or interfaces. This IA addresses one such 3GPP defined interface and the equivalent interface that requires an IA – the 3GPP Cx interface and the DB-0 interface within the MSF architecture.

The HSS is a 3GPP defined element where subscriber information relating to identity, contactability, service preferences and other subscription information relating to IMS and other 3GPP defined network domains is stored (see 3GPP TS 23.002 [5]). The Subscriber Location Function (SLF) in 3GPP is defined as a Diameter redirect that is used in networks where more than one HSS has been deployed. Nodes wishing to contact the HSS that holds subscription records for a specific subscriber send their requests to the SLF first, where the correct HSS address for the subscriber is inserted into the message. The SLF then returns the message to the node, which can then route the message to the correct HSS. Figure I.1 below shows the Interfaces defined for GMI 2006 to the HSS and to the SLS (the MSF equivalent of the SLF), including the DB-0 interface to the S-CSC and the I-CSC.

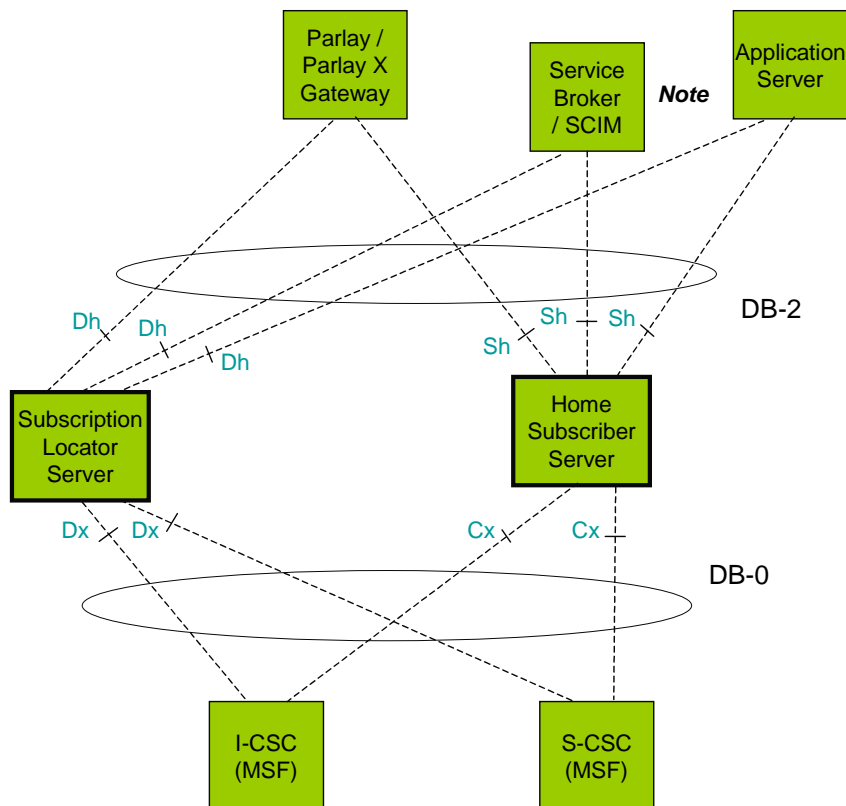


Figure I.1: Reference points to the HSS

Cx and Dx interfaces in 3GPP is identified in 3GPP TS 23.002 [5], have requirements for it's functionality defined in 3GPP TS 23.228 [4], and have the protocol implementation on the interface defined in 3GPP TS 29.228 [1] and 3GPP TS 29.229 [2]. They are specified as a Vendor specific application that is implemented on the DIAMETER Base Protocol (RFC3588 [6]). The DB-0 interface has very similar requirements and so can draw almost entirely on the 3GPP documents for definition.

#### I.A. References

- [1] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx interface; signalling flows and message contents".
- [2] 3GPP TS 29.229: "Cx Interface based on Diameter – Protocol details".
- [3] MSF-ARCH-003.00-FINAL: "MSF Release 3 Architecture".
- [4] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – Stage 2".
- [5] 3GPP TS 23.002: "Network architecture".
- [6] IETF RFC3588: "Diameter Base Protocol".
- [7] 3GPP TS 29.230: "Diameter applications; 3GPP specific codes and identifiers".
- [8] ETSI TS 183 033: "Endorsement of 3GPP TS.29.228 (Release 6) and TS.29.229 (Release 6)".

## II. General on Diameter Cx Application

The protocol used on the Cx and Dx interfaces within 3GPP is defined as a Vendor-Specific Diameter Application. This means that implementations of the Cx and Dx interfaces need to support the Diameter Base Protocol as described in RFC3588 [6].

### II.A. Identification of the Cx Application

At establishment of a Diameter Session, Diameter Base Protocol (RFC3588 [6]) requires the two nodes engaging in the session to send Capability-Exchange-Request/Answer (CER/CEA) message pairs to establish which Diameter Applications can be used within that Session. When Cx Application is to be used, the nodes SHALL include the application identification of the Cx Application as described in 3GPP TS 29.230 [7].

Because Cx Application is defined by 3GPP, the nodes SHALL include the IANA allocated vendor identity for 3GPP (10415) within an instance of the Supported-Vendor-Id AVP in the CER/CEA exchange, as well as the Cx Application identity, see section 5.6 of 3GPP TS 29.229 [2]. The description for how vendor identity information is transported in Diameter messages, AVPs and in the CER/CEA exchange is defined in RFC3588 [6].

The implication of this is that manufacturers implementing the DB-0 interface SHALL include the 3GPP Vendor Identity in an instance of the Supported-Vendor-Id AVP of their CER/CEA implementations.

#### *II.A.1. Identification of extensions to the Cx Application*

Diameter Base Protocol (RFC3588 [6]) provides the possibility for individual vendors to extend applications in 'proprietary' ways. This is done by identifying the specific Vendor by use of the Vendor-Id AVP as described in RFC3588 [6].

TISPAN has used this mechanism to define extensions to the 3GPP Cx application. When TISPAN defined extensions are used on the Cx interface, the ETSI vendor identity (13019) also SHALL be included in an instance of the Supported-Vendor-Id AVP in the CER/CEA exchange so that extensions using the vendor identity are advertised as being available for use, and AVP's utilized in the extension include the ETSI Vendor Identity in their structure (as described in RFC3588 [6]). When a Cx interface implementation does not advertise the ETSI Vendor Identity in the CER/CEA exchange at the initiation of a Diameter session, any AVP's that include the ETSI vendor identity SHALL be ignored, as described in RFC 3588 [6]. ETSI extensions to Cx application are defined in ETSI TS 183 033 [8].

### III. Cx Interface Profile

Unless stated, implementation of DB-0 interface in MSF GMI 2006 architecture SHALL be in accordance with definitions in 3GPP TS 29.228 [1] and 3GPP TS 29.229 [2].

Note: The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", "OPTIONAL", "CONDITIONAL" and "IF" in this document are to be interpreted as described in the Technical Committee Operating Procedures.

#### III.A. DB-0 Interface between S-CSC and HSS

##### III.A.1. *Commands*

The DB-0 Interface between S-CSC and HSS SHALL implement the following commands;-

- Server-Assignment-Request/Answer (SAR/SAA) command pair as defined in 3GPP TS 29.228 [1] section 6.1.2.
- Registration-Termination-Request/Answer (RTR/RTA) command pair as defined in 3GPP TS 29.228 [1] section 6.1.3.
- Push-Profile-Request/Answer (PPR/PPA) command pair as defined in 3GPP TS 29.228 [1] section 6.2.2.
- Multimedia-Auth-Request/Answer (MAR/MAA) command pair as defined in 3GPP TS 29.228 [1] section 6.3.

##### III.A.1.a) Additional Authentication Methods

MSF implementations of the MSF R3 architecture MAY require support of additional authentication methods beyond those defined by 3GPP. In 3GPP Release 6, the only authentication technique defined by 3GPP is Digest-AKAv1-MD5. To support this authentication type, message contents for the MAR/MAA command pair SHALL be implemented as defined in section 6.3 of 3GPP TS 29.228 [1], whilst the content of the SIP-Auth-Data-Item AVP included in the MAA message SHALL be as defined in Table 6.3.5, section 6.3 of 3GPP TS 29.228 [1] and section 6.3.13 of 3GPP TS 29.229 [2].

The MAR/MAA command pair is defined in such a way that additional Authentication schemes can be easily added to Cx Interface Application. SIP-Auth-Data-Item AVP is structured as a nested AVP meaning that the content of the AVP can be altered without impacting the top level structure of the MAA command itself. Therefore, for the MSF to define an additional authentication mechanism, the impact that this will have on the Cx Interface is;-

- Define the new identification for the authentication mechanism to be included in the SIP-Authentication-Scheme AVP (see section 7.9.2 of 3GPP TS 29.228 [1])

- Define AVP's to be include in the nested SIP-Auth-Data-Item AVP which will have content to allow the S-CSCF to authenticate the subscriber. These AVP's SHALL include the Vendor Identity for the MSF (24411) within the Vendor-Id AVP.
- Define the mechanism by which re-authentication can occur for that authentication scheme, in situations where synchronization between user equipment and network is misaligned (if required).
- The MSF Vendor Identity SHALL be included in the Supported-Vendor-Id AVP in the CER/CEA exchange at Diameter session initiation (see RFC3588 [6]).

It should be noted that ETSI TISPAN have defined an additional authentication technique in ETSI TS 183 033 [8] – authentication using NASS Bundling. If this authentication technique is to be supported by the implementation of the DB-0 interface, NASS Bundling authentication information SHALL be implemented as defined in ETSI TS 183 033 [8] and the CER/CEA exchange to establish in the Diameter Session for the Cx application SHALL include the ETSI vendor identity (13019) within an instance of the Supported-Vendor-Id AVP, in accordance with RFC3588 [6].

Within ETSI TS 183 033 [8], TISPAN have also defined how authentication information related to using HTTP Digest can be communicated over the Cx interface. Again, this is defined as an ETSI specific extension and hence requires the ETSI vendor identity to be included in the associated AVP's and the CER/CEA exchange at Diameter Session Initiation. This is however only included in an Informative annex of the TS. If used by an MSF implementation of the DB-0 interface, HTTP Digest authentication information SHALL be implemented as defined in ETSI TS 183 033 [8] and the CER/CEA exchange to establish in the Diameter Session for the Cx application SHALL include the ETSI vendor identity (13019) within an instance of the Supported-Vendor-Id AVP, in accordance with RFC3588 [6].

### III.B. DB-0 Interface between I-CSC and HSS

#### III.B.1. *Commands*

- The DB-0 Interface between I-CSC and HSS shall implement the following commands;- User-Authentication-Request/Answer (UAR/UAA) command pair as defined in 3GPP TS 29.228 [1] section 6.1.1.
- Location-Info-Request/Answer (LIR/LIA) command pair as defined in 3GPP TS 29.228 [1] section 6.1.4.

### III.C. DB-0 Interface between S-CSC and SLS

#### III.C.1. *Commands*

The DB-0 Interface between S-CSC and HSS and between S-CSC and SLS SHALL implement the following commands;-

- Server-Assignment-Request (SAR) command as defined in 3GPP TS 29.228 [1] section 6.1.2.
- Multimedia-Auth-Request (MAR) command as defined in 3GPP TS 29.228 [1] section 6.3.

NOTE: Only Request messages are sent to the SLS. The SLS only inserts the HSS address information in the Diameter message header, to allow the S-CSC to route the request to the correct HSS for the subscriber whom the request relates to.

### III.D. DB-0 Interface between I-CSC and SLS

#### *III.D.1. Commands*

The DB-0 Interface between I-CSC and HSS shall implement the following commands;-

- User-Authentication-Request (UAR) command as defined in 3GPP TS 29.228 [1] section 6.1.1.
- Location-Info-Request (LIR) command as defined in 3GPP TS 29.228 [1] section 6.1.4.

NOTE: Only Request messages are sent to the SLS. The SLS only inserts the HSS address information in the Diameter message header, to allow the I-CSC to route the request to the correct HSS for the subscriber whom the request relates to.