1

5   # SMASH Implementation Requirements

9

33 # CONTENTS

106 **Tables**

116

117   Foreword

118   The *SMASH Implementation Requirements* (DSP0217) was prepared by the Server Management
119   Working Group and Server Desktop Mobile Platforms (SDMP) Working Group of the DMTF.

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

Acknowledgements

123   The authors wish to acknowledge the following people.

124   Contributors:

125   •   Aaron Merkin – IBM

126   •   Jeff Hilland – HP

127   •   Hemal Shah – Broadcom Corporation

128   Participants from the original DMTF Server Management Working Group and Server Desktop Mobile
129   Platforms (SDMP) Working Group:

130   •   Jon Hass – Dell

131   •   Khachatur Papanyan – Dell

132   •   Radhakrishna Dasari – Dell

133   •   Jeff Hilland – HP

134   •   Aaron Merkin – IBM

135   •   John Leung – Intel

136   •   Joel Clark – Intel

137   •   Hemal Shah – Broadcom Corporation

138

139 <h1>Introduction</h1>

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

142   **SMASH Implementation Requirements**

1   Scope

144 This document specifies the requirements for implementing the System Management Architecture for
145 Server Hardware (SMASH) version 2.0. This document specifies those requirements by defining which
146 other DMTF specifications are required, conditional, and optional. The mandatory specifications to be
147 implemented are defined in clause 4. The optional and conditional specifications are defined in clauses 5,
148 7, 8, and 9.

2   Normative References

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

2.1   Approved References

154 DMTF DSP0200, *CIM Operations over HTTP 1.3,*
155 http://www.dmtf.org/standards/published_documents/DSP0200_1.3.pdf

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

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

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

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

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

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

168 DMTF DSP0800, *Base Server Profile SM CLP Command Mapping Specification, 1.0*,
169 http://www.dmtf.org/standards/published_documents/DSP0800_1.0.pdf

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

232   DMTF DSP0837*, USB Redirection Profile SM CLP Command Mapping Specification, 1.0*,
233   http://www.dmtf.org/standards/published_documents/DSP0837_1.0.pdf

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

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

238   DMTF DSP0843*, Media Redirection Profile SM CLP Command Mapping Specification, 1.0*,
239   http://www.dmtf.org/standards/published_documents/DSP0843_1.0.pdf

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

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

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

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

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

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

252   DMTF DSP1009, *Sensors Profile, 1.1*,
253   http://www.dmtf.org/standards/published_documents/DSP1009_1.1.pdf

254   DMTF DSP1010, *Record Log Profile, 1.0*,
255   http://www.dmtf.org/standards/published_documents/DSP1010_1.0.pdf

256   DMTF DSP1010, *Record Log Profile, 2.0*,
257   http://www.dmtf.org/standards/published_documents/DSP1010_2.0.pdf

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

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

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

264 DMTF DSP1014, *Ethernet Port Profile, 1.0*,
265 http://www.dmtf.org/standards/published_documents/DSP1014_1.0.pdf

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

268 DMTF DSP1015, *Power Supply Profile, 1.1*,
269 http://www.dmtf.org/standards/published_documents/DSP1015_1.1.pdf

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

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

274 DMTF DSP1018, *Service Processor Profile, 1.1*,
275 http://www.dmtf.org/standards/published_documents/DSP1018_1.1.pdf

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

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

280 DMTF DSP1021, *Shared Device Management Profile, 1.0*,
281 http://www.dmtf.org/standards/published_documents/DSP1021_1.0.pdf

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

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

286 DMTF DSP1024, *Text Console Redirection Profile, 1.0*,
287 http://www.dmtf.org/standards/published_documents/DSP1024_1.0.pdf

288 DMTF DSP1025, *Software Update Profile, 1.0*,
289 http://www.dmtf.org/standards/published_documents/DSP1025_1.0.pdf

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

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

294 DMTF DSP1027, *Power State Management Profile, 2.0*,
295 http://www.dmtf.org/standards/published_documents/DSP1027_2.0.pdf

296 DMTF DSP1029*, OS Status Profile, 1.0*,
297 http://www.dmtf.org/standards/published_documents/DSP1029_1.0.pdf

298   DMTF DSP1029*, OS Status Profile, 1.1*,
299   http://www.dmtf.org/standards/published_documents/DSP1029_1.1.pdf

300   DMTF DSP1030*, Battery Profile, 1.0*,
301   http://www.dmtf.org/standards/published_documents/DSP1030_1.0.pdf

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

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

306   DMTF DSP1036, *IP Interface Profile, 1.0*,
307   http://www.dmtf.org/standards/published_documents/DSP1036_1.0.pdf

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

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

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

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

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

318   DMTF DSP1061*, BIOS Management Profile, 1.0*,
319   http://www.dmtf.org/standards/published_documents/DSP1061_1.0.pdf

320   DMTF DSP1070*, Opaque Management Data Profile, 1.0*,
321   http://www.dmtf.org/standards/published_documents/DSP1070_1.0.pdf

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

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

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

328   DMTF DSP1077*, USB Redirection Profile, 1.0*,
329   http://www.dmtf.org/standards/published_documents/DSP1077_1.0.pdf

330   DMTF DSP1086*, Media Redirection Profile, 1.0*,
331   http://www.dmtf.org/standards/published_documents/DSP1086_1.0.pdf

332   DMTF DSP1108*, Physical Computer System View Profile, 1.0*,
333   http://www.dmtf.org/standards/published_documents/DSP1108_1.0.pdf

334   DMTF DSP1116*, IP Configuration Profile, 1.0*,
335   http://www.dmtf.org/standards/published_documents/DSP1116_1.0.pdf

336   DMTF DSP8007, *Platform Message Registry*, *1.0*,
337   http://schemas.dmtf.org/wbem/messageregistry/1/dsp8007_1.0.xml

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

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

340 IETF RFC 4346, T. Dierks et al., *The TLS Protocol Version 1.1*, http://www.ietf.org/rfc/rfc4346.txt

341 IETF RFC 5246, T. Dierks et al., *The TLS Protocol Version 1.2*, http://www.ietf.org/rfc/rfc5246.txt

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

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

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

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

2.2 Other References

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

3 Terms and Definitions

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

353 **3.1**
354 **can**

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

356 **3.2**
357 **cannot**

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

359 **3.3**
360 **conditional**

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

363 **3.4**
364 **mandatory**

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

367 **3.5**
368 **may**

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

370 **3.6**
371 **need not**

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

373 **3.7**
374 **optional**

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

376 **3.8**
377 **shall**
378 indicates requirements to be followed strictly in order to conform to the document and from which no
379 deviation is permitted

380 **3.9**
381 **shall not**
382 indicates requirements to be followed in order to conform to the document and from which no deviation is
383 permitted

384 **3.10**
385 **should**
386 indicates that among several possibilities, one is recommended as particularly suitable, without
387 mentioning or excluding others, or that a certain course of action is preferred but not necessarily required

388 **3.11**
389 **should not**
390 indicates that a certain possibility or course of action is deprecated but not prohibited

391 # 4   Mandatory Specification Requirements

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

393 ## 4.1   Mandatory Profile Requirements

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

395 - DMTF DSP1004, *Base Server Profile,* 1.0

396 - DMTF DSP1018, *Service Processor Profile,* 1.1

397 - DMTF DSP1008, *Modular System Profile,* 1.0

398 ## 4.2   Mandatory Protocol Requirements

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

400 - DMTF DSP0214, *Server Management Command Line Protocol Specification,* 1.0

401 - DMTF DSP0226, *Web Services for Management*, 1.0

402 # 5   Conditional Profile Specification Requirements

403 This clause details the requirements for profiles and their associated mapping specifications.
404 Implementations may expose different sets of Profiles via the protocols. This implies that a Mapping
405 Specification for a Profile is only required if the Profile is exposed through the CLP irrespective of whether
406 or not it is exposed via WS Management. Unless otherwise indicated, profile version is 1.0 for each profile
407 referenced in this clause.

408 ## 5.1   Base Server Profile

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

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

5.2   Boot Control Profile

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

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

5.3   Service Processor Profile

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

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

5.4   CLP Service Profile

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

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

5.5   CPU Profile

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

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

5.6   Device Tray Profile

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

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

5.7   DHCP Client Profile

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

448   If DSP0214, the *Server Management Command Line Protocol Specification*, is implemented, the
449   *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* 1.0 or *Power State Management Profile 2.0* 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* 1.0 or *Power Supply Profile 1.1* 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* 1.0 or *Record Log Profile 2.0* 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* 1.0 or *Sensors Profile 1.1* 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:

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

5.22 SM CLP Admin Domain Profile

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

5.23 SMASH Collections Profile

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

5.24 Software Inventory Profile

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

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

5.25 Software Update Profile

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

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

5.26 SSH Service Profile

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

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

5.27 System Memory Profile

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

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

5.28 Telnet Service Profile

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

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

557 5.29 Text Console Redirection Profile

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

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

563 5.30 Platform Watchdog Profile

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

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

569 5.31 KVM Redirection Profile

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

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

575 5.32 PCI Device Profile

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

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

581 5.33 OS Status Profile

582 The *OS Status Profile* 1.0 or *OS Status Profile 1.1* may be implemented. If the *OS Status Profile* is
583 implemented, the following requirements shall be met:

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

587 5.34 Indicator LED Profile

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

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

593 5.35 Indications Profile

594 The *Indications Profile* may be implemented.

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

597   •   The *Indications Profile* (DSP1054) should be implemented.

598   •   An instance of concrete subclass of CIM_Indication should be the payload of WS-Event
599   Delivery message. If an instance of CIM_AlertIndication is used as a payload for WS-Event
600   Delivery message, then the contents of the instance should be from DSP8007, the *Platform*
601   *Message Registry*.

602   •   Any vendor-specific messages that are formulated should be from a published message registry
603   with the owning entity set to other than the DMTF.

604   5.36 SMI-S Host Hardware Raid Controller Profile

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

608   •   SMI-S Host Hardware Raid Profile from the *Storage Management Initiative Specification* shall
609   not be implemented. The scoping class of the SMI-S HHR Controller profile shall be the central
610   class of DSP1018, (*Service Processor Profile*), DSP1008 (*Modular System Profile*), or
611   DSP1004 (*Base Server Profile*).

612   •   HHR Controller Profile and all the HHR Controller Profile referenced profiles shall implement
613   DSP1033 to advertise profile registration and shall not implement the SMI-S Server Profile from
614   the *Storage Management Initiative Specification*.

615   •   HHR Controller Profile and all the HHR Controller Profile referenced profiles may not implement
616   mandatory indications. HHR Controller Profile and all the HHR Controller Profile referenced
617   profiles may not implement the mandatory SMI-S Indication Profile from the *Storage*
618   *Management Initiative Specification*.

619   5.37 Media Redirection Profile

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

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

625   5.38 USB Redirection Profile

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

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

631   6   Optional Profile Specification Requirements

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

636 **6.1 Battery Profile 1.0**

637 The *Battery Profile* 1.0 may be implemented.

638 **6.2 BIOS Management Profile 1.0**

639 The *BIOS Management Profile* 1.0 may be implemented.

640 **6.3 Opaque Management Data Profile 1.0**

641 The *Opaque Management Data Profile* 1.0 may be implemented.

642 **6.4 Physical Computer System View Profile 1.0**

643 The *Physical Computer System View Profile* 1.0 should be implemented.

644 **6.5 Power State Management Profile 2.0**

645 The *Power State Management Profile 2.0* may be implemented.

646 **6.6 Record Log Profile 2.0**

647 The *Record Log Profile 2.0* may be implemented.

648 **6.7 OS Status Profile 1.1**

649 The *OS Status Profile 1.1* may be implemented.

650 **6.8 Sensors Profile 1.1**

651 The *Sensors Profile 1.1* may be implemented.

652 **6.9 Power Supply Profile 1.1**

653 The *Power Supply Profile 1.1* may be implemented.

654 **6.10 IP Configuration 1.0**

655 The *IP Configuration Profile 1.0* may be implemented.

656 # 7 Conditional Protocol Implementation Requirements

657 A SMASH-compliant implementation shall use a CIM-based data model for representing managed
658 resources and services. This clause describes the Management Protocol and Transport Protocol
659 requirements for a SMASH implementation.

660 **7.1 SM CLP Protocol Conditional Requirements**

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

663 • DSP0216, the *SM CLP to CIM Common Mapping Specification*, shall be implemented.

664 • DSP0215, the *Server Management Managed Element Addressing Specification*, shall be
665 implemented.

666   • DSP1005, the *CLP Service Profile*, shall be implemented.

7.2   Management Protocol

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

670   • DSP0227, the *WS-Management – CIM Binding Specification*, shall be implemented.

671   • DSP0230, the *WS-CIM Mapping Specification*, shall be implemented.

672   • Implementations shall not support bindings to the protocol other than that specified in DSP0227.

7.2.1   XML Namespaces

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

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

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

7.2.2   WS-Transfer

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

680   **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.

7.2.3   WS-Enumeration

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

684   **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.

Operation	Requirement	Messages
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.

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

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

691   ### 7.2.4   WS-Eventing

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

696   **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.

697   #### 7.2.4.1   WS-Eventing Messaging Security

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

699   **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 Clause 8), because it can carry sensitive information	Subscriber

Plane	WS-Eventing Message	Recommended Security Class	Security Principal Requiring Authentication
	wse:Renew	Class B (as defined in Clause 8), because it can carry sensitive information	Subscriber
	wse:SubscriptionEnd	Class B (as defined in Clause 8), because it can carry sensitive information	Subscriber
	wse:Unsubscribe	Class B (as defined in Clause 8), because it can carry sensitive information	Subscriber
Delivery	wse:Delivery (Push)	Class A or B (as defined in Clause 8); 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 Clause 8); B for sensitive information	MAP, but not necessarily with its own credentials
	wse:Delivery (Batched)	Class A or B (as defined in Clause 8); B for sensitive information	MAP, but not necessarily with its own credentials
	wsen:Pull (Pull delivery)	Class A or B (as defined in Clause 8); B for sensitive information	Subscriber
	Ack of delivery (on a separate connection)	Class A (as defined in Clause 8)	Subscriber

700 **7.2.4.2   WS-Eventing Delivery Mode**

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

703 • Implementations shall support WS-Eventing Push Mode as described in clause 7.2.10 of
704   DSP0226.

705 • Implementations should support WS-Eventing PushWithAck Mode as described in clause
706   7.2.11 of DSP0226.

707 **7.2.4.3   Eventing Source Port**

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

709 **7.2.4.4   Subscription-Related Property Definition Guidance**

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

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

715 **7.2.5   Transport Protocol**

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

7.2.5.1 Transport TCP Port Requirements

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

722 • Web Services Protocol Ports shall be supported on the following transport ports and shall be
723 transport specific:

724 – HTTP

725 – HTTPS

726 • Support for the following sideband DMTF Web Services Protocol Ports is optional:

727 – OOB-WS-HTTP

728 • TCP Port 623

729 – OOB-WS-HTTPS

730 • TCP Port 664

731 8 Security Implementation Requirements

732 This clause describes transport requirements, roles and authorization, user account management, and
733 authentication.

734 8.1 WS Management Protocol Specific Security Requirements

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

737 8.1.1 Transport Requirements

738 SMASH defines two security classes for HTTP 1.1 transport:

739 1) **Class A**: The security class A requires HTTP digest authentication for the user authentication.
740 For this class, no encryption capabilities are required beyond the encryption of the password
741 during the digest authentication exchange. If security Class A is supported, implementations
742 should support MD5 or SHA-1 as the cryptographic algorithm.

743 • **String = "HTTP_DIGEST"**

744 – URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest

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

748 • **String = "HTTP_TLS_1"**

749 – URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest

750 • **String = "HTTP_TLS_2"**

751 – URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic

752 • **String = "HTTP_IPSEC"**

753 – URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest/ipsec

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

756　　Refer to 7.2.4.1 for WS-Eventing security requirements.

8.1.2　Cryptographic Algorithms and Cipher Suites

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

760　　　　　　　　　　　　**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 or later Refer to RFC 2246, RFC 4346, and RFC 5246. It is recommended that the latest 1.x version of TLS is implemented.
"HTTP_TLS_2"	TLS_RSA_WITH_AES_128_CBC_SHA	TLS version 1.0 or later Refer to RFC 2246, RFC 4346, and RFC 5246. It is recommended that the latest 1.x version of TLS is implemented.
"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.

8.1.3　Roles and Authorization

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

763　　　　　　　　　　　　　　**Table 6 – Operational Roles Supported**

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

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

8.1.4　User Account Management

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

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

772 **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

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

775 **8.1.5 Authentication Mechanisms**

776 Implementations shall support one or two levels of authentication.

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

779   **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	

780 9 Discovery Requirements

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

784 9.1 Network Endpoint Discovery Stage

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

787 9.2 WS Management Access Point Discovery

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

790 9.2.1 WS-Management Identify Method

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

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

```
795  <s:Body>
796     <wsmid:IdentifyResponse>
797        <wsmid:ProtocolVersion> xs:anyURI </wsmid:ProtocolVersion>
798        <wsmid:ProductVendor> xs:string </wsmid:ProductVendor>
799        <wsmid:ProductVersion> xs:string </wsmid:ProductVersion>
800        <SMASH:SMASHVersion> xs:string </SMASH:SMASHVersion>
801        <wsmid:SecurityProfiles>
802            <wsmid:SecurityProfileName> xs:string or URI </wsmid:SecurityProfileName> +
803        </wsmid:SecurityProfiles>
804     </wsmid:IdentifyResponse>
805  </s:Body>
```

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

807   **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

Element	Requirement	Notes
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"
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

808 **9.2.2 wsmid:Identify Security Implementation Requirements**

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

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

813 **9.3 RegisteredSpecification Instance**

814 The SMASH implementation should support an instance of CIM_RegisteredSpecification to indicate
815 support for this version of the specification.

816 Table 10 identifies the element requirements for CIM_RegisteredSpecification.

817 **Table 10 – CIM_RegisteredSpecification Element Requirements**

Element	Requirement	Description
Properties		
InstanceID	Mandatory	Key, see schema definition.
SpecificationType	Mandatory	This property shall have a value of 3 ("Initiative Wrapper ").
RegisteredOrganization	Mandatory	This property shall have a value of 2 (DMTF).
RegisteredName	Mandatory	This property shall have a value of "SMASH".
RegisteredVersion	Mandatory	This property shall have a value of "2.1.0".

Element	Requirement	Description
AdvertiseTypes	Mandatory	Required, see Schema definition.
AdvertiseTypeDescriptions	Mandatory	See Schema definition.
Operations		
GetInstance	Mandatory	
EnumerateInstances	Mandatory	
EnumerateInstanceNames	Mandatory	

818   The instance of CIM_RegisteredSpecification shall be exposed in the interop namespace. The instance to
819   CIM_RegisteredSpecification shall be associated with at least one instance of CIM_RegisteredProfile of
820   one of the mandatory profiles defined in this specification using an instance of
821   CIM_ReferencedSpecification. The Antecedent property of the instance of CIM_ReferencedSpecification
822   shall reference the instance of the CIM_RegisteredProfile. The Dependent property of the instance of
823   CIM_ReferencedSpecification shall reference the instance CIM_RegisteredSpecification.

824 # ANNEX A
825 ## (informative)
826
827 # Change Log

Version	Date	Description
1.0.0	2009-10-14	
2.0.0	2009-08-04	DMTF Standard
2.1.0	2014-12-06	DMTF Standard

828   **Bibliography**

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

832