Document Number: DSP0217

Date: 2009-08-04

Version: 2.0.0

SMASH Implementation Requirements

Document Type: Specification

Document Status: DMTF Standard

Document Language: E

Implementation of certain elements of this standard or proposed standard may be subject to third party patent rights, including provisional patent rights (herein "patent rights"). DMTF makes no representations to users of the standard as to the existence of such rights, and is not responsible to recognize, disclose, or identify any or all such third party patent right, owners or claimants, nor for any incomplete or inaccurate identification or disclosure of such rights, owners or claimants. DMTF shall have no liability to any party, in any manner or circumstance, under any legal theory whatsoever, for failure to recognize, disclose, or identify any such third party patent rights, or for such party's reliance on the standard or incorporation thereof in its product, protocols or testing procedures. DMTF shall have no liability to any party implementing such standard, whether such implementation is foreseeable or not, nor to any patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a patent owner for such implementations.

For information about patents held by third-parties which have notified the DMTF that, in their opinion, such patent may relate to or impact implementations of DMTF standards, visit http://www.dmtf.org/about/policies/disclosures.php.

CONTENTS

Tables

Foreword

The *SMASH Implementation Requirements* (DSP0217) was prepared by the Server Management Working Group of the DMTF.

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

Acknowledgements

The authors wish to acknowledge the following people.

Contributors:

- Aaron Merkin – IBM
- Jeff Hilland – HP

Participants from the DMTF Server Management Working Group:

- Jon Hass – Dell
- Khachatur Papanyan – Dell
- Radhakrishna Dasari – Dell
- Jeff Hilland – HP
- Aaron Merkin – IBM
- John Leung – Intel
- Joel Clark – Intel

Introduction

This specification describes the conformance requirements for implementing the System Management Architecture for Server Hardware (SMASH) version 2.0.

SMASH Implementation Requirements

1 Scope

This document specifies the requirements for implementing the System Management Architecture for Server Hardware (SMASH) version 2.0. This document specifies those requirements by defining which other DMTF specifications are required, conditional, and optional. The mandatory specifications to be implemented are defined in clause 4. The optional and conditional specifications are defined in clauses 5, 6, 7, and 8.

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 DSP0214, *Server Management Command Line Protocol Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0214_1.0.pdf

DMTF DSP0215, *Server Management Managed Element (SM ME) Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0215_1.0.pdf

DMTF DSP0216, *SM CLP to CIM Common Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0216_1.0.pdf

DMTF DSP0226, *Web Services for Management (WS 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 DSP0800, *Base Server Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0800_1.0.pdf

DMTF DSP0801, *CLP Service Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0801_1.0.pdf

DMTF DSP0802, *SMASH Collections Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0802_1.0.pdf

DMTF DSP0803, *SM CLP Admin Domain Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0803_1.0.pdf

DMTF DSP0804, *Modular System Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0804_1.0.pdf

DMTF DSP0805, *Sensors Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0805_1.0.pdf

DMTF DSP0806, *Device Tray Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0806_1.0.pdf

DMTF DSP0807, *Pass-Through Module Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0807_1.0.pdf

DMTF DSP0808, *CPU Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0808_1.0.pdf

DMTF DSP0809, *System Memory Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0809_1.0.pdf

DMTF DSP0810, *Record Log Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0810_1.0.pdf

DMTF DSP0811, *Simple Identity Management Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0811_1.0.pdf

DMTF DSP0812, *Physical Asset Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0812_1.0.pdf

DMTF DSP0813, *Boot Control Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0813_1.0.pdf

DMTF DSP0814, *Fan Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0814_1.0.pdf

DMTF DSP0815, *Ethernet Port Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0815_1.0.pdf

DMTF DSP0817, *IP Interface Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0817_1.0.pdf

DMTF DSP0818, *DHCP Client Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0818_1.0.pdf

DMTF DSP0819, *DNS Client Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0819_1.0.pdf

DMTF DSP0820, *Telnet Service Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0820_1.0.pdf

DMTF DSP0821, *SSH Service Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0821_1.0.pdf

DMTF DSP0822, *Power Supply Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0822_1.0.pdf

DMTF DSP0823, *Power State Management Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0823_1.0.pdf

DMTF DSP0824, *Service Processor Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0824_1.0.pdf

DMTF DSP0825, *Shared Device Management Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0825_1.0.pdf

DMTF DSP0826, *Software Inventory Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0826_1.0.pdf

DMTF DSP0827, *Software Update Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0827_1.0.pdf

DMTF DSP0828, *Text Console Redirection Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0828_1.0.pdf

DMTF DSP0830, *Role Based Authorization Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0830_1.0.pdf

DMTF DSP0831, *Platform Watchdog Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0831_1.0.pdf

DMTF DSP0835, *Indicator LED Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0835_1.0.pdf

DMTF DSP0836, *KVM Redirection Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0836_1.0.pdf

DMTF DSP0838, *PCI Device Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0838_1.0.pdf

DMTF DSP0842, *OS Status Profile SM CLP Command Mapping Specification, 1.0*, http://www.dmtf.org/standards/published_documents/DSP0842_1.0.pdf

DMTF DSP1004, *Base Server Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1004_1.0.pdf

DMTF DSP1005, *CLP Service Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1005_1.0.pdf

DMTF DSP1006, *SMASH Collections Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1006_1.0.pdf

DMTF DSP1007, *SM CLP Admin Domain Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1007_1.0.pdf

DMTF DSP1008, *Modular System Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1008_1.0.pdf

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

DMTF DSP1010, *Record Log Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1010_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 DSP1014, *Ethernet Port Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1014_1.0.pdf

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

DMTF DSP1016, *Telnet Service Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1016_1.0.pdf

DMTF DSP1017, *SSH Service Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1017_1.0.pdf

DMTF DSP1018, *Service Processor Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1018_1.0.pdf

DMTF DSP1019, *Device Tray Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1019_1.0.pdf

DMTF DSP1020, *Pass-Through Module Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1020_1.0.pdf

DMTF DSP1021, *Shared Device Management Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1021_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 DSP1024, *Text Console Redirection Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1024_1.0.pdf

DMTF DSP1025, *Software Update Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1025_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 DSP1029*, OS Status Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1029_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 DSP1036, *IP Interface Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1036_1.0.pdf

DMTF DSP1037, *DHCP Client Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1037_1.0.pdf

DMTF DSP1038, *DNS Client Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1038_1.0.pdf

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

DMTF DSP1040*, Watchdog Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1040_1.0.pdf

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

DMTF DSP1074*, Indicator LED Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1074_1.0.pdf

DMTF DSP1075*, PCI Device Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1075_1.0.pdf

DMTF DSP1076*, KVM Redirection Profile, 1.0*, http://www.dmtf.org/standards/published_documents/DSP1076_1.0.pdf

DMTF DSP8007, *Platform Message Registry*, *1.0*, http://www.dmtf.org/standards/published_documents/DSP8007_1.0.pdf

DMTF DSP8039, SMASH XML Schema, 1.0, http:/schemas.dmtf.org/wbem/smash/1/dsp8039.xsd

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

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

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

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

SNIA, *Storage Management Initiative Specification (SMI-S) 1.3.0*, http://www.snia.org/tech_activities/standards/curr_standards/smi

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 Mandatory Specification Requirements

This section lists mandatory profiles and protocols that are required for this specification.

4.1 Mandatory Profile Requirements

At least one of the following profiles shall be implemented:

- DMTF DSP1004, *Base Server Profile,* 1.0
- DMTF DSP1018, *Service Processor Profile,* 1.0
- DMTF DSP1008, *Modular System Profile,* 1.0

4.2 Mandatory Protocol Requirements

At least one of the following protocols shall be implemented:

- DMTF DSP0214, *Server Management Command Line Protocol Specification,* 1.0
- DMTF DSP0226, *Web Services for Management*, 1.0

5 Conditional Profile Specification Requirements

This section details the requirements for profiles and their associated mapping specifications. Implementations may expose different sets of Profiles via the protocols. This implies that a Mapping Specification for a Profile is only required if the Profile is exposed through the CLP irrespective of whether or not it is exposed via WS Management.

5.1 Base Server Profile

The *Base Server Profile* may be implemented. If the *Base Server Profile* is implemented, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the optional behavior of implementing the *SMASH Collections Profile* specified in the *Base Server Profile* shall be implemented. The *Base Server Profile SM CLP Command Mapping Specification* shall be implemented.

5.2 Boot Control Profile

The *Boot Control Profile* may be implemented. If the *Boot Control Profile* is implemented, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented and the profile is exposed using the SM CLP, the *Boot Control Profile SM CLP Command Mapping Specification* shall be implemented.

5.3 Service Processor Profile

The *Service Processor Profile* may be implemented. If the *Service Processor Profile* is implemented, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented and the profile is exposed using the SM CLP, the optional behavior of implementing the *SMASH Collections Profile* specified in the *Service Processor Profile* shall be implemented. The *Service Processor Profile SM CLP Command Mapping Specification* shall be implemented.

5.4 CLP Service Profile

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented and the profile is exposed using the SM CLP, the *CLP Service Profile* shall be implemented.

Either the optional behavior of implementing the *SSH Service Profile* specified in the *CLP Service Profile* or the optional behavior of implementing the *Telnet Service Profile* specified in the *CLP Service Profile* should be implemented. The *CLP Service Profile SM CLP Command Mapping Specification* shall be implemented.

5.5 CPU Profile

The *CPU Profile* may be implemented. If the *CPU Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *CPU Profile SM CLP Command Mapping Specification* shall be implemented.

5.6 Device Tray Profile

The *Device Tray Profile* may be implemented. If the *Device Tray Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Device Tray Profile SM CLP Command Mapping Specification* shall be implemented.

5.7 DHCP Client Profile

The *DHCP Client Profile* may be implemented. If the *DHCP Client Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *DHCP Client Profile SM CLP Command Mapping Specification* shall be implemented.

5.8 DNS Client Profile

The *DNS Client Profile* may be implemented. If the *DNS Client Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *DNS Client Profile SM CLP Command Mapping Specification* shall be implemented.

5.9 Ethernet Port Profile

The *Ethernet Port Profile* may be implemented. If the *Ethernet Port Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Ethernet Port Profile SM CLP Command Mapping Specification* shall be implemented.

5.10 Fan Profile

The *Fan Profile* may be implemented. If the *Fan Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Fan Profile SM CLP Command Mapping Specification* shall be implemented.

5.11 IP Interface Profile

The *IP Interface Profile* may be implemented. If the *IP Interface Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *IP Interface Profile SM CLP Command Mapping Specification* shall be implemented.

5.12 Modular System Profile

The *Modular System Profile* may be implemented. If the *Modular System Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Modular System Profile SM CLP Command Mapping Specification* shall be implemented.

5.13 Pass-through Module Profile

The *Pass-through Module Profile* may be implemented. If the *Pass-through Module Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Pass-through Module Profile SM CLP Command Mapping Specification* shall be implemented.

5.14 Physical Asset Profile

The *Physical Asset Profile* may be implemented. If the *Physical Asset Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Physical Asset Profile SM CLP Command Mapping Specification* shall be implemented.

5.15 Power State Management Profile

The *Power State Management Profile* may be implemented. If the *Power State Management Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Power State Management Profile SM CLP Command Mapping Specification* shall be implemented.

5.16 Power Supply Profile

The *Power Supply Profile* may be implemented. If the *Power Supply Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Power Supply Profile SM CLP Command Mapping Specification* shall be implemented.

5.17 Record Log Profile

The *Record Log Profile* may be implemented. If the *Record Log Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Record Log Profile SM CLP Command Mapping Specification* shall be implemented.

5.18 Role Based Authorization Profile

The *Role Based Authorization Profile* may be implemented. If the *Role Based Authorization Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Role Based Authorization Profile SM CLP Command Mapping Specification* shall be implemented.

5.19 Sensors Profile

The *Sensors Profile* may be implemented. If the *Sensors Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Sensors Profile SM CLP Command Mapping Specification* shall be implemented.

5.20 Shared Device Management Profile

The *Shared Device Management Profile* may be implemented. If the *Shared Device Management Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Shared Device Management Profile SM CLP Command Mapping Specification* shall be implemented.

5.21 Simple Identity Management Profile

The *Simple Identity Management Profile* may be implemented. If the *Simple Identity Management Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Simple Identity Management Profile SM CLP Command Mapping Specification* shall be implemented.

5.22 SM CLP Admin Domain Profile

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented and the profile is exposed using the SM CLP, the *SM CLP Admin Domain Profile SM CLP Command Mapping Specification* shall be implemented.

5.23 SMASH Collections Profile

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented and the profile is exposed using the SM CLP, the *SMASH Collections Profile SM CLP Command Mapping Specification* shall be implemented.

5.24 Software Inventory Profile

The *Software Inventory Profile* may be implemented. If the *Software Inventory Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Software Inventory Profile SM CLP Command Mapping Specification* shall be implemented.

5.25 Software Update Profile

The *Software Update Profile* may be implemented. If the *Software Update Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Software Update Profile SM CLP Command Mapping Specification* shall be implemented.

5.26 SSH Service Profile

The *SSH Service Profile* may be implemented. If the *SSH Service Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *SSH Service Profile SM CLP Command Mapping Specification* shall be implemented.

5.27 System Memory Profile

The *System Memory Profile* may be implemented. If the *System Memory Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *System Memory Profile SM CLP Command Mapping Specification* shall be implemented.

5.28 Telnet Service Profile

The *Telnet Service Profile* may be implemented. If the *Telnet Service Profile* is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the *Telnet Service Profile SM CLP Command Mapping Specification* shall be implemented.

5.29 Text Console Redirection Profile

The *Text Console Redirection Profile* may be implemented. If the *Text Console Redirection Profile* is implemented, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented and the profile is exposed using the SM CLP, the *Text Console Redirection Profile SM CLP Command Mapping Specification* shall be implemented.

5.30 Platform Watchdog Profile

The *Platform Watchdog Profile* may be implemented. If the *Platform Watchdog Profile* is implemented, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented and the profile is exposed using the SM CLP, the *Platform Watchdog Profile SM CLP Command Mapping Specification* shall be implemented.

5.31 KVM Redirection Profile

The *KVM Redirection Profile* may be implemented. If the *KVM Redirection Profile* is implemented, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented and the profile is exposed using the SM CLP, the *KVM Redirection Profile SM CLP Command Mapping Specification* shall be implemented.

5.32 PCI Device Profile

The *PCI Device Profile* may be implemented. If the *PCI Device Profile* is implemented, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented and the profile is exposed using the SM CLP, the *PCI Device Profile SM CLP Command Mapping Specification* shall be implemented.

5.33 OS Status Profile

The *OS Status Profile* may be implemented. If the *OS Status Profile* is implemented, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented and the profile is exposed using the SM CLP, the *OS Status Profile SM CLP Command Mapping Specification* shall be implemented.

5.34 Indicator LED Profile

The *Indicator LED Profile* may be implemented. If the *Indicator LED Profile* is implemented, the following requirements shall be met:

If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented and the profile is exposed using the SM CLP, the *Indicator LED Profile SM CLP Command Mapping Specification* shall be implemented.

5.35 Indications Profile

The *Indications Profile* may be implemented.

If DSP0226, *Web Services for Management Specification* is implemented, the following requirements should be met:

- The *Indications Profile* (DSP1054) should be implemented.
- An instance of concrete subclass of CIM_Indication should be the payload of WS-Event Delivery message. If an instance of CIM_AlertIndication is used as a payload for WS-Event Delivery message, then the contents of the instance should be from DSP8007, the *Platform Message Registry*.
- Any vendor-specific messages that are formulated should be from a published message registry with the owning entity set to other than the DMTF.

5.36 SMI-S Host Hardware Raid Controller Profile

The Host Hardware Raid Controller Profile (HHR Controller Profile) from the *Storage Management Initiative Specification (SMI-S)* may be implemented. If HHR Controller Profile is implemented, the following requirements shall be met:

- SMI-S Host Hardware Raid Profile from the *Storage Management Initiative Specification* shall not be implemented. The scoping class of the SMI-S HHR Controller profile shall be the central class of DSP1018, (*Service Processor Profile*), DSP1008 (*Modular System Profile*), or DSP1004 (*Base Server Profile*).
- HHR Controller Profile and all the HHR Controller Profile referenced profiles shall implement DSP1033 to advertise profile registration and shall not implement the SMI-S Server Profile from the *Storage Management Initiative Specification*.
- HHR Controller Profile and all the HHR Controller Profile referenced profiles may not implement mandatory indications. HHR Controller Profile and all the HHR Controller Profile referenced profiles may not implement the mandatory SMI-S Indication Profile from the *Storage Management Initiative Specification*.

6 Conditional Protocol Implementation Requirements

A SMASH-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 SMASH implementation.

6.1 SM CLP Protocol Conditional Requirements

If DSP0214*, the Server Management Command Line Protocol Specification,* is implemented, the following requirements shall be met:

- DSP0216, the *SM CLP to CIM Common Mapping Specification*, shall be implemented.
- DSP0215, the *Server Management Managed Element Addressing Specification*, shall be implemented.
- DSP1005, the *CLP Service Profile*, shall be implemented.

6.2 Management Protocol

If DSP0226, the *Web Services for Management Specification,* is implemented, the following requirements shall be met:

- DSP0227, the *WS-Management – CIM Binding Specification*, shall be implemented.
- DSP0230, the *WS-CIM Mapping Specification*, shall be implemented.
- Implementations shall not support bindings to the protocol other than that specified in DSP0227.

6.2.1 XML Namespaces

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

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

Note that the schema location URL is http:/schemas.dmtf.org/wbem/smash/1/dsp8039.xsd

6.2.2 WS-Transfer

It is mandatory for implementations to support WS-Transfer as described in section 4 of DSP0226. Table 1 defines support for WS-Transfer operations and their respective requirements.

Table 1 – WS-Transfer Operations

Operation	Requirement	Notes
Get	Mandatory	This operation retrieves resource representations. Implementations shall support the Get operation. Profiles require GetInstance support.
Put	Conditional	If a resource can be updated, the service shall support the Put operation. If an implemented profile requires ModifyInstance support, the Put operation shall be supported.
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.

6.2.3 WS-Enumeration

It is mandatory for implementations to support WS-Enumeration as described in section 5 of DSP0226. Table 2 defines support for WS-Enumeration operations and their respective requirements.

Table 2 – 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 R5.1-4 in DSP0226. Implementation of this operation is not recommended.
GetStatus	Optional	See Rule R5.1-4 in DSP0226. Implementation of this operation is not recommended.
Release	Mandatory	This operation is used to release an enumeration context.
EnumerationEnd	Optional	See Rule R5.1-4 in DSP0226. Implementation of this operation is not recommended.

It is recommended that the wsman:OptimizeEnumeration option be implemented as a child element of the wsen:Enumerate element. Refer to section 5.2.3 of DSP0226 for details. The service must accept the element, but it does not have to honor it, as described in Rule R5.2.3-1 of DSP0226.

It is optional for implementations to support the generic enumeration operations that are described in clause 15.1 of DSP0227, except the WS-Management equivalent of EnumerateInstances specified in clause 15.1.5, which is mandatory as indicated in Table 2.

6.2.4 WS-Eventing

Support for WS-Eventing is conditional. A service advertising conformance to the Indications Profile shall support WS-Eventing as described in clause 10 of DSP0226 and further constrained by the definition described in this section. Table 3 defines support for WS-Eventing operations and their respective requirements.

Table 3 – WS-Eventing Operations

Operation	Requirement	Notes
Subscribe	Mandatory	
Renew	Mandatory	
Unsubscribe	Mandatory	
SubscriptionEnd	Optional	
GetStatus	Optional	See Rule R7.3-1 in DSP0226. Implementation of this operation is not recommended.

6.2.4.1 WS-Eventing Messaging Security

For WS-Eventing the messaging security recommendations defined in Table 4 should be followed.

Table 4 – 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 7), because it can carry sensitive information	Subscriber
	wse:Renew	Class B (as defined in Section 7), because it can carry sensitive information	Subscriber
	wse:SubscriptionEnd	Class B (as defined in Section 7), because it can carry sensitive information	Subscriber
	wse:Unsubscribe	Class B (as defined in Section 7), because it can carry sensitive information	Subscriber
Delivery	wse:Delivery (Push)	Class A or B (as defined in Section 7); 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 (as defined in Section 7); B for sensitive information	MAP, but not necessarily with its own credentials
	wse:Delivery (Batched)	Class A or B (as defined in Section 7); B for sensitive information	MAP, but not necessarily with its own credentials
	wsen:Pull (Pull delivery)	Class A or B (as defined in Section 7); B for sensitive information	Subscriber
	Ack of delivery (on a separate connection)	Class A (as defined in Section 7)	Subscriber

6.2.4.2 WS-Eventing Delivery Mode

DSP0226 defines four standard delivery modes (Push Mode, PushWithAck Mode, Batched Delivery Mode, and Pull Delivery Mode). Two of these delivery modes apply to SMASH as follows:

- Implementations shall support WS-Eventing Push Mode as described in section 7.2.10 of DSP0226.
- Implementations should support WS-Eventing PushWithAck Mode as described in section 7.2.11 of DSP0226.

6.2.4.3 Eventing Source Port

Implementations shall use the well known transport ports for eventing.

6.2.4.4 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 set to 30 seconds.

6.2.5 Transport Protocol

Implementations shall use HTTP 1.1 as the SOAP transport for DSP0226. For detailed information about the transport protocol required, refer to the *Systems Management Architecture for Server Hardware White Paper* (DSP2001).

6.2.5.1 Transport TCP Port Requirements

Implementations shall support the IANA-defined system ports for product deployment, but may listen on other ports.

- Web Services Protocol Ports shall be supported on the following transport ports and shall be transport specific:
  - HTTP
  - HTTPS
- Support for the following sideband DMTF Web Services Protocol Ports is optional:
  - OOB-WS-HTTP
    - TCP Port 623
  - OOB-WS-HTTPS
    - TCP Port 664

7 Security Implementation Requirements

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

7.1 WS Management Protocol Specific Security Requirements

If DSP0226, the *Web Services for Management Specification,* is implemented, the requirements specified in this section shall be met.

7.1.1 Transport Requirements

SMASH 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 security Class A is supported, implementations should support MD5 or SHA-1 as the cryptographic algorithm.
   - **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”**
  - URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest/ipsec

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

Refer to 6.2.4.1 for WS-Eventing security requirements.

7.1.2 Cryptographic Algorithms and Cipher Suites

Table 5 lists the required cryptographic algorithms or cipher suites for the security profiles mentioned in this section.

Table 5- Required Cryptographic Algorithms or Cipher Suites

Security Profile	Required Algorithm(s) or Cipher suite	Notes
“HTTP_DIGEST”	HMAC-MD5 or HMAC-SHA1	
“HTTP_TLS_1”	TLS_RSA_WITH_AES_128_CBC_SHA	TLS version 1.0 Refer to RFC 2246.
“HTTP_TLS_2”	TLS_RSA_WITH_AES_128_CBC_SHA	TLS version 1.0 Refer to RFC 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, RFC 4303, and RFC 4106.

7.1.3 Roles and Authorization

Table 6 outlines the Operational Roles supported by implementations and the respective requirements.

Table 6 – Operational Roles Supported

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

A SMASH-compliant service should support the administrator and read-only roles. An implementation may support the operator roles.

7.1.4 User Account Management

The authentication and authorization mechanisms defined are tied with user account management. Implementations should support a role-based authorization model.

Each user should have the ability to modify its own account credentials. An account in the administrator role should be able to perform account management for all users. Table 7 outlines the operations supported for user account management and the respective requirements.

Table 7 – User Account Operations

Operation	Requirement	Notes
Create an account	Optional	Recommended for the administrator role
Delete an account	Optional	Recommended for the administrator role
Enable an account	Optional	
Disable an account	Optional	
Modify the privileges of an account	Optional	
Modify the password of an account	Conditional	Based on implementation of the Simple Identity Management Profile. Recommended for all roles
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

The modifications of privileges include the changing of bindings between accounts or groups and roles. The privileges defined for SMASH 2.0 are static privileges.

7.1.5 Authentication Mechanisms

Implementations shall support one or two levels of authentication.

Table 8 outlines requirements for the three types of authentication mechanisms supported by SMASH 2.0 implementations.

Table 8 – Authentication Mechanisms

Authentication Mechanisms	Requirement	Notes
Machine-Level	Optional	Mandatory for class B security compliance
User-Level	Mandatory	At a minimum
Third-Party	Optional	

8 Discovery Requirements

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

8.1 Network Endpoint Discovery Stage

The *SMASH White Paper* (DSP2001) describes endpoint discovery methods. A SMASH 2.0 compliant implementation need not support any of the described methods.

8.2 WS Management Access Point Discovery

If DSP0226, the *Web Services for Management Specification,* is implemented, the requirements specified in this section shall be met.

8.2.1 WS-Management Identify Method

Refer to section 8 of DSP0226 for a definition of the Identify method. A SMASH-compliant management service shall support the Identify method on each SMASH access port that it supports.

In addition to the child element defined in DSP0226, the following extension elements are defined by SMASH as children of the IdentifyResponse element:

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

Table 9 defines the IdentifyResponse payload requirements for SMASH 2.0.

Table 9 – 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
wsmid:IdentifyResponse/wsmid:ProductVendor	Optional	
wsmid:IdentifyResponse/wsmid:ProductVersion	Optional	
wsmid:IdentifyResponse/SMASH:SMASHVersion	Mandatory	Identifies the SMASH version supported, which shall be formatted as "*n.n.n*" Example: "2.0.0"

Element	Requirement	Notes
wsmid:IdentifyResponse/wsmid:SecurityProfiles/ wsmid:SecurityProfileName	Mandatory	String 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

8.2.2 wsmid:Identify Security Implementation Requirements

Implementations may support wsmid:Identify without authentication, as described in Rule R10.9-4 of DSP0226.

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

ANNEX A
(informative)

Change Log

Version	Date	Editor	Description
1.0.0a	11/02/2006	A. Merkin	Preliminary Standard
2.0.0a	05/07/2007	J. Hilland	Preliminary Standard
2.0.0	05/15/2009	J. Hilland	DMTF Standard

Bibliography

DMTF DSP2001, *Systems Management Architecture for Server Hardware (SMASH) Command Line Protocol (CLP) Architecture White Paper, 2.0*, http://www.dmtf.org/standards/published_documents/DSP2001_2.0.pdf