Document Number: DSP0232

Date: 2009-10-16

Version: 1.0.1

DASH Implementation Requirements

Document Type: Specification

Document Status: DMTF Standard

Document Language: E

CONTENTS

Tables

74

Foreword

The *DASH Implementation Requirements* (DSP0232) was prepared by the Desktop and Mobile Working Group of the DMTF.

DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability.

Acknowledgments

The authors wish to acknowledge the following people.

Editors:

- Joe Kozlowski – Dell Inc.
- Steven Breed – Dell Inc.

Contributors:

- Stephen Fong – Advanced Micro Devices
- Bob Blair – Advanced Micro Devices
- Paul Vancil – Advanced Micro Devices
- Simon Assouad – Broadcom Corporation
- Murali Rajagopal – Broadcom Corporation
- Hemal Shah – Broadcom Corporation
- Jon Hass – Dell Inc.
- Rick Landau – Dell Inc.
- Christoph Graham – Hewlett-Packard
- Jeff Hilland – Hewlett-Packard
- David Hines – Intel Corporation
- Joel Clark – Intel Corporation
- Andy Currid – NVIDIA Corporation
- Steve Hand – Symantec Corporation
- Jim Davis – WBEM Solutions

Introduction

This specification describes the conformance requirements for implementing the Desktop and Mobile Architecture for System Hardware (DASH) version 1.0.

DASH Implementation Requirements

1 Scope

This document describes the requirements for implementing the Desktop and Mobile Architecture for System Hardware version 1.0. This document does not define the implementation requirements directly. In clause 5, the mandatory specifications to be implemented are defined. In clauses 6, 7, 8, 9, and 10 the optional and conditional specifications are defined.

2 Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

2.1 Approved References

DMTF DSP0136, *Alert Standard Forma*t Specification *2.0*,
http://www.dmtf.org/standards/documents/ASF/DSP0136.pdf

DMTF DSP0226, *Web Services for Management 1.0*,
http://www.dmtf.org/standards/published_documents/DSP0226_1.0.pdf

DMTF DSP0227, *WS-Management — CIM Binding Specification 1.0*,
http://www.dmtf.org/standards/published_documents/DSP0227_1.0.pdf

DMTF DSP0230, *WS-CIM Mapping Specification 1.0,*
http://www.dmtf.org/standards/published_documents/DSP0230_1.0.pdf

DMTF DSP1009, *Sensors Profile 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1009_1.0.pdf

DMTF DSP1011, *Physical Asset Profile 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1011_1.0.pdf

DMTF DSP1012, *Boot Control Profile 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1012_1.0.pdf

DMTF DSP1013, *Fan Profile 1.0,*
http://www.dmtf.org/standards/published_documents/DSP1013_1.0.pdf

DMTF DSP1015, *Power Supply Profile 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1015_1.0.pdf

DMTF DSP1022, *CPU Profile 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1022_1.0.pdf

DMTF DSP1023, *Software Inventory Profile 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1023_1.0.pdf

DMTF DSP1026, *System Memory Profile 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1026_1.0.pdf

DMTF DSP1027, *Power State Management Profile 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1027_1.0.pdf

DMTF DSP1033, *Profile Registration Profile 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1033_1.0.pdf

DMTF DSP1034, *Simple Identity Management Profile 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1034_1.0.pdf

DMTF DSP1039, *Role Based Authorization Profile 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1039_1.0.pdf

DMTF DSP1054, *Indications Profile 1.0,*
http://www.dmtf.org/standards/published_documents/DSP1054_1.0.pdf

DMTF DSP1058, *Base Desktop and Mobile Profile 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1058_1.0.pdf

DMTF DSP8007 *Platform Message Registry 1.0,*
http://schemas.dmtf.org/wbem/messageregistry/1/dsp8007.xml

IETF RFC 2246, T. Dierks et al., *The TLS Protocol Version 1.0*, http://www.ietf.org/rfc/rfc2246.txt

IETF RFC 3268, P. Chown, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*, http://www.ietf.org/rfc/rfc3268.txt

IETF RFC 4301, S. Kent, *Security Architecture for the Internet Protocol*,
http://www.rfc-editor.org/rfc/rfc4301.txt

IETF RFC 4303, S. Kent, *IP Encapsulating Security Payload*, http://www.ietf.org/rfc/rfc4303.txt

IETF RFC 4106, J. Viega and D. McGrew, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*, http://www.rfc-editor.org/rfc/rfc4106.txt

2.2 Other References

ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*,
http://isotc.iso.org/livelink/livelink.exe?func=ll&objId=4230456&objAction=browse&sort=subtype

3 Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

3.1
can
used for statements of possibility and capability, whether material, physical, or causal

3.2
cannot
used for statements of possibility and capability, whether material, physical, or causal

3.3
conditional
indicates requirements to be followed strictly in order to conform to the document when the specified conditions are met

3.4
mandatory
indicates requirements to be followed strictly in order to conform to the document and from which no deviation is permitted

3.5
may
indicates a course of action permissible within the limits of the document

3.6
need not
indicates a course of action permissible within the limits of the document

3.7
optional
indicates a course of action permissible within the limits of the document

3.8
shall
indicates requirements to be followed strictly in order to conform to the document and from which no deviation is permitted

3.9
shall not
indicates requirements to be followed in order to conform to the document and from which no deviation is permitted

3.10
should
indicates that among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required

3.11
should not

indicates that a certain possibility or course of action is deprecated but not prohibited

4 Symbols and Abbreviated Terms

The following symbols and abbreviations are used in this document.

4.1
ASF
Alert Standard Format

4.2
IANA
Internet Assigned Numbers Authority

4.3
IP
Internet Protocol

4.4
MAC
Media Access Control

4.5
MAP
Management Access Point

4.6
RMCP
Remote Management and Control Protocol

4.7
TCP
Transmission Control Protocol

4.8
TLS
Transport Layer Security

4.9
UDP
User Datagram Protocol

4.10
URI
Uniform Resource Identifier

4.11
WS
Web Services

5 Mandatory Profiles and Specifications

The mandatory profiles and specifications shown in Table 1 shall be implemented in accordance with this specification.

Table 1 – Mandatory Profiles and Specifications

Name	Number	Version	Description
Base Desktop and Mobile Profile	DSP1058	1.0	
WS-Management Specification	DSP0226	1.0	
WS-Management — CIM Binding Specification	DSP0227	1.0	
WS-CIM Mapping Specification	DSP0230	1.0	
Role Based Authorization Profile	DSP1039	1.0	
Simple Identity Management Profile	DSP1034	1.0	
Profile Registration Profile	DSP1033	1.0	

6 Optional Profiles

The optional profiles shown in Table 2 may be implemented. When a profile is implemented, the requirements specified in this section shall be met.

Table 2 – Optional Profiles

Name	Number	Version	Description
Boot Control Profile	DSP1012	1.0	
CPU Profile	DSP1022	1.0	
Fan Profile	DSP1013	1.0	
Indications Profile	DSP1054	1.0	An instance of one of the concrete subclasses of CIM_Indication shall be the payload of a WS-Eventing message. The contents for AlertIndication should be drawn from *Platform Message Registry* DSP8007. It is recommended that any vendor-specific messages are formulated with a published message registry with the owning entity other than the DMTF.
Physical Asset Profile	DSP1011	1.0	
Power State Management Profile	DSP1027	1.0	
Power Supply Profile	DSP1015	1.0	
Sensors Profile	DSP1009	1.0	
Software Inventory Profile	DSP1023	1.0	
System Memory Profile	DSP1026	1.0	

7 Protocol Implementation Requirements

A DASH-compliant implementation shall use a CIM-based data model for representing managed resources and services. This section describes the Management Protocol and Transport Protocol requirements for a DASH implementation.

7.1 Management Protocol

It is mandatory for DASH implementations to use the protocol defined in *Web Services for Management Specification* (DSP0226) as the management protocol for supporting operations. The implementation of the Web Services for Management protocol shall expose CIM schema.

7.1.1 XML Namespaces

The following URI identifies an XML namespace that contains DASH-specific XML definitions

```
(1)    http://schemas.dmtf.org/wbem/dash/1/dash.xsd
```

7.1.2 WS-Transfer

It is mandatory for DASH implementations to support WS-Transfer as described in clause 7 of DSP0226. Table 3 defines support for WS-Transfer operations and their respective DASH requirements.

262 **Table 3 – WS-Transfer Operations**

Operation	Requirement	Notes
Get	Mandatory	This operation retrieves resource representations.
Put	Conditional	This operation updates resources. If an implemented profile requires ModifyInstance support, the Put operation shall be supported to fulfill that requirement.
Create	Conditional	This operation creates resource instances. If an implemented profile requires CreateInstance support, the Create operation shall be supported.
Delete	Conditional	This operation deletes resources. If an implemented profile requires DeleteInstance support, the Delete operation shall be supported.

263 ### 7.1.3 WS-Enumeration

264 It is mandatory for DASH implementations to support WS-Enumeration as described in clause 8 of
265 DSP0226. Table 4 defines support for WS-Enumeration operations and their respective DASH
266 requirements.

267 **Table 4 – WS-Enumeration Operations**

Operation	Requirement	Messages
Enumerate	Mandatory	This operation is used to initiate an enumeration and receive an enumeration context.
Pull	Mandatory	This operation is used to pull a sequence of elements of a resource.
Renew	Optional	See Rule R8.1-4 in DSP0226. Implementation of this operation is not recommended.
GetStatus	Optional	See Rule R8.1-4 in DSP0226. Implementation of this operation is not recommended.
Release	Mandatory	This operation is used to release an enumeration context.
EnumerationEnd	Optional	See Rule R8.1-4 in DSP0226. Implementation of this operation is not recommended.

268 It is recommended that the wsman:OptimizeEnumeration option be implemented as a child element of the
269 wsen:Enumerate element. Refer to clause 8.2.3 of DSP0226 for details. The service must accept the
270 element, but it does not have to honor it as described in Rule R8.2.3-1 of DSP0226.

271 #### 7.1.3.1 WS-Enumeration Filter Dialects

272 It is recommended for DASH implementations to support Selector Filter Dialect for filtered enumeration
273 and subscription as described in Annex E of DSP0226. This recommendation does not contravene
274 Rule R8.2.1-5 of DSP0226.

275 It is optional for DASH implementations to support *Association Queries* with the dialect filter URI as
276 specified in DSP0227.

277 It is optional for DASH implementations to support the CQL filter dialect for enumeration as described in
278 clause 8.1 of DSP0227. This clause does not contravene Rule R8.2.1-5 of DSP0226.

279 ### 7.1.4 WS-Eventing

280 Support for WS-Eventing is conditional. A service advertising conformance to the *Indications Profile*
281 (DSP1054) shall support WS-Eventing as described in clause 10 of DSP0226 and further constrained by
282 the definition described in this section 7.1.4. Table 5 defines support for WS-Eventing operations and
283 their respective DASH requirements.

284 **Table 5 – WS-Eventing Operations**

Operation	Requirement	Notes
Subscribe	Mandatory	
Renew	Mandatory	
Unsubscribe	Mandatory	
SubscriptionEnd	Optional	
GetStatus	Optional	See Rule R10.3-1 in DSP0226. Implementation of this operation is not recommended.

285 #### 7.1.4.1 WS-Eventing Messaging Security

286 For WS-Eventing the messaging security defined in Table 6 should be followed.

287 **Table 6 – WS-Eventing Message Security Recommendations**

Plane	WS-Eventing Message	Recommended Security Class	Security Principal Requiring Authentication
Control	wse:Subscribe	Class B as defined in section 8.1, because it can carry sensitive information	Subscriber
	wse:Renew	Class B, because it can carry sensitive information	Subscriber
	wse:SubscriptionEnd	Class B, because it can carry sensitive information	Subscriber
	wse:Unsubscribe	Class B, because it can carry sensitive information	Subscriber
Delivery	wse:Delivery (Push)	Class A or B as defined in section 8.1 (B for sensitive information or for more compute-intensive information)	MAP, but not necessarily with its own credentials
	wse:Delivery (PushWithAck)	Class A or B (B for sensitive information)	MAP, but not necessarily with its own credentials
	wse:Delivery (Batched)	Class A or B (B for sensitive information)	MAP, but not necessarily with its own credentials
	wsen:Pull (Pull delivery)	Class A or B (B for sensitive information)	Subscriber

7.1.4.2 WS-Eventing Delivery Mode

DASH implementations shall support WS-Eventing Push Mode as described in clause 10.2.9.2 of DSP0226. DASH implementations should support WS-Eventing PushWithAck Mode as described in clause 10.2.9.3 of DSP0226.

7.1.4.3 Subscription Related Property Definition Guidance

The PersistenceType property in a CIM_ListenerDestination instance created internally in response to wse:Subscribe should be set to 3 (Transient).

The value for the FailureTriggerTimeInterval property on the CIM_IndicationSubscription or CIM_FilterCollectionSubscription instance created internally in response to wse:Subscribe should be to 30 seconds.

7.2 Transport Protocol

DASH implementations shall use HTTP 1.1 as the SOAP transport for DSP0226. For detailed information about the transport protocol required by DASH, refer to section 5.2 of the *Desktop and Mobile Systems Management White Paper* (DSP2014).

8 Security Implementation Requirements

This section describes transport requirements, roles and authorization, user account management, and authentication.

8.1 Transport Requirements

DASH defines two security classes for HTTP 1.1 transport:

1) **Class A**: The security class A requires HTTP digest authentication for the user authentication. For this class, no encryption capabilities are required beyond the encryption of the password during the digest authentication exchange. If class A is implemented, MD5 digest algorithm shall be supported. The SHA-1 digest algorithm may be supported.

   - String = "HTTP_DIGEST"
     - URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest

2) **Class B**: This class defines three security profiles that are based on either TLS or IPsec with specifically selected modes and cryptographic algorithms. For class B compliance, the support for at least one of the following security profiles is mandatory:

   - String = "HTTP_TLS_1"
     - URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest
   - String = "HTTP_TLS_2"
     - URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic
   - String = "HTTP_IPSEC"

     For this profile IPsec provides both machine-level authentication and encryption services and HTTP digest provides user-level authentication.
     - URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest/ipsec

A DASH implementation shall support at least one of the preceding security classes. It is recommended that a DASH implementation be Class B compliant for privacy/confidentiality and additional security.

326 Refer to 7.1.4.1 for WS-Eventing security requirements.

327 8.1.1 Cryptographic Algorithms and Cipher Suites

328 Table 7 lists the required cryptographic algorithms or cipher suites for the security profiles mentioned in
329 this section.

330 **Table 7- Required Cryptographic Algorithms or Cipher Suites**

Security Profile	Required Algorithm(s) or Cipher suite	Notes
"HTTP_DIGEST"	MD5	SHA- is optional.
"HTTP_TLS_1"	TLS_RSA_WITH_AES_128_CBC_SHA	TLS version 1.0 Refer to RFC 3268 and 2246.
"HTTP_TLS_2"	TLS_RSA_WITH_AES_128_CBC_SHA	TLS version 1.0 Refer to RFC 3268 and 2246.
"HTTP_IPSEC"	AES-GCM (key size: 128 bits, ICV or Digest len: 16 B) or AES-CBC (Key size: 128 bits) with HMAC-SHA1-96	Refer to RFC 4301, 4303, and 4106.

331 8.2 Roles and Authorization

332 Table 8 outlines the Operational Roles supported by DASH implementations and the respective DASH
333 requirements.

334 **Table 8 – Operational Roles Supported by DASH**

Operational Role	Requirement	Notes
Read-only User	Optional	
Operator	Optional	
Administrator	Mandatory	

335 A DASH-compliant service shall support the administrator role. An implementation may support the
336 operator and/or read-only user roles.

337 8.3 User Account Management

338 The authentication and authorization mechanisms defined are tied with user account management. DASH
339 implementations shall support a role-based authorization model.

340 Each user shall have the ability to modify its own account credentials. An account in the administrator role
341 shall be able to perform account management for all users. Table 9 outlines the operations supported for
342 user account management and the respective DASH requirements.

343 **Table 9 – User Account Operations**

Operation	Requirement	Notes
Create an account	Optional	Recommended for the administrator role
Delete an account	Optional	Recommended for the administrator role

Operation	Requirement	Notes
Enable an account	Optional	
Disable an account	Optional	
Modify the privileges of an account	Optional	
Modify the password of an account	Mandatory	Required for the administrator account
Change the role of an account	Optional	
Create a group of accounts	Optional	
Delete a group of accounts	Optional	
Add an account to a group	Optional	
Remove an account from a group	Optional	
Change the role of a group	Optional	
Modify the privileges of a group	Optional	
Change the associations of roles and accounts	Optional	Recommended for the administrator role

344 The modifications of privileges include the changing of bindings between accounts or groups and roles.

345 ## 8.4 Authentication Mechanisms

346 DASH implementations shall support one or two levels of authentication.

347 Table 10 outlines requirements for the three types of authentication mechanisms supported by DASH 1.0
348 implementations.

349 **Table 10 – Authentication Mechanisms**

Authentication Mechanisms	Requirement	Notes
Machine-Level	Optional	
User-Level	Mandatory	
Third-Party	Optional	

350 # 9 Discovery Requirements

351 Multiple discovery stages are required to accumulate the necessary information from the managed
352 system. This section defines the implementation requirements of the stages involved in discovering
353 managed systems and their management capabilities.

354 ## 9.1 Network Endpoint Discovery Stage

355 Section 8.2 of the *Desktop and Mobile Systems Management White Paper* (DSP2014) describes
356 endpoint discovery methods. A DASH 1.0 compliant implementation need not support any of the
357 described methods.

9.2 Management Access Point Discovery Stage

A DASH-compliant MAP should support the following phase process for MAP discovery:

- **Phase 1**: RMCP Presence Ping/Pong.

A DASH-compliant MAP shall support the following phase process for MAP discovery:

- **Phase 2**: WS-Management Identify method.

9.2.1 RMCP Presence Ping/Pong

Presence Ping is an RMCP command that is defined in the *Alert Standard Format Specification*, (DSP0136). The command involves a request-response message exchange initiated by a management client (Ping) and completed by a management service (Pong).

The format of the RMCP Presence Pong (40h) data section shall conform to section 3.2.4.3 of DSP0136 with the following definition:

Supported Interactions field (Data Byte 10 of Presence Pong), bit 5 set to 1b if DASH is supported

A DASH-compliant MAP should support this command on the ASF-RMCP well-known UDP port (623). Support of Presence Ping/Pong on the ASF-Secure-RMCP well-known UDP port (664) is not recommended for a DASH service.

9.2.2 WS-Management Identify Method

Refer to clause 11 of RFC 2246 for a definition of the Identify method. A DASH-compliant management service shall support the Identify method on each DASH access port that it supports.

In addition to the child element defined in RFC 2246, the following extension elements are defined by DASH as children of the *IdentifyResponse* element:

```
4.1 <s:Body>
   <wsmid:IdentifyResponse>
      <wsmid:ProtocolVersion> xs:anyURI </wsmid:ProtocolVersion>
      <wsmid:ProductVendor> xs:string </wsmid:ProductVendor>
      <wsmid:ProductVersion> xs:string </wsmid:ProductVersion>
      <dash:DASHVersion> xs:string </dash:DASHVersion>
      <wsmid:SecurityProfiles>
         <wsmid:SecurityProfileName> xs:string or URI </wsmid:SecurityProfileName> +
      </wsmid:SecurityProfiles>
   </wsmid:IdentifyResponse>
</s:Body>
```

Table 11 defines the IdentifyResponse payload requirements for DASH 1.0.

Table 11 – WS-Management IdentifyResponse Payload Elements

Element	Requirement	Notes
wsmid:IdentifyResponse	Mandatory	The body of the response
wsmid:IdentifyResponse/wsmid:ProtocolVersion	Mandatory	URI identifying DSP0226 1.0 http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
wsmid:IdentifyResponse/wsmid:ProductVendor	Optional	

Element	Requirement	Notes
wsmid:IdentifyResponse/wsmid:ProductVersion	Optional	
wsmid:IdentifyResponse/dash:DASHVersion	Mandatory	Identifies the DASH version supported, which shall be formatted as "*n.n.n*". Example: "1.0.0"
wsmid:IdentifyResponse/wsmid:SecurityProfiles/ wsmid:SecurityProfileName	Mandatory	URI identifying the security profile supported **Class A:** "HTTP_DIGEST": http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest **Class B:** "HTTP_TLS_1": http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest" "HTTP_TLS_2": http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic" "HTTP_IPSEC": http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest

9.2.3 wsmid:Identify Security Implementation Requirements

Implementations may support wsmid:Identify without authentication as described in Rule R11.4 of DSP0226.

If an implementation supports wsmid:Identify without authentication, it should support it through a URL that contains the suffix "/wsman-anon/identify."

9.3 Enumeration of Management Capabilities Stage

The DMTF *Profile Registration Profile* (DSP1033) specifies methods for enumerating the management capabilities of a CIM-based management access point in a scalable manner. Scalability here refers to the fact that each registered profile concisely describes support for a set of related management capabilities that is independent of the number of CIM instances supported by the management access point.

10 In-Band and Out-of-Band Traffic Requirements

A DASH compliant service shall support, at minimum, a shared IPv4 and MAC address as defined below:

- A physical system's out-of-band Management Access Point and the In-Band host shall share the MAC address and IPv4 address of the network interface. Manageability traffic shall be routed to the MAP through the well known system ports to be defined by IANA. Implementations may support the use and configuration of other ports.

Developers may use any port necessary during product development. Implementations shall support the IANA-defined system ports for product deployment.

- Sideband DMTF Web Services Protocol Ports
  - OOB-WS-HTTP
    - TCP 623
  - OOB-WS-HTTPS (If class B is implemented)
    - TCP 664
- In-band Web Services Protocol Ports may be supported on the following transport ports and shall be transport specific:
  - HTTP
  - HTTPS (If class B is implemented)

NOTE: In-band and out of band MAPs shall listen on different ports.

ANNEX A
(informative)

Change Log

Version	Date	Author	Description
1.0.0	3/5/2009	J. Kozlowski	DMTF Standard Release
1.0.1	8/14/2009		DMTF Standard Release

ANNEX B
(informative)

HTTP Status Codes

This section is intended to direct implementers to the appropriate specifications for implementation requirements surrounding HTTP status codes:

- DSP0226 ANNEX C, line 4298; "RC.2-9: When delivering faults, an HTTP status code of 500 should be used in the response for s:Receiver faults, and a code of 400 should be used for s:Sender faults."
- WS-I Basic Profile 4.3.9 “HTTP Server Error Status Codes
  HTTP uses the 5xx series of status codes to indicate failure due to a server error.
  R1126 An INSTANCE MUST use a "500 Internal Server Error" HTTP status code if the response message is a SOAP Fault."

NOTE: If an implementation returns a HTTP 200 (OK), it will be handled by the HTTP libraries directly. Sometimes, code using such libraries, only indicate that there is a fault, and do not return the fault itself.

Bibliography

DMTF DSP2014, *Systems Management Architecture for Mobile and Desktop Hardware White Paper 1.1.0,* http://www.dmtf.org/standards/published_documents/DSP2014_1.1.0.pdf
(Informative text in this document details Protocol, Security, and Discovery.)