



Document Number: DSP0217

Date: 2007-09-11

Version: 2.0.0a

SMASH Implementation Requirements

Document Type: Specification

Document Status: Preliminary Standard

Document Language: E

SMASH Implementation Requirements

Copyright notice

Copyright © 2007 Distributed Management Task Force, Inc. (DMTF). All rights reserved.

DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability. Members and non-members may reproduce DMTF specifications and documents for uses consistent with this purpose, provided that correct attribution is given. As DMTF specifications may be revised from time to time, the particular version and release date should always be noted.

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patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a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.

CONTENTS

Foreword	5
Introduction	6
1 Scope	7
2 Normative References.....	7
2.1 Approved References	7
2.2 References under Development	9
2.3 Other References.....	9
3 Terms and Definitions	10
4 Mandatory Specification Requirements	11
4.1 Mandatory Profile Requirements	11
4.2 Mandatory Protocol Requirements	11
5 Conditional Profile Specification Requirements	11
5.1 Base Server Profile	11
5.2 Boot Control Profile.....	11
5.3 Service Processor Profile	12
5.4 CLP Service Profile.....	12
5.5 CPU Profile	12
5.6 Device Tray Profile.....	12
5.7 DHCP Client Profile	12
5.8 DNS Client Profile.....	12
5.9 Ethernet Port Profile.....	12
5.10 Fan Profile.....	13
5.11 IP Interface Profile	13
5.12 Modular System Profile.....	13
5.13 Pass-through Module Profile	13
5.14 Physical Asset Profile	13
5.15 Power State Management Profile	13
5.16 Power Supply Profile.....	13
5.17 Record Log Profile	14
5.18 Role Based Authorization Profile	14
5.19 Sensors Profile.....	14
5.20 Shared Device Management Profile	14
5.21 Simple Identity Management Profile	14
5.22 SM CLP Admin Domain Profile.....	14
5.23 SMASH Collections Profile	14
5.24 Software Inventory Profile.....	15
5.25 Software Update Profile	15
5.26 SSH Service Profile	15
5.27 System Memory Profile.....	15
5.28 Telnet Service Profile.....	15
5.29 Text Console Redirection Profile	15
5.30 Watchdog Profile.....	15
5.31 KVM Redirection Profile.....	16
5.32 PCI Device Profile.....	16
5.33 OS Status Profile	16
5.34 Indicator LED Profile	16
5.35 Indications Profile.....	16
5.36 SMI-S Host Hardware Raid Controller Profile	16
6 Conditional Protocol Implementation Requirements	17
6.1 SM CLP Protocol Conditional Requirements.....	17
6.2 Management Protocol.....	17

SMASH Implementation Requirements

7	Security Implementation Requirements	20
7.1	WS Management Protocol Specific Security Requirements.....	20
8	Discovery Requirements	23
8.1	Network Endpoint Discovery Stage	23
8.2	WS Management Access Point Discovery	23
	ANNEX A (informative) Change Log.....	25
	ANNEX B (informative) Acknowledgements	26

Tables

Table 1	– WS-Transfer Operations	17
Table 2	– WS-Enumeration Operations	18
Table 3	– WS-Eventing Operations	18
Table 4	– WS-Eventing Message Security Recommendations	19
Table 6	– Operational Roles Supported.....	21
Table 7	– User Account Operations.....	22
Table 8	– Authentication Mechanisms	22
Table 9	– WS-Management IdentifyResponse Payload Elements	23

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.

Introduction

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

1

SMASH Implementation Requirements

2 1 Scope

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

8 2 Normative References

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

12 2.1 Approved References

13 DMTF [DSP0214](#), *Server Management Command Line Protocol Specification, 1.0.0*

14 DMTF [DSP0216](#), *SM CLP to CIM Common Mapping Specification, 1.0.0*

15 DMTF [DSP0215](#), *Server Management Managed Element Addressing Specification, 1.0.0*

16 DMTF [DSP1004](#), *Base Server Profile, 1.0.0*

17 DMTF [DSP0800](#), *Base Server Profile SM CLP Command Mapping Specification, 1.0.0*

18 DMTF [DSP1012](#), *Boot Control Profile, 1.0.0*

19 DMTF [DSP0813](#), *Boot Control Profile SM CLP Command Mapping Specification, 1.0.0*

20 DMTF [DSP1018](#), *Service Processor Profile, 1.0.0*

21 DMTF [DSP0824](#), *Service Processor Profile SM CLP Command Mapping Specification, 1.0.0*

22 DMTF [DSP1005](#), *CLP Service Profile, 1.0.0*

23 DMTF [DSP0801](#), *CLP Service Profile SM CLP Command Mapping Specification, 1.0.0*

24 DMTF [DSP1022](#), *CPU Profile, 1.0.0*

25 DMTF [DSP0808](#), *CPU Profile SM CLP Command Mapping Specification, 1.0.0*

26 DMTF [DSP1019](#), *Device Tray Profile, 1.0.0*

27 DMTF [DSP0806](#), *Device Tray Profile SM CLP Command Mapping Specification, 1.0.0*

28 DMTF [DSP1037](#), *DHCP Client Profile, 1.0.0*

29 DMTF [DSP0818](#), *DHCP Client Profile SM CLP Command Mapping Specification, 1.0.0*

30 DMTF [DSP1038](#), *DNS Client Profile, 1.0.0*

31 DMTF [DSP0819](#), *DNS Client Profile SM CLP Command Mapping Specification, 1.0.0*

- 32 DMTF [DSP1014](#), *Ethernet Port Profile, 1.0.0*
- 33 DMTF [DSP0815](#), *Ethernet Port Profile SM CLP Command Mapping Specification, 1.0.0*
- 34 DMTF [DSP1013](#), *Fan Profile, 1.0.0*
- 35 DMTF [DSP0814](#), *Fan Profile SM CLP Command Mapping Specification, 1.0.0*
- 36 DMTF [DSP1054](#), *Indications Profile, 1.0.0*
- 37 DMTF [DSP1036](#), *IP Interface Profile, 1.0.0*
- 38 DMTF [DSP0817](#), *IP Interface Profile SM CLP Command Mapping Specification, 1.0.0*
- 39 DMTF [DSP1008](#), *Modular System Profile, 1.0.0*
- 40 DMTF [DSP0804](#), *Modular System Profile SM CLP Command Mapping Specification, 1.0.0*
- 41 DMTF [DSP1020](#), *Pass-Through Module Profile, 1.0.0*
- 42 DMTF [DSP0807](#), *Pass-Through Module Profile SM CLP Command Mapping Specification, 1.0.0*
- 43 DMTF [DSP1011](#), *Physical Asset Profile, 1.0.0*
- 44 DMTF [DSP0812](#), *Physical Asset Profile SM CLP Command Mapping Specification, 1.0.0*
- 45 DMTF [DSP8007](#), *Platform Message Registry, 1.0.0*
- 46 DMTF [DSP1027](#), *Power State Management Profile, 1.0.0*
- 47 DMTF [DSP0823](#), *Power State Management Profile SM CLP Command Mapping Specification, 1.0.0*
- 48 DMTF [DSP1015](#), *Power Supply Profile, 1.0.0*
- 49 DMTF [DSP0822](#), *Power Supply Profile SM CLP Command Mapping Specification, 1.0.0*
- 50 DMTF [DSP1033](#), *Profile Registration Profile, 1.0.0*
- 51 DMTF [DSP1010](#), *Record Log Profile, 1.0.0*
- 52 DMTF [DSP0810](#), *Record Log Profile SM CLP Command Mapping Specification, 1.0.0*
- 53 DMTF [DSP1039](#), *Role Based Authorization Profile, 1.0.0*
- 54 DMTF [DSP0830](#), *Role Based Authorization Profile SM CLP Command Mapping Specification, 1.0.0*
- 55 DMTF [DSP1009](#), *Sensors Profile, 1.0.0*
- 56 DMTF [DSP0805](#), *Sensors Profile SM CLP Command Mapping Specification, 1.0.0*
- 57 DMTF [DSP1021](#), *Shared Device Management Profile, 1.0.0*
- 58 DMTF [DSP0825](#), *Shared Device Management Profile SM CLP Command Mapping Specification, 1.0.0*
- 59 DMTF [DSP1034](#), *Simple Identity Management Profile, 1.0.0*
- 60 DMTF [DSP0811](#), *Simple Identity Management Profile SM CLP Command Mapping Specification, 1.0.0*
- 61 DMTF [DSP1007](#), *SM CLP Admin Domain Profile, 1.0.0*
- 62 DMTF [DSP0803](#), *SM CLP Admin Domain Profile SM CLP Command Mapping Specification, 1.0.0*
- 63 DMTF [DSP1006](#), *SMASH Collections Profile, 1.0.0*

SMASH Implementation Requirements

- 64 DMTF [DSP0802](#), *SMASH Collections Profile SM CLP Command Mapping Specification, 1.0.0*
- 65 DMTF [DSP1023](#), *Software Inventory Profile, 1.0.0*
- 66 DMTF [DSP0826](#), *Software Inventory Profile SM CLP Command Mapping Specification, 1.0.0*
- 67 DMTF [DSP1025](#), *Software Update Profile, 1.0.0*
- 68 DMTF [DSP0827](#), *Software Update Profile SM CLP Command Mapping Specification, 1.0.0*
- 69 DMTF [DSP1017](#), *SSH Service Profile, 1.0.0*
- 70 DMTF [DSP0821](#), *SSH Service Profile SM CLP Command Mapping Specification, 1.0.0*
- 71 DMTF [DSP1026](#), *System Memory Profile, 1.0.0*
- 72 DMTF [DSP0809](#), *System Memory Profile SM CLP Command Mapping Specification, 1.0.0*
- 73 DMTF [DSP1016](#), *Telnet Service Profile, 1.0.0*
- 74 DMTF [DSP0820](#), *Telnet Service Profile SM CLP Command Mapping Specification, 1.0.0*
- 75 DMTF [DSP1024](#), *Text Console Redirection Profile, 1.0.0*
- 76 DMTF [DSP0828](#), *Text Console Redirection Profile SM CLP Command Mapping Specification, 1.0.0*
- 77 DMTF [DSP0226](#), *Web Services for Management, 1.0.0*
- 78 DMTF [DSP0227](#), *WS-Management — CIM Binding Specification, 1.0.0*
- 79 DMTF [DSP0230](#), *WS-CIM Mapping Specification, 1.0.0*
- 80 DMTF [DSP1040](#), *Watchdog Profile, 1.0.0*
- 81 DMTF [DSP0830](#), *Watchdog Profile SM CLP Command Mapping Specification, 1.0.0*
- 82 DMTF [DSP1076](#), *KVM Redirection Profile, 1.0.0*
- 83 DMTF [DSP0836](#), *KVM Redirection Profile SM CLP Command Mapping Specification, 1.0.0*
- 84 DMTF [DSP1029](#), *OS Status Profile, 1.0.0*
- 85 DMTF [DSP0842](#), *OS Status Profile SM CLP Command Mapping Specification, 1.0.0*
- 86 DMTF [DSP1075](#), *PCI Device Profile, 1.0.0*
- 87 DMTF [DSP0838](#), *PCI Device Profile SM CLP Command Mapping Specification, 1.0.0*
- 88 DMTF [DSP1075](#), *Indicator LED Profile, 1.0.0*
- 89 DMTF [DSP0835](#), *Indicator LED Profile SM CLP Command Mapping Specification, 1.0.0*
- 90 SNIA SMI-S Storage Management Technical Specification, [1.3.0, Rev2](#)

91 **2.2 References under Development**

92 None.

93 **2.3 Other References**

94 [ISO/IEC Directives, Part 2](#), *Rules for the structure and drafting of International Standards*

95 DMTF [DSP2001](#), *Systems Management Architecture for Server Hardware (SMASH) Command Line*
96 *Protocol (CLP) Architecture White Paper, 2.0.0*

97 **3 Terms and Definitions**

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

99 **3.1**

100 **can**

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

102 **3.2**

103 **cannot**

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

105 **3.3**

106 **conditional**

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

109 **3.4**

110 **mandatory**

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

113 **3.5**

114 **may**

115 indicates a course of action permissible within the limits of the document

116 **3.6**

117 **need not**

118 indicates a course of action permissible within the limits of the document

119 **3.7**

120 **optional**

121 indicates a course of action permissible within the limits of the document

122 **3.8**

123 **shall**

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

126 **3.9**

127 **shall not**

128 indicates requirements to be followed in order to conform to the document and from which no deviation is
129 permitted

130 **3.10**

131 **should**

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

134 **3.11**
 135 **should not**
 136 indicates that a certain possibility or course of action is deprecated but not prohibited

137 **4 Mandatory Specification Requirements**

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

139 **4.1 Mandatory Profile Requirements**

140 At least one of the following profiles shall be implemented:

- 141 • DMTF [DSP1004](#), *Base Server Profile*, 1.0.0
- 142 • DMTF [DSP1018](#), *Service Processor Profile*, 1.0.0
- 143 • DMTF [DSP1008](#), *Modular System Profile*, 1.0.0

144 **4.2 Mandatory Protocol Requirements**

145 At least one of the following protocols shall be implemented:

- 146 • DMTF [DSP0214](#), *Server Management Command Line Protocol Specification*, 1.0.0
- 147 • DMTF [DSP0226](#), *Web Services for Management*, 1.0.0

148 **5 Conditional Profile Specification Requirements**

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

153 **5.1 Base Server Profile**

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

156 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
 157 optional behavior of implementing the *SMASH Collections Profile* specified in the *Base Server Profile*
 158 shall be implemented. The *Base Server Profile SM CLP Command Mapping Specification* shall be
 159 implemented.

160 **5.2 Boot Control Profile**

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

163 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the
 164 profile is exposed using the SM CLP, the *Boot Control Profile SM CLP Command Mapping*
 165 *Specification* shall be implemented.

166 **5.3 Service Processor Profile**

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

169 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the
170 profile is exposed using the SM CLP, the optional behavior of implementing the *SMASH Collections*
171 *Profile* specified in the *Service Processor Profile* shall be implemented. The *Service Processor*
172 *Profile SM CLP Command Mapping Specification* shall be implemented.

173 **5.4 CLP Service Profile**

174 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the
175 profile is exposed using the SM CLP, the *CLP Service Profile* shall be implemented.

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

180 **5.5 CPU Profile**

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

183 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
184 *CPU Profile SM CLP Command Mapping Specification* shall be implemented.

185 **5.6 Device Tray Profile**

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

188 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
189 *Device Tray Profile SM CLP Command Mapping Specification* shall be implemented.

190 **5.7 DHCP Client Profile**

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

193 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
194 *DHCP Client Profile SM CLP Command Mapping Specification* shall be implemented.

195 **5.8 DNS Client Profile**

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

198 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
199 *DNS Client Profile SM CLP Command Mapping Specification* shall be implemented.

200 **5.9 Ethernet Port Profile**

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

203 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
204 *Ethernet Port Profile SM CLP Command Mapping Specification* shall be implemented.

205 **5.10 Fan Profile**

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

208 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the *Fan*
209 *Profile SM CLP Command Mapping Specification* shall be implemented.

210 **5.11 IP Interface Profile**

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

213 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the *IP*
214 *Interface Profile SM CLP Command Mapping Specification* shall be implemented.

215 **5.12 Modular System Profile**

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

218 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
219 *Modular System Profile SM CLP Command Mapping Specification* shall be implemented.

220 **5.13 Pass-through Module Profile**

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

223 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
224 *Pass-through Module Profile SM CLP Command Mapping Specification* shall be implemented.

225 **5.14 Physical Asset Profile**

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

228 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
229 *Physical Asset Profile SM CLP Command Mapping Specification* shall be implemented.

230 **5.15 Power State Management Profile**

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

233 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
234 *Power State Management Profile SM CLP Command Mapping Specification* shall be implemented.

235 **5.16 Power Supply Profile**

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

238 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
239 *Power Supply Profile SM CLP Command Mapping Specification* shall be implemented.

240 **5.17 Record Log Profile**

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

243 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
244 *Record Log Profile SM CLP Command Mapping Specification* shall be implemented.

245 **5.18 Role Based Authorization Profile**

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

248 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
249 *Role Based Authorization Profile SM CLP Command Mapping Specification* shall be implemented.

250 **5.19 Sensors Profile**

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

253 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
254 *Sensors Profile SM CLP Command Mapping Specification* shall be implemented.

255 **5.20 Shared Device Management Profile**

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

258 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
259 *Shared Device Management Profile SM CLP Command Mapping Specification* shall be
260 implemented.

261 **5.21 Simple Identity Management Profile**

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

264 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
265 *Simple Identity Management Profile SM CLP Command Mapping Specification* shall be
266 implemented.

267 **5.22 SM CLP Admin Domain Profile**

268 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the
269 profile is exposed using the SM CLP, the *SM CLP Admin Domain Profile SM CLP Command Mapping*
270 *Specification* shall be implemented.

271 **5.23 SMASH Collections Profile**

272 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the
273 profile is exposed using the SM CLP, the *SMASH Collections Profile SM CLP Command Mapping*
274 *Specification* shall be implemented.

275 5.24 Software Inventory Profile

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

278 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
279 *Software Inventory Profile SM CLP Command Mapping Specification* shall be implemented.

280 5.25 Software Update Profile

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

283 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
284 *Software Update Profile SM CLP Command Mapping Specification* shall be implemented.

285 5.26 SSH Service Profile

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

288 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
289 *SSH Service Profile SM CLP Command Mapping Specification* shall be implemented.

290 5.27 System Memory Profile

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

293 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
294 *System Memory Profile SM CLP Command Mapping Specification* shall be implemented.

295 5.28 Telnet Service Profile

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

298 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the
299 *Telnet Service Profile SM CLP Command Mapping Specification* shall be implemented.

300 5.29 Text Console Redirection Profile

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

303 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the
304 profile is exposed using the SM CLP, the *Text Console Redirection Profile SM CLP Command*
305 *Mapping Specification* shall be implemented.

306 5.30 Watchdog Profile

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

309 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the
310 profile is exposed using the SM CLP, the *Watchdog Profile SM CLP Command Mapping*
311 *Specification* shall be implemented.

312 **5.31 KVM Redirection Profile**

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

315 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the
316 profile is exposed using the SM CLP, the *KVM Redirection Profile SM CLP Command Mapping*
317 *Specification* shall be implemented.

318 **5.32 PCI Device Profile**

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

321 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the
322 profile is exposed using the SM CLP, the *PCI Device Profile SM CLP Command Mapping*
323 *Specification* shall be implemented.

324 **5.33 OS Status Profile**

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

327 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the
328 profile is exposed using the SM CLP, the *OS Status Profile SM CLP Command Mapping*
329 *Specification* shall be implemented.

330 **5.34 Indicator LED Profile**

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

333 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the
334 profile is exposed using the SM CLP, the *Indicator LED Profile SM CLP Command Mapping*
335 *Specification* shall be implemented.

336 **5.35 Indications Profile**

337 The *Indications Profile* may be implemented.

338 If [DSP0226](#), *Web Services for Management Specification* is implemented, the following requirements
339 should be met:

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

346 **5.36 SMI-S Host Hardware Raid Controller Profile**

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

- 350 • SMI-S Host Hardware Raid Profile from SMI-S Storage Management Technical Specification shall
351 not be implemented. The scoping class of SMI-S HHR Controller profile shall be the central class of
352 [DSP1018](#), the Service Processor Profile or [DSP1008](#), the Modular System Profile, or [DSP1004](#), the
353 Base Server Profile.
- 354 • HHR Controller Profile and all the HHR Controller Profile referenced profiles shall implement
355 [DSP1033](#) to advertise profile registration and shall not implement SMI-S Server Profile from SMI-S
356 Storage Management Technical Specification.
- 357 • HHR Controller Profile and all the HHR Controller Profile referenced profiles may not implement
358 mandatory indications. HHR Controller Profile and all the HHR Controller Profile referenced profiles
359 may not implement mandatory SMI-S Indication Profile from SMI-S Storage Management Technical
360 Specification.

361 6 Conditional Protocol Implementation Requirements

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

365 6.1 SM CLP Protocol Conditional Requirements

366 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the following
367 requirements shall be met:

- 368 • [DSP0216](#), the *SM CLP to CIM Common Mapping Specification*, shall be implemented.
- 369 • [DSP0215](#), the *Server Management Managed Element Addressing Specification*, shall be
370 implemented.
- 371 • [DSP1005](#), the *CLP Service Profile*, shall be implemented.

372 6.2 Management Protocol

373 If [DSP0226](#), the *Web Services for Management Specification*, is implemented, the following requirements
374 shall be met:

- 375 • [DSP0227](#), the *WS-Management – CIM Binding Specification*, shall be implemented.
- 376 • [DSP0230](#), the *WS-CIM Mapping Specification*, shall be implemented.
- 377 • Implementations shall not support bindings to the protocol other than that specified in [DSP0227](#).

378 6.2.1 WS-Transfer

379 It is mandatory for implementations to support WS-Transfer as described in section 4 of [DSP0226](#). Table
380 1 defines support for WS-Transfer operations and their respective requirements.

381 **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.

382 6.2.2 WS-Enumeration

383 It is mandatory for implementations to support WS-Enumeration as described in section 5 of [DSP0226](#).
384 Table 2 defines support for WS-Enumeration operations and their respective requirements.

385 **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.

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

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

392 6.2.3 WS-Eventing

393 Support for WS-Eventing is conditional. A service advertising conformance to the Indications Profile Shall
394 support WS-Eventing as described in clause 10 of [DSP0226](#) and further constrained by the definition
395 described in this section. Table 3 defines support for WS-Eventing operations and their respective
396 requirements.

397 **Table 3 – WS-Eventing Operations**

Operation	Requirement	Notes
Subscribe	Mandatory	

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

398 **6.2.3.1 WS-Eventing Messaging Security**

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

400 **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

401 **6.2.3.2 WS-Eventing Delivery Mode**

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

- 404 • Implementations shall support WS-Eventing Push Mode as described in section 7.2.10 of
405 [DSP0226](#).

- 406 • Implementations should support WS-Eventing PushWithAck Mode as described in section
407 7.2.11 of [DSP0226](#).

408 **6.2.3.3 Eventing Source Port**

409 Implementations shall use the well known transport ports for eventing.

410 **6.2.3.4 Subscription related property definition guidance**

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

413 The value for the FailureTriggerTimeInterval property on the CIM_IndicationSubscription or
414 CIM_FilterCollectionSubscription instance created internally in response to wse:Subscribe should be to
415 30 seconds.

416 **6.2.4 Transport Protocol**

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

420 **6.2.4.1 Transport TCP Port Requirements**

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

- 423 • Web Services Protocol Ports shall be supported on the following transport ports and shall be
424 transport specific:
- 425 – HTTP
 - 426 – HTTPS
- 427 • Support for the following sideband DMTF Web Services Protocol Ports is optional:
- 428 • OOB-WS-HTTP
 - 429 • TCP Port 623
 - 430 • OOB-WS-HTTPS
 - 431 • TCP Port 664

432 **7 Security Implementation Requirements**

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

435 **7.1 WS Management Protocol Specific Security Requirements**

436 If [DSP0226](#), the *Web Services for Management Specification*, is implemented, the requirements specified
437 in this section shall be met.

438 **7.1.1 Transport Requirements**

439 SMASH defines two security classes for HTTP 1.1 transport:

- 440 1) **Class A:** The security class A requires HTTP digest authentication for the user authentication.
441 For this class, no encryption capabilities are required beyond the encryption of the password

442 during the digest authentication exchange. If security Class A is supported, implementations
 443 should support MD5 or SHA-1 as the cryptographic algorithm.

- 444 • **String = “HTTP_DIGEST”**
- 445 – URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest
- 446 2) **Class B:** This class defines three security profiles that are based on either TLS or IPsec with
 447 specifically selected modes and cryptographic algorithms. For class B compliance, the support
 448 for at least one of the following security profiles is mandatory:
- 449 • **String = “HTTP_TLS_1”**
- 450 – URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest
- 451 • **String = “HTTP_TLS_2”**
- 452 – URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic
- 453 • **String = “HTTP_IPSEC”**
- 454 – URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest/ipsec

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

457 Refer to 6.2.3.1 for WS-Eventing security requirements.

458 7.1.2 Cryptographic Algorithms and Cipher Suites

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

461 **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, 4303, and 4106

462 7.1.3 Roles and Authorization

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

464 **Table 6 – Operational Roles Supported**

Operational Role	Requirement	Notes
Read-only User	Mandatory	
Operator	Optional	

Administrator	Mandatory	
---------------	-----------	--

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

467 **7.1.4 User Account Management**

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

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

473 **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 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

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

476 **7.1.5 Authentication Mechanisms**

477 Implementations shall support one or two levels of authentication. Start to write

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

480 **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	

481 **8 Discovery Requirements**

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

485 **8.1 Network Endpoint Discovery Stage**

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

488 **8.2 WS Management Access Point Discovery**

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

491 **8.2.1 WS-Management Identify Method**

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

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

```

496 <s:Body>
497   <wsmid:IdentifyResponse>
498     <wsmid:ProtocolVersion> xs:anyURI </wsmid:ProtocolVersion>
499     <wsmid:ProductVendor> xs:string </wsmid:ProductVendor>
500     <wsmid:ProductVersion> xs:string </wsmid:ProductVersion>
501     <SMASH:SMASHVersion> xs:string </SMASH:SMASHVersion>
502     <wsmid:SecurityProfiles>
503       <wsmid:SecurityProfileName> xs:string or URI </wsmid:SecurityProfileName> +
504     </wsmid:SecurityProfiles>
505   </wsmid:IdentifyResponse>
506 </s:Body>
    
```

507 Table 9 defines the IdentifyResponse payload requirements for SMASH 2.0.

508 **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	

Element	Requirement	Notes
wsmid:IdentifyResponse/SMASH:SMASHVersion	Mandatory	Identifies the SMASH version supported, which shall be formatted as “ <i>n.n.n</i> ” Example: “2.0.0”
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

509 **8.2.2 wsmid:Identify Security Implementation Requirements**

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

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

514
515
516
517

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

518
519
520
521

ANNEX B (informative)

Acknowledgements

522 The authors wish to acknowledge the following people.

523 Contributors:

- 524 • Aaron Merkin – IBM
- 525 • Jeff Hilland – HP

526 Participants from the DMTF Server Management Working Group:

- 527 • Jon Hass – Dell
- 528 • Khachatur Papanyan – Dell
- 529 • Radhakrishna Dasari – Dell
- 530 • Jeff Hilland – HP
- 531 • Aaron Merkin – IBM
- 532 • John Leung – Intel
- 533 • Joel Clark – Intel