IPTV Remote Management Implementation Agreement

MSF-IA-HTTPs.001-FINAL

MultiService Forum
Implementation Agreement

Contribution Number: msf2008.163.04
Document Filename: MSF-IA-HTTPs.001-FINAL
Working Group: Management
Title: Implementation Agreement for IPTV Remote Management
Editor: Dawn Xie, ZTE Inc.
dawnxie@zteusa.com

Contributors:

Shan Wey	Nokia Siemens Networks	shan.wey@nsn.com
Lily Chen	Verizon	lily.f.chen@core.verizon.com
Te-Sheng Lin	Verizon	te-sheng.lin@verizon.com
George Yum	Verizon	takkin.g.yum@verizon.com

Working Group Chairperson: Lily Chen
Date: August 4th, 2008

Abstract:

The MultiService Forum (MSF) is responsible for developing Implementation Agreements or Architectural Frameworks which can be used by developers and network operators to ensure interoperability between components from different vendors. MSF Implementation Agreements are formally ratified via a Straw Ballot and then a Principal Member Ballot.

Draft MSF Implementation Agreements or Architectural Framework 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 or Architectural Framework should be progressed through the balloting process. A Draft MSF Implementation Agreement or Architectural Framework is given a document number in the same manner as an Implementation Agreement.

Draft Implementation Agreements 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 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 or Architectural Framework becomes final. Earlier Draft Implementation Agreements or Architectural Frameworks remain published until the Technical Committee votes to withdraw them.

The use of capitalization of the key words “MUST”, “SHALL”, “REQUIRED”, “MUST NOT”, “SHOULD NOT”, “SHOULD”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY” or “OPTIONAL” is as described in section V-B of the MSF Technical Committee Operating Procedures.

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/

Note: Attention is called to the possibility that use or implementation of this MSF Implementation Agreement may require use of subject matter covered by intellectual property rights owned by parties who have not authorized such use. By publication of this Implementation Agreement, no position is taken by MSF as its Members with respect to the existence or validity of any intellectual property rights in connection therewith, nor does any warranty, express or implied, arise by reason of the publication by MSF of this Implementation Agreement. Moreover, the MSF shall not have any responsibility whatsoever for determining the existence of IPR for which a license may be required for the use or implementation of an MSF Implementation Agreement, or for conducting inquiries into the legal validity or scope of such IPR that is brought to its attention.

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
48377 Fremont Blvd., Suite 117
Fremont, CA 94538 USA
Phone: +1 510 492-4050
Fax: +1 510 492-4001
info@msforum.org
http://www.msforum.org

I. The MultiService Forum

The MultiService Forum (MSF) is a global association of service providers, system suppliers and other organizations committed to developing and promoting open-architecture, multiservice communication systems. Founded in 1998, the MSF is an open-membership organization comprised of the world's leading telecommunications companies.

The MSF's activities include developing implementation agreements, promoting worldwide compatibility and interoperability, and encouraging input to appropriate national and international standards bodies.

As part of MSF’s effort to drive and promote interoperability, the MSF has created a number of programs geared toward accelerating real world network deployments:

1. Global MSF Interoperability (GMI) events. GMI events provide a real-world setting for vendors to test their solutions and provide evidence that vendor products meet the interoperability standards set forth by MSF Implementation Agreements. Each MSF GMI event is built around a set of capabilities defined for a given release of the MSF Architecture.

2. Next Generation Network (NGN) Test Bed. The NGN test bed provides a facility to enable carriers and vendors to perform in-depth testing of a specific interface as defined in a given release of the MSF architecture.

3. Certification Programs. For more mature technologies the MSF can provide Certification of compliance to a given Implementation Agreement where MSF members believe that it is of value to the industry to do so.

II. An introduction to MSF documentation and GMI 2008

This document is part of the MSF Release 4 set of architectural, protocol and test documentation.

The MSF Release 4 Architecture is a physical implementation of the functional architectures that have been proposed by the key Standards Development Organizations. As such the MSF Release 4 Architecture represents the current state of the industry and it identifies current open interfaces between physically separate network elements.

MSF Implementation Agreements define the protocols to be used over specific open interfaces. Where possible MSF Implementation Agreements are based on industry standard protocols augmented with additional information so as to ensure interoperability between communicating network elements. This level of interoperability is achieved by closing any gaps and tightening any optional capabilities in those industry standards to remove the danger of mutually incompatible selections by vendors. An MSF Implementation Agreement is targeted at a given release of the MSF architecture but can be used in any circumstance where an operator wishes to deploy the open interface and its functionality within their own network.

The MSF Release 4 architecture and its associated implementation agreements are used as the basis for GMI 2008. GMI 2008 is a global test event executed to demonstrate multi-vendor, multi-service interoperability based around IMS and includes IPTV and web based services.

As part of GMI 2008 a number of detailed test scenarios have been developed and a number of test plans defined. Test plans contain the set of test cases required to demonstrate a given MSF Release 4 capability and serve to exercise and validate the set of Implementation Agreements required to realize the capability.

Following the completion of GMI 2008 the MSF Release 4 architecture and individual implementation agreements will be updated if the testing identifies any deficiencies in the documents.

For more information about the scope of GMI2008 please go to http://www.msforum.org

III. Impact on previously published MSF documents

This is a new specification for MSF release 4 and GMI 2008.

1. Introduction

This document specifies the implementation agreement of interface Mi-2, the interface to accomplish IPTV STB remote management.

The following IPTV architecture, recognized by MSF Architecture R4.0, includes the Mi-2 interface:

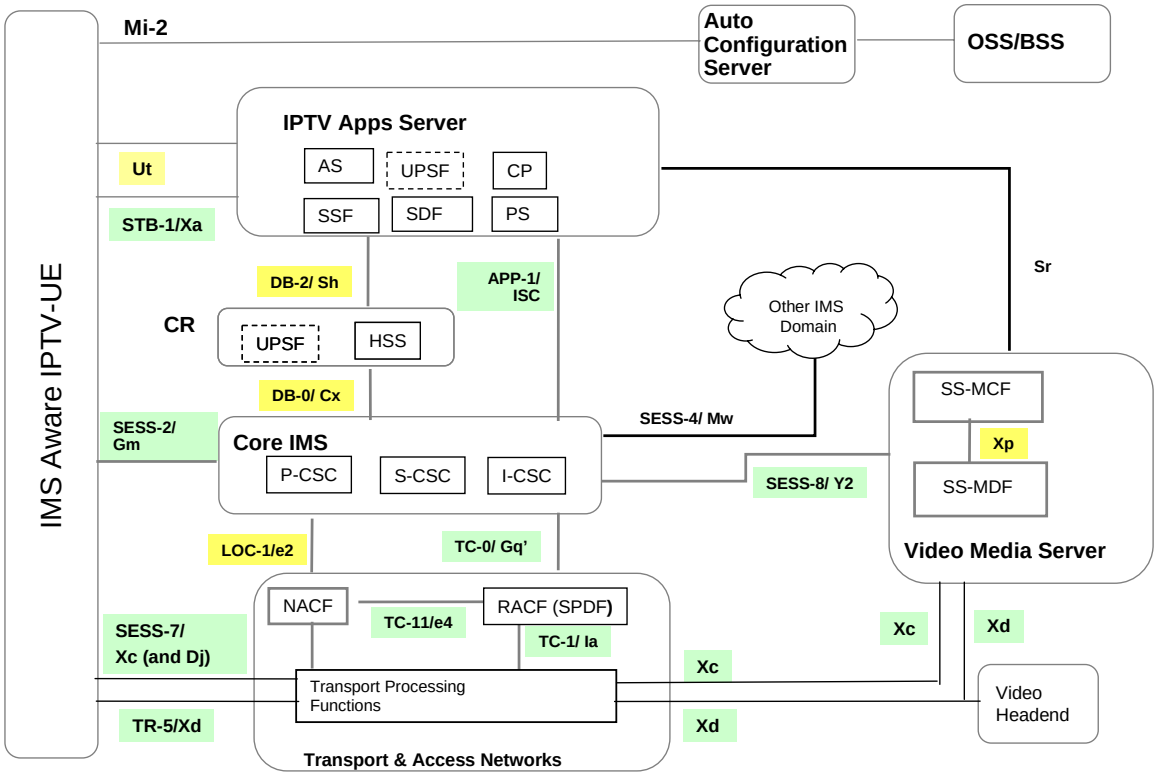

Figure 1: MSF IPTV Architecture

The architecture does not reflect an IGD (Internet Gateway Device) between the IPTV-UE (i.e. Set Top Box) and the IPTV core functions, nor between the IPTV-UE and Auto-Configuration Server (ACS). Although an IGD may be used in the GMI IPTV IOT network, this architectural view assumes a direct logical connection between the IPTV-UE and ACS.

There is also no interaction between the Mi-2 interface and the rest of interfaces in the diagram. The other interfaces are related to media and signaling control and transport, while Mi-2 is for the management plane.

The Mi-2 interface can be tested independently to the rest of the interfaces. It does not rely on the User Agent supporting IMS. However, since the planned GMI2008 IPTV interoperability testing is IMS-based, in order to participate in both IMS-IPTV and IPTV remote management interoperability testing, the User Agent needs to support IMS.

The interface between ACS and OSS/BSS is out of scope for this implementation agreement.

The following text uses phrase STB (Set Top Box) inter-exchangeable with phrase IPTV User Agent.

2. Implementation Agreement

Mi-2 interface will conform to DSL Forum's TR069 [1] [2] and TR135 [3] specifications.

Mi-2 interface shall support HTTPS option of TR069, to ensure secure communication between ACS and STB.

TR069 [1] [2] describes the CPE WAN Management Protocol (CWMP), intended for communication between a CPE and Auto-Configuration Server (ACS). The CPE WAN Management Protocol defines a mechanism that encompasses secure auto-configuration of a CPE, and also incorporates other CPE management functions into a common framework.

TR135, *Data Model for a TR-069 Enabled STB*, defines the data model for remote management of Digital Television (IPTV or broadcast) functionality on STB devices via CWMP as defined in [1] and [2]. It covers the data model for describing an STB device as well as rules regarding notifications on parameter value change. General use cases are also described including standard data model profiles that would typically be seen while remotely managing a device of this nature.

The current version of TR135 does not include management objects for SIP protocol, used in IMS-based IPTV service provisioning. The future version of TR-135 shall include specification for SIP management support. Presently, it is out of scope for this implementation agreement.

By implementing TR135, a management server (i.e. Auto Configuration Server) is able to capture the capabilities of the managed STB, perform performance monitoring, and fault and trouble management. This document describes the implementation agreement to achieve the interoperability in the mentioned management areas:

- Configuration Management
- Performance Monitoring
- Fault and Trouble Management

It is important to point out that the implementation agreement defined here is different to the functions accomplished by the *IPTV Application Server*, which is also part of the IPTV solution. *IPTV Application Server* performs service provisioning and monitoring, while the *ACS* performs network and device management. For example, the interaction between the STB and *IPTV Application Server* starts, terminates, modifies or monitors the IPTV services. The *ACS* performs configuration, fault and performance management for the STB components, such as its video decoder, audio decoder, IP front end, and protocols, such as IGMP, RTP protocols.

3. Configuration Management

A TR-069 and TR-135 enabled STB supports these configuration capabilities:

1. Able to construct a data instance following TR-135 data model. ACS obtains this data instance from the STB to determine the capabilities of the STB and construct the corresponding data instance in its own database.
2. Able to support STB and component configuration change requests, received from ACS. Note these configuration change requests (e.g. enable or disable a component) are typically for fault or performance management of the STB.

A STB shall support these profiles defined in TR-135, for configuration management:

- Baseline Profile
- IPTVBaseline Profile
- RTCP Profile
- RTPAVPF Profile
- IPTVHomeNetwork Profile
- IGMP Profile

4. Performance Monitoring

TR-135 defines these profiles for performance management:

- BasicPerfMon Profile
- ECPerfMon Profile
- VideoPerfMon Profile
- AudioPerfMon Profile
- AudienceStats Profile

However, this implementation agreement is about interoperability testing, not about capability or performance testing of STB. So instead of requiring participating STB to support all the performance parameters defined in TR-135, following are the more focused requirements:

- A STB shall support the performance monitoring mechanism defined in TR-135 [3] section I.3, using the ServiceMonitoring object.
- A STB shall support these objects in BasicPerfMon profile:
    - .STBService.{i}.ServiceMonitoring.MainStream.{i}.
        - Enable
        - Status
        - ServiceType
        - AVStream
    - .STBService.{i}.ServiceMonitoring.MainStream.{i}.Total.
        - Reset
        - ResetTime
    - .STBService.{i}.ServiceMonitoring.MainStream.{i}.Total.VideoReponseStats.
        - MinimumVideoSystemResponse
        - MaximumVideoSystemResponse
    - .STBService.{i}.ServiceMonitoring.MainStream.{i}.Sample.
        - SampleSeconds
        - SignificantChanges
    - .STBService.{i}.ServiceMonitoring.MainStream.{i}.Sample.VideoReponseStats.
        - SampleSeconds
        - AverageVideoSystemResponse
        - MinimumVideoSystemResponse
        - MaximumVideoSystemResponse

The interoperability testing of STB performance monitoring aims to verify the capabilities listed above, and to evaluate the impact of implementing the performance management mechanism on a STB.

Note: The vendor STB implementation should not use the above selected parameters as implementation guidance. The STB implementation should comply with TR-135 recommendation.

5. Fault and Trouble Management

A TR-069 enabled STB shall support these standard fault and trouble management capabilities:

1. **Show fault conditions**: An ACS may use GetParameterValues method to obtain the value of one or more STB parameters, to detect STB faulty states.
2. **Automatically notify fault conditions**: An ACS may use SetParameterAttributes to modify attributes associated with one or more STB Parameter. One of the attributes is Notification, which indicates the actions STB should take when the value of the parameter changes. A STB may then call the Inform method to initiate a transaction sequence after a session with an ACS is established.
3. **Change STB and component configuration**: An ACS may use SetParameterValues method to modify the value of one or more STB Parameters.
4. **Upgrade software/firmware**: An ACS may use Download method to cause the STB to download a specified file from the designated location, to perform software/firmware upgrade.
5. **Reboot:** This method causes the STB to reboot, and should be used with extreme caution. The STB MUST send the response and complete the remainder of the session prior to rebooting. This method is primarily intended for troubleshooting purposes. This method is *not* intended for use by an ACS to initiate a reboot after modifying the CPE's configuration (e.g., setting STB parameters or initiating a download). If a STB requires a reboot after its configuration is modified, the STB MUST initiate that reboot on its own after the termination of its session with ACS.
6. **Reset to factory default configuration:** This method resets the CPE to its factory default state, and should be used with extreme caution. The CPE MUST initiate the factory reset procedure only after successful completion of the session.

For bullet 1 and 2, TR-135 specifies these status objects that ACS may poll to determine the STB fault condition, or trig STB to automatically report status change through notification. A STB shall support these status objects:

- Baseline Profile:
  - .STBService.{i}.Components.FrontEng.{i}.Status
  - .STBService.{i}.Components.FrontEng.{i}.IP.Inbound.{i}.Status
  - .STBService.{i}.Components.FrontEng.{i}.IP.Outbound.{i}.Status
  - .STBService.{i}.Components.AudioDecode.{i}.Status
  - .STBService.{i}.Components.VideoDecoder.{i}.Status
  - .STBService.{i}.Components.AudioOutput.{i}.Status
  - .STBService.{i}.Components.VideoOutput.{i}.Status
  - .STBService.{i}.AVStreams.AVStream.{i}.Status
  - .STBService.{i}.AVPlayers.AVPlayer.{i}.Status
- RTCP Profile:
  - .STBService.{i}.Components.FrontEng.{i}.IP.RTCP.Status
- RTPAVPF Profile:
  - .STBService.{i}.Components.FrontEng.{i}.IP.RTPAVPF.Status
- IGMP Profile:
  - .STBService.{i}.Components.FrontEng.{i}.IP.IGMP.Status

- BasePerfMon Profile
  - .STBService.{i}.ServiceMonitoring.MainStream.{i}.Status

For bullet 3, TR-135 specifies the following objects that ACS may set in order to recover faults:

1. Disable and enable the STB components, by setting "Enable" object:
   - RTCP Profile:
     - .STBService.{i}.Components.FrontEng.{i}.IP.RTCP.Enable
   - RTPAVPF Profile
     - .STBService.{i}.Components.FrontEng.{i}.IP.RTPAVPF.Enable
   - IGMP Profile
     - .STBService.{i}.Components.FrontEng.{i}.IP.IGMP.Enable:
2. Change RTCP transmission repeat interval:
   - .STBService.{i}.Components.FrontEng.{i}.IP.RTCP.TxRepeatInterval
3. Configure RTP AVPF
4. Enable IGMP logging
5. Configure IGMP QoS and VLAN marking, robustness and unsolicited report interval
6. Configure IP front end dejittering buffer
7. Force an IP Front End to connect to a specific service for troubleshooting, by setting .STBService.{i}.Components.FrontEnd.{i}.IP.ServiceConnect.URL
8. Configure Audio output level and mute setting
9. Configure Video output format
10. Configure AV player's preferred audio and subtitle language
11. Change service monitoring sampling parameters

However, this implementation agreement is about interoperability testing, not about checking the STB functionality completeness. So instead of requiring participating STB to support all the capabilities listed above, following are the required set:

- Configure Audio output level and mute setting
- Configure Video output format
- Configure AV player's preferred audio and subtitle language

Note: The vendor STB implementation should not use the above selected scenarios as implementation guidance. The STB implementation should comply with TR-135 recommendation.

6. Abbreviations

ACS	Auto-Configuration Server
BSS	Business Support Systems
CWMP	CPE WAN Management Protocol
IGD	Internet Gateway Device
IOT	Interoperability Test
OSS	Operation Support Systems
STB	Set-top Box

7. References

[1] TR-069 Amendment 1, *CPE WAN Management Protocol*, DSL Forum Technical Report
[2] TR-106 Amendment 1, *Home Network Data Model Template for TR-069-Enabled Devices*, DSL Forum Technical Report
[3] TR-135, *Data Model for a TR-069 Enabled STB*, DSL Forum Technical Report

[4] MSF 2008.104, Test Plan for IPTV STB Remote Management
[5] MSF 2008.045, MSF R4 Physical Architecture