



1

2

3

4

Document Number: DSP1082

Date: 2011-09-16

Version: 1.0.0

5 **Credential Management Profile**

6 **Document Type: Specification**

7 **Document Status: DMTF Standard**

8 **Document Language: en-US**

9

10 Copyright notice

11 Copyright © 2011 Distributed Management Task Force, Inc. (DMTF). All rights reserved.

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

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26 withdrawn or modified after publication, and shall be indemnified and held harmless by any party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

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

32

Contents

34	Foreword	5
35	Introduction	6
36	1 Scope	7
37	2 Normative references	7
38	3 Terms and definitions	7
39	4 Symbols and abbreviated terms	8
40	5 Synopsis	8
41	6 Description	9
42	6.1 Credential store	10
43	6.2 Credentials	10
44	6.3 Authorization	10
45	7 Implementation	11
46	7.1 Credentials	11
47	7.2 Credential store	11
48	7.3 Utilizing credentials	11
49	7.4 Credential access authorization	12
50	8 Methods	13
51	8.1 Profile conventions for operations	13
52	8.2 CIM_CredentialManagementService	13
53	8.3 CIM_CredentialContext	13
54	8.4 CIM_ConcreteDependency (CIM_CredentialStore)	14
55	8.5 CIM_HostedService	14
56	8.6 CIM_CredentialStore	14
57	8.7 CIM_MemberOfCollection (CIM_Credential)	14
58	8.8 CIM_MemberOfCollection (CIM_CredentialStore)	15
59	8.9 CIM_OwningCollectionElement	15
60	8.10 CIM_ServiceAffectsElement (CIM_CredentialStore)	15
61	8.11 CIM_ServiceAffectsElement (CIM_Credential)	16
62	8.12 CIM_Credential	16
63	8.13 CIM_Identity	16
64	8.14 CIM_AssociatedPrivilege	16
65	9 Use cases	17
66	9.1 Profile registration	17
67	9.2 Determining the credential management service for a credential	17
68	10 CIM elements	18
69	10.1 CIM_Credential	18
70	10.2 CIM_CredentialManagementService	19
71	10.3 CIM_CredentialContext	19
72	10.4 CIM_ConcreteDependency	19
73	10.5 CIM_HostedService	20
74	10.6 CIM_CredentialStore	20
75	10.7 CIM_MemberOfCollection (CIM_Credential)	20
76	10.8 CIM_MemberOfCollection (CIM_CredentialStore)	21
77	10.9 CIM_OwningCollectionElement	21
78	10.10 CIM_ServiceAffectsElement (CIM_CredentialStore)	21
79	10.11 CIM_ServiceAffectsElement (CIM_Credential)	22
80	10.12 CIM_CredentialManagementCapabilities	22
81	10.13 CIM_Identity	22
82	10.14 CIM_AssociatedPrivilege	23
83	ANNEX A (informative) Change Log	24

84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117

Figures

Figure 1 – Credential Management Profile: Class diagram 9
Figure 2 – Profile registration 17

Tables

Table 1 – Related profiles 9
Table 2 – CIM_AssociatedPrivilege.Activities mapping to CIM_CredentialStore operations 12
Table 3 – CIM_AssociatedPrivilege.Activities mapping to CIM_Credential operations 12
Table 8 – Operations: CIM_CredentialContext 13
Table 9 – Operations: CIM_ConcreteDependency 14
Table 10 – Operations: CIM_HostedService 14
Table 11 – Operations: CIM_MemberOfCollection (CIM_Credential) 15
Table 12 – Operations: CIM_MemberOfCollection (CIM_CredentialStore) 15
Table 13 – Operations: CIM_OwningCollectionElement 15
Table 14 – Operations: CIM_ServiceAffectsElement (CIM_CredentialStore) 16
Table 15 – Operations: CIM_ServiceAffectsElement (CIM_Credential) 16
Table 15 – Operations: CIM_ServiceAffectsElement (CIM_Credential) 16
Table 16 – CIM elements: Credential Management Profile 18
Table 17 – Class: CIM_Credential 18
Table 18 – Class: CIM_CredentialManagementService 19
Table 19 – Class: CIM_CredentialContext 19
Table 20 – Class: CIM_ConcreteDependency 19
Table 21 – Class: CIM_HostedService 20
Table 22 – Class: CIM_CredentialStore 20
Table 23 – Class: CIM_MemberOfCollection (CIM_Credential) 20
Table 24 – Class: CIM_MemberOfCollection (CIM_CredentialStore) 21
Table 25 – Class: CIM_OwningCollectionElement 21
Table 26 – Class: CIM_ServiceAffectsElement (CIM_CredentialStore) 22
Table 27 – Class: CIM_ServiceAffectsElement (CIM_Credential) 22
Table 28 – Class: CIM_CredentialManagementCapabilities 22
Table 29 – Class: CIM_Identity 23
Table 30 – Class: CIM_AssociatedPrivilege 23

118

Foreword

119 The *Credential Management Profile* (DSP1082) was prepared by the Security Working Group of DMTF.

120 DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems
121 management and interoperability. For information about the DMTF, see <http://www.dmtf.org>.

122 **Acknowledgments**

123 The DMTF acknowledges the following individuals for their contributions to this document:

- 124 • Khachatur Papanyan – Dell
- 125 • Hemal Shah – Broadcom
- 126 • Sharon Smith – Intel
- 127 • George Ericson – EMC
- 128 • Vincent Perry – Intel
- 129 • David Hines – Intel

130

131

Introduction

132 The information in this specification is intended to be sufficient for a provider or consumer of this data to
133 identify unambiguously the classes, properties, methods, and values that are mandatory to be
134 instantiated and manipulated to represent and manage users and groups that are modeled using the
135 DMTF Common Information Model (CIM) core and extended model definitions.

136 The target audience for this specification is implementers who are writing CIM-based providers or
137 consumers of management interfaces that represent the component described in this document.

138 Document conventions

139 Typographical conventions

140 The following typographical conventions are used in this document:

- 141 • Document titles are marked in *italics*.
- 142 • Important terms that are used for the first time are marked in *italics*.
- 143 • ABNF rules are in `monospaced font`.

144 ABNF usage conventions

145 Format definitions in this document are specified using ABNF (see [RFC5234](#)), with the following
146 deviations:

- 147 • Literal strings are to be interpreted as case-sensitive Unicode characters, as opposed to the
148 definition in [RFC5234](#) that interprets literal strings as case-insensitive US-ASCII characters.

149

150

Credential Management Profile

151 1 Scope

152 The *Credential Management Profile* extends the management capability of the referencing profiles by
153 adding the capability to model credentials including key-based credentials such as PKI public key
154 infrastructure (PKI) and X509 and biometric credentials. The *Credential Management Profile* is not
155 intended to be used to represent the account and principal information. This profile is intended to be the
156 base profile for representing credentials and to be specialized by specific types of credential management
157 profiles.

158 2 Normative references

159 The following referenced documents are indispensable for the application of this document. For dated or
160 versioned references, only the edition cited (including any corrigenda or DMTF update versions) applies.
161 For references without a date or version, the latest published edition of the referenced document
162 (including any corrigenda or DMTF update versions) applies.

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

165 DMTF DSP0004, *CIM Infrastructure Specification 2.6*,
166 http://www.dmtf.org/standards/published_documents/DSP0004_2.6.pdf

167 DMTF DSP1001, *Management Profile Specification Usage Guide 1.0*,
168 http://www.dmtf.org/standards/published_documents/DSP1001_1.0.pdf

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

171 DMTF DSP1096, *Certificate Management Profile 1.0*,
172 http://www.dmtf.org/standards/published_documents/DSP1096_1.0.pdf

173 IETF RFC5234, *Augmented BNF for Syntax Specifications: ABNF*, January 2008,
174 <http://www.ietf.org/rfc/rfc5234.txt>

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

177 3 Terms and definitions

178 In this document, some terms have a specific meaning beyond the normal English meaning. Those terms
179 are defined in this clause.

180 The terms "shall" ("required"), "shall not," "should" ("recommended"), "should not" ("not recommended"),
181 "may," "need not" ("not required"), "can" and "cannot" in this document are to be interpreted as described
182 in [ISO/IEC Directives, Part 2](#), Annex H. The terms in parenthesis are alternatives for the preceding term,
183 for use in exceptional cases when the preceding term cannot be used for linguistic reasons. Note that
184 [ISO/IEC Directives, Part 2](#), Annex H specifies additional alternatives. Occurrences of such additional
185 alternatives shall be interpreted in their normal English meaning.

186 The terms "clause," "subclause," "paragraph," and "annex" in this document are to be interpreted as
187 described in [ISO/IEC Directives, Part 2](#), Clause 5.

188 The terms "normative" and "informative" in this document are to be interpreted as described in [ISO/IEC](#)
189 [Directives, Part 2](#), Clause 3. In this document, clauses, subclauses, or annexes labeled "(informative)" do
190 not contain normative content. Notes and examples are always informative elements.

191 The terms defined in [DSP0004](#), [DSP0200](#), and [DSP1001](#) apply to this document. The following additional
192 terms are used in this document.

193 **3.1**

194 **Container Credential Store**

195 an instance of CIM_CredentialStore associated to the given Credential Instance through
196 CIM_MemberOfCollection association

197 **3.2**

198 **Credential Instance**

199 an instance of a subclass of CIM_Credential

200 **3.3**

201 **Owned Credential Store**

202 a credential store supported by a service that stores credentials used by the service to identify itself to
203 clients

204 Such a credential store is represented by CIM_CredentialStore with the Usage property set to 2 (Owned).

205 **3.4**

206 **Trusted Credential Store**

207 a credential store supported by a service that stores credentials used by the service to verify credentials
208 presented to it by clients

209 Such a credential store is represented by CIM_CredentialStore with the Usage property set to 3
210 (Trusted).

211 **4 Symbols and abbreviated terms**

212 The abbreviations defined in [DSP0004](#), [DSP0200](#), and [DSP1001](#) apply to this document.

213 **5 Synopsis**

214 **Profile Name:** Credential Management

215 **Version:** 1.0.0

216 **Organization:** DMTF

217 **CIM schema version:** 2.29

218 **Central Class:** CIM_CredentialManagementService

219 **Scoping Class:** CIM_System

220 This abstract profile specification shall not be directly implemented; implementations shall be based on a
221 profile specification that specializes the requirements of this profile.

222 The *Credential Management Profile* provides the capability to represent and manage credentials in a
223 managed system.

224 The Central Class of the *Credential Management Profile* shall be CIM_CredentialManagementService.
 225 The Central Instance shall be an instance of CIM_CredentialManagementService. The Scoping Class
 226 shall be CIM_System. The Scoping Instance shall be the instance of CIM_System that is associated with
 227 the Central Instance through the CIM_HostedService association.

228 Table 1 identifies profiles related to this profile.

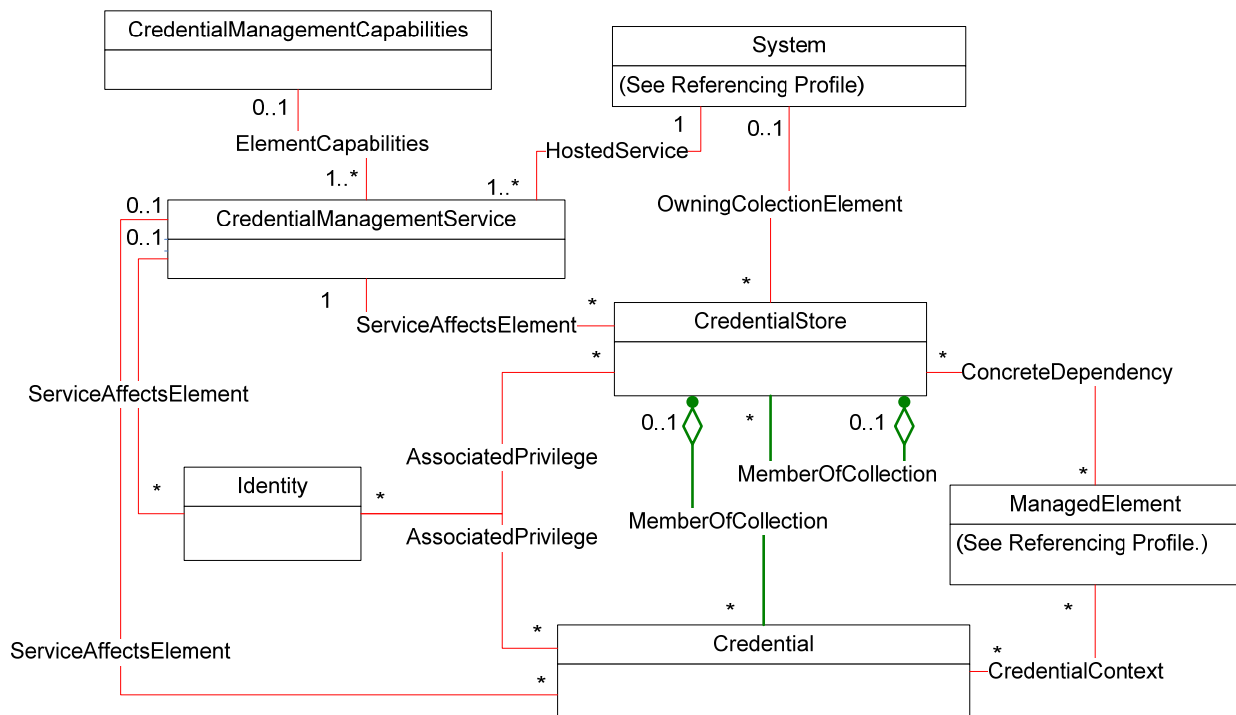
229 **Table 1 – Related profiles**

Profile Name	Organization	Version	Relationship	Behavior
None				

230 **6 Description**

231 The *Credential Management Profile* describes the properties and methods for credential management in
 232 a managed system. This profile does not provide a mechanism for an application to verify authorization.

233 Figure 1 represents the class schema for the profile. For simplicity, the prefix *CIM_* has been removed
 234 from the names of the classes.



235

236 **Figure 1 – Credential Management Profile: Class diagram**

237 The *Credential Management Profile* consists of the representation of the following:

- 238 • credential management services using CIM_CredentialManagementService,
- 239 • credential stores accumulating different types of credentials using CIM_CredentialStore,
- 240 • credentials using CIM_Credential derived classes such as CIM_UnsignedCredential,
- 241 CIM_X509CRL, and CIM_X509Certificate,

- 242
- security principals that have access authorization to the credential stores and credentials.

243 6.1 Credential store

244 A credential store aggregates the key-based credentials and non-key-based credentials of the managed
245 system directly or indirectly by aggregating other credential stores. The following two usage scenarios are
246 predominant with credential stores:

- 247 1) Another entity connects with the managed system service and presents its digital identification for
248 the service to verify. To verify the connected entity's identification, the service looks up a
249 credential store for a matching trusted credential to verify against. In this case, the credential
250 store is identified as a Trusted Credential Store.
- 251 2) The managed system's service connects to an entity where the connected entity requires the
252 managed system's service to present its digital identification. The service's digital identification is
253 stored in the credential store identified as an Owned Credential Store.

254 For example:

- 255 1) A web service running on the managed system utilizes an Owned Credential Store for the X509
256 certificate that is presented to the connecting web client.
- 257 2) LDAP client services on the managed system utilize a Trusted Credential Store to store trusted
258 X509 certificates to verify against the certificate presented by the LDAP server, which the
259 managed system connects to in the process of authentication.

260 Both the Owned Credential Store and the Trusted Credential Store are represented by the
261 CIM_CredentialStore class that is associated to the CIM_ManagedElement class representing the
262 service that utilizes the credential store by the CIM_ConcreteDependency association.

263 6.2 Credentials

264 Credentials are used by the managed system for establishing trust. Credentials are represented by the
265 classes derived from the CIM_Credential class. Credentials are managed using the subclasses of the
266 CIM_CredentialManagementService class.

267 6.3 Authorization

268 Credentials may have different levels of access authorization. An authorized entity is represented by a
269 security principal through the CIM_Identity class. A security principal may be authorized to access the
270 credential store or a particular credential within a credential store. The AssociatedPrivilege association
271 contains the privileges of the security principal as well as references to the credential store, the
272 credential, or both.

273 When an implementation has the ability to authorize on both levels (per credential store and per the
274 credential), the implementation calculates the effective authorization privileges for a particular security
275 principal by combining the credential store and credential authorization privileges together in one of the
276 following ways:

- 277 1) Collection Privileges Override – The effective credential privileges are the credential store
278 privileges overriding the particular credential privileges.
- 279 2) Member Privileges Override – The effective credential privileges are the particular credential
280 privileges overriding the credential store privileges.
- 281 3) Collection-Member Privileges Union – The effective credential privilege is the union of the
282 credential store privileges and the particular credential privileges.

283 4) Collection-Member Privileges Intersection – The effective credential privilege is the intersection
284 of the credential store privileges and the particular credential privileges.

285 The implementation supporting the credential store level and credential level privileges will implement one
286 of the above methodologies for calculating the effective privileges for a credential. The
287 CIM_CredentialManagementCapabilities class will advertise which of the above methodologies an
288 implementation supports.

289 **7 Implementation**

290 This clause details the requirements related to the arrangement of instances and their properties for
291 implementations of this profile.

292 **7.1 Credentials**

293 This clause details representation of a credential. Credentials shall be represented by Credential
294 Instances (see 3.4). Zero or more Credential Instances shall be implemented.

295 Each credential represented by a Credential Instance shall be managed by one and only one credential
296 management service represented by the Central Instance.

297 If the implementation supports a Container Credential Store (see 3.1) as detailed in 7.2, then the
298 Credential Instance may be associated to the Central Instance through the CIM_ServiceAffectsElement
299 association. Otherwise, each Credential Instance shall be associated to the Central Instance through the
300 CIM_ServiceAffectsElement association.

301 **7.2 Credential store**

302 This subclause details the requirements related to representing and managing the credential store. If
303 management or representation of the credential store is supported, the requirements specified in this
304 clause shall be met.

305 **7.2.1 General requirement**

306 Credential stores on a managed system shall be represented by the CIM_CredentialStore class. Zero or
307 more instances of CIM_CredentialStore shall be implemented. The instance of CIM_CredentialStore shall
308 be associated with the CIM_ComputerSystem that represents the managed system by the
309 CIM_OwningCollectionElement association. The instance of CIM_CredentialStore shall be associated
310 with the Central Instance through the CIM_ServiceAffectsElement association.

311 **7.2.2 Credential store hierarchy**

312 Credential stores may contain other credential stores. If the container credential store contains other
313 credential stores, the Container Credential Store shall be associated through the
314 CIM_MemberOfCollection association to the CIM_CredentialStore instances that represent the contained
315 credential stores.

316 **7.3 Utilizing credentials**

317 This subclause details requirements for the managed element that utilizes the credential. If the
318 implementation implements the representation of the managed element utilizing the credentials, the
319 requirements in this subclause shall apply.

320 An instance of a subclass of CIM_ManagedElement shall represent the managed element utilizing the
321 credentials.

322 If the managed element utilizes all the credentials within the credential store, then the instance of a
 323 subclass of CIM_ManagedElement shall be associated with the Container Credential Store using the
 324 CIM_ConcreteDependency association, where the Antecedent property shall reference the Container
 325 Credential Store and the Dependent property shall reference the instance of a subclass of
 326 CIM_ManagedElement.

327 If the managed element utilizes only some individual credentials of the credential store, then the instance
 328 of a subclass of CIM_ManagedElement shall be associated with each instance of the Credential that is
 329 utilized through the CIM_CredentialContext association, where the ElementInContext property shall
 330 reference the Credential Instance and the ElementProvidingContext property shall reference the instance
 331 of a subclass of CIM_ManagedElement.

332 **7.4 Credential access authorization**

333 This subclause details requirements for the authorization of the security principal to access a credential. If
 334 the implementation implements the representation of the credentials access authorization, then the
 335 requirements in this subclause and its subclauses shall apply.

336 **7.4.1 Security principal authorization**

337 If the security principal authorization is implemented, then the CIM_Identity instance representing the
 338 security principal shall be associated with a CIM_Credential instance or CIM_CredentialStore instance
 339 through the CIM_AssociatedPrivilege association.

340 For the CIM_CredentialStore instance referenced by an instance of CIM_AssociatedPrivilege, the
 341 referenced CIM_Identity shall be authorized to perform the operation in the “Credential Operation” column
 342 of Table 2, if and only if the CIM_AssociatedPrivilege.Activities property contains the value from the
 343 “CIM_AssociatedPrivilege.Activities” column of the respective row of Table 2.

344 **Table 2 – CIM_AssociatedPrivilege.Activities mapping to CIM_CredentialStore operations**

CIM_AssociatedPrivilege.Activities	Credential Operation
2 (Create) or 6 (Write)	Import a credential into a credential store
5 (Read)	Export a credential from a credential store
3 (Delete)	Delete a credential from a credential store

345 For the CIM_Credential instance referenced by an instance of CIM_AssociatedPrivilege, the referenced
 346 CIM_Identity shall be authorized to perform the operation in the “Credential Operation” column of Table 3,
 347 if and only if the CIM_AssociatedPrivilege.Activities property contains the value from the
 348 “CIM_AssociatedPrivilege.Activities” column of the respective row of Table 3.

349 **Table 3 – CIM_AssociatedPrivilege.Activities mapping to CIM_Credential operations**

CIM_AssociatedPrivilege. Activities	Credential Operation
6 (Write)	Modify a Credential
5 (Read)	Get a Credential
3 (Delete)	Delete a Credential

350 If the same CIM_Identity instance references both the CIM_CredentialStore instance and the
 351 CIM_Credential instance that is a member of the CIM_CredentialStore instance, then see 7.4.2 for
 352 reconciliation of the privileges.

353 **7.4.2 Credential store and member credential privilege accumulation**

354 If the implementation supports representing access authorization for a credential store, then the
 355 requirements in this subclause shall apply.

356 The CIM_CredentialManagementCapabilities instance shall be implemented and shall be associated to
 357 the CIM_CredentialManagementService instance through the CIM_ElementCapabilities association.

358 The CIM_CredentialManagementCapabilities.CumulativePrivilegeMethodology shall be implemented and
 359 shall be of non-empty, non-null value.

360 **8 Methods**

361 This subclause details the requirements for supporting intrinsic operations and extrinsic methods for the
 362 CIM elements defined by this profile.

363 No extrinsic methods have been defined for this profile.

364 **8.1 Profile conventions for operations**

365 For each profile class (including associations), the implementation requirements for operations, including
 366 those in the following default list, are specified in class-specific subclauses of this clause.

367 The default list of operations is as follows:

- 368 • GetInstance
- 369 • Associators
- 370 • AssociatorNames
- 371 • References
- 372 • ReferenceNames
- 373 • EnumerateInstances
- 374 • EnumerateInstanceNames

375 **8.2 CIM_CredentialManagementService**

376 All operations in the default list in 8.1 shall be implemented as defined in [DSP0200](#).

377 NOTE: Related profiles may define additional requirements on operations for the profile class.

378 **8.3 CIM_CredentialContext**

379 Table 4 lists implementation requirements for operations. If implemented, these operations shall be
 380 implemented as defined in [DSP0200](#). In addition, and unless otherwise stated in Table 4, all operations in
 381 the default list in 8.1 shall be implemented as defined in [DSP0200](#).

382 NOTE: Related profiles may define additional requirements on operations for the profile class.

383 **Table 4 – Operations: CIM_CredentialContext**

Operation	Requirement	Messages
Associators	Unspecified	None
AssociatorNames	Unspecified	None
References	Unspecified	None

ReferenceNames	Unspecified	None
----------------	-------------	------

384 **8.4 CIM_ConcreteDependency (CIM_CredentialStore)**

385 Table 5 lists implementation requirements for operations. If implemented, these operations shall be
 386 implemented as defined in [DSP0200](#). In addition, and unless otherwise stated in Table 5, all operations in
 387 the default list in 8.1 shall be implemented as defined in [DSP0200](#).

388 NOTE: Related profiles may define additional requirements on operations for the profile class.

389 **Table 5 – Operations: CIM_ConcreteDependency**

Operation	Requirement	Messages
Associators	Unspecified	None
AssociatorNames	Unspecified	None
References	Unspecified	None
ReferenceNames	Unspecified	None

390 **8.5 CIM_HostedService**

391 Table 6 lists implementation requirements for operations. If implemented, these operations shall be
 392 implemented as defined in [DSP0200](#). In addition, and unless otherwise stated in Table 6, all operations in
 393 the default list in 8.1 shall be implemented as defined in [DSP0200](#).

394 NOTE: Related profiles may define additional requirements on operations for the profile class.

395 **Table 6 – Operations: CIM_HostedService**

Operation	Requirement	Messages
Associators	Unspecified	None
AssociatorNames	Unspecified	None
References	Unspecified	None
ReferenceNames	Unspecified	None

396 **8.6 CIM_CredentialStore**

397 All operations in the default list in 8.1 shall be implemented as defined in [DSP0200](#).

398 NOTE: Related profiles may define additional requirements on operations for the profile class.

399 **8.7 CIM_MemberOfCollection (CIM_Credential)**

400 Table 7 lists implementation requirements for operations. If implemented, these operations shall be
 401 implemented as defined in [DSP0200](#). In addition, and unless otherwise stated in Table 7, all operations in
 402 the default list in 8.1 shall be implemented as defined in [DSP0200](#).

403 NOTE: Related profiles may define additional requirements on operations for the profile class.

404

Table 7 – Operations: CIM_MemberOfCollection (CIM_Credential)

Operation	Requirement	Messages
Associators	Unspecified	None
AssociatorNames	Unspecified	None
References	Unspecified	None
ReferenceNames	Unspecified	None

405 **8.8 CIM_MemberOfCollection (CIM_CredentialStore)**

406 Table 8 lists implementation requirements for operations. If implemented, these operations shall be
 407 implemented as defined in [DSP0200](#). In addition, and unless otherwise stated in Table 8, all operations in
 408 the default list in 8.1 shall be implemented as defined in [DSP0200](#).

409 NOTE: Related profiles may define additional requirements on operations for the profile class.

410

Table 8 – Operations: CIM_MemberOfCollection (CIM_CredentialStore)

Operation	Requirement	Messages
Associators	Unspecified	None
AssociatorNames	Unspecified	None
References	Unspecified	None
ReferenceNames	Unspecified	None

411 **8.9 CIM_OwningCollectionElement**

412 Table 9 lists implementation requirements for operations. If implemented, these operations shall be
 413 implemented as defined in [DSP0200](#). In addition, and unless otherwise stated in Table 9, all operations in
 414 the default list in 8.1 shall be implemented as defined in [DSP0200](#).

415 NOTE: Related profiles may define additional requirements on operations for the profile class.

416

Table 9 – Operations: CIM_OwningCollectionElement

Operation	Requirement	Messages
Associators	Unspecified	None
AssociatorNames	Unspecified	None
References	Unspecified	None
ReferenceNames	Unspecified	None

417 **8.10 CIM_ServiceAffectsElement (CIM_CredentialStore)**

418 Table 10 lists implementation requirements for operations. If implemented, these operations shall be
 419 implemented as defined in [DSP0200](#). In addition, and unless otherwise stated in Table 10, all operations
 420 in the default list in 8.1 shall be implemented as defined in [DSP0200](#).

421 NOTE: Related profiles may define additional requirements on operations for the profile class.

422

Table 10 – Operations: CIM_ServiceAffectsElement (CIM_CredentialStore)

Operation	Requirement	Messages
Associators	Unspecified	None
AssociatorNames	Unspecified	None
References	Unspecified	None
ReferenceNames	Unspecified	None

423 **8.11 CIM_ServiceAffectsElement (CIM_Credential)**

424 Table 11 lists implementation requirements for operations. If implemented, these operations shall be
 425 implemented as defined in [DSP0200](#). In addition, and unless otherwise stated in Table 11, all operations
 426 in the default list in 8.1 shall be implemented as defined in [DSP0200](#).

427 NOTE: Related profiles may define additional requirements on operations for the profile class.

428

Table 11 – Operations: CIM_ServiceAffectsElement (CIM_Credential)

Operation	Requirement	Messages
Associators	Unspecified	None
AssociatorNames	Unspecified	None
References	Unspecified	None
ReferenceNames	Unspecified	None

429 **8.12 CIM_Credential**

430 All operations in the default list in 8.1 shall be implemented as defined in [DSP0200](#).

431 NOTE: Related profiles may define additional requirements on operations for the profile class.

432 **8.13 CIM_Identity**

433 All operations in the default list in 8.1 shall be implemented as defined in [DSP0200](#).

434 NOTE: Related profiles may define additional requirements on operations for the profile class.

435 **8.14 CIM_AssociatedPrivilege**

436 Table 12 lists implementation requirements for operations. If implemented, these operations shall be
 437 implemented as defined in [DSP0200](#). In addition, and unless otherwise stated in Table 12, all operations
 438 in the default list in 8.1 shall be implemented as defined in [DSP0200](#).

439 NOTE: Related profiles may define additional requirements on operations for the profile class.

440

Table 12 – Operations: CIM_AssociatedPrivilege

Operation	Requirement	Messages
Associators	Unspecified	None
AssociatorNames	Unspecified	None
References	Unspecified	None
ReferenceNames	Unspecified	None

441

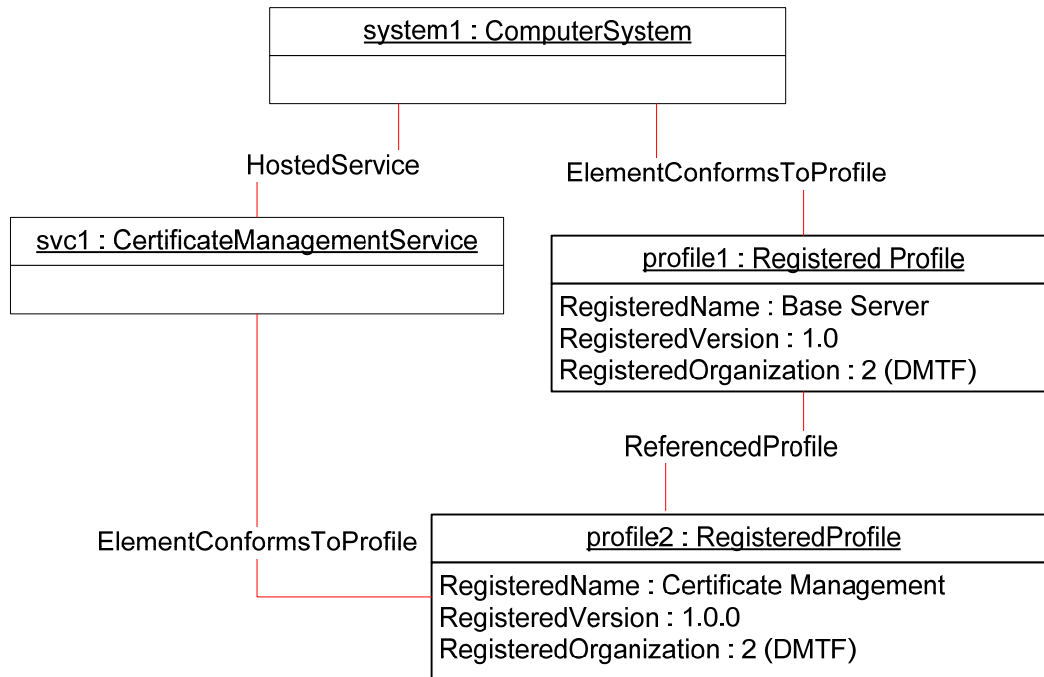
442 **9 Use cases**

443 This clause contains object diagrams and use cases for the *Credential Management Profile*. The contents
 444 of this clause are for informative purposes only and do not constitute normative requirements for
 445 implementations of this specification.

446 **9.1 Profile registration**

447 Figure 2 describes one of the ways that the implementation can advertise the instantiation of the profile
 448 specialized from the *Credential Management Profile*. Using the scoping instance methodology as
 449 described in the [Profile Registration Profile](#), profile2 contains the version information for the [Certificate](#)
 450 [Management Profile](#) implementation.

451 Note that because the *Credential Management Profile* is an abstract profile, the Profile Registration
 452 Profile does not allow the *Credential Management Profile*'s direct advertisement but rather only its
 453 specialized profiles such as the [Certificate Management Profile](#) can be advertised as shown in the figure
 454 below.



455

456 **Figure 2 – Profile registration**

457 **9.2 Determining the credential management service for a credential**

458 The client can determine the credential management service for a particular credential as follows:

- 459 1) Select the instance of CIM_CredentialManagementService associated with the Credential Instance
 460 representing the particular credential through the CIM_ServiceAffectsElement association.
- 461 2) If the instance of CIM_CredentialManagementService exists, then the selected instance represents
 462 the credential management service. Otherwise, select the container credential store of the Credential
 463 Instance.

- 464 3) Select the instance of CIM_CredentialManagementService associated with the Container Credential
- 465 Store through the CIM_ServiceAffectsElement association, which represents the credential
- 466 management service.
- 467 4) The selected instance of CIM_CredentialManagementService represents the credential management
- 468 service.

469 **10 CIM elements**

470 Table 13 shows the instances of CIM elements for this profile. Instances of the CIM elements shall be
 471 implemented as described in Table 13. Clauses 7 (“Implementation”) and 8 (“Methods”) may impose
 472 additional requirements on these elements.

473 **Table 13 – CIM elements: Credential Management Profile**

Element Name	Requirement	Description
Classes		
CIM_AssociatedPrivilege	Conditional	See 10.14.
CIM_Credential	Mandatory	See 10.1 and 7.1.
CIM_CredentialManagementService	Mandatory	See 10.2.
CIM_CredentialManagementCapabilities	Optional	See 7.4.2 and 10.12.
CIM_CredentialContext	Optional	See 10.3 and 7.3.
CIM_ConcreteDependency	Optional	See 10.4 and 7.3.
CIM_HostedService	Mandatory	See 10.5.
CIM_CredentialStore	Optional	See 10.6 and 7.2.
CIM_Identity	Optional	See 10.13.
CIM_MemberOfCollection (CIM_Credential)	Optional	See 10.7 and 7.1.
CIM_MemberOfCollection (CIM_CredentialStore)	Optional	See 10.8 and 7.2.2.
CIM_OwningCollectionElement	Conditional	See 10.9 and 7.2.
CIM_ServiceAffectsElement (CIM_CredentialStore)	Conditional	See 10.10 and 7.1.
CIM_ServiceAffectsElement (CIM_Credential)	Conditional	See 10.11 and 7.1.
Indications		
None defined in this profile		

474 **10.1 CIM_Credential**

475 CIM_Credential is used to represent the credentials on the managed system. Table 14 details the
 476 requirements for instances of CIM_Credential.

477 **Table 14 – Class: CIM_Credential**

Elements	Requirement	Notes
ElementName	Mandatory	Pattern ".*"

478 **10.2 CIM_CredentialManagementService**

479 CIM_CredentialManagementService is used to manage credentials represented by Credential Instances.
 480 Table 15 details the requirements for instances of CIM_CredentialManagementService.

481 **Table 15 – Class: CIM_CredentialManagementService**

Elements	Requirement	Notes
SystemCreationClassName	Mandatory	Key
CreationClassName	Mandatory	Key
SystemName	Mandatory	Key
Name	Mandatory	Key
ElementName	Mandatory	Pattern ".*"

482 **10.3 CIM_CredentialContext**

483 CIM_CredentialContext is used to associate a Credential Instance with an instance of a subclass of
 484 CIM_ManagedElement that represents the managed element that utilizes the credential. Table 16 details
 485 the requirements for instances of CIM_CredentialContext.

486 **Table 16 – Class: CIM_CredentialContext**

Elements	Requirement	Notes
ElementInContext	Mandatory	Key: This property shall be a reference to the Credential Instance. Cardinality * indicating zero or more references
ElementProvidingContext	Mandatory	Key: This property shall be a reference to the instance of the subclass of CIM_ManagedElement. Cardinality * indicating zero or more references

487 **10.4 CIM_ConcreteDependency**

488 CIM_ConcreteDependency is used to associate an instance of a CIM_ManagedElement subclass with
 489 instances of CIM_CredentialStore that the managed element utilizes. Table 17 details the requirements
 490 for instances of CIM_ConcreteDependency.

491 **Table 17 – Class: CIM_ConcreteDependency**

Elements	Requirement	Notes
Antecedent	Mandatory	Key: This property shall be a reference to the CIM_ManagedElement. Cardinality * indicating zero or more references
Dependent	Mandatory	Key: This property shall be a reference to the CIM_CredentialStore. Cardinality * indicating zero or more references

492 **10.5 CIM_HostedService**

493 CIM_HostedService is used to associate an instance of CIM_CredentialManagementService with the
 494 Scoping Class. Table 18 details the requirements for instances of CIM_HostedService.

495 **Table 18 – Class: CIM_HostedService**

Elements	Requirement	Notes
Antecedent	Mandatory	Key: This property shall be a reference to the Scoping Instance. Cardinality 1 indicating one and only one reference
Dependent	Mandatory	Key: This property shall be a reference to the Central Instance. Cardinality 1..* indicating one or more references

496 **10.6 CIM_CredentialStore**

497 CIM_CredentialStore is used to represent the key store that accumulates credentials represented by
 498 Credential Instances. Table 19 details the requirements for instances of CIM_CredentialStore.

499 **Table 19 – Class: CIM_CredentialStore**

Elements	Requirement	Notes
InstanceID	Mandatory	Key
ElementName	Mandatory	Pattern ".**"
Usage	Mandatory	None

500 **10.7 CIM_MemberOfCollection (CIM_Credential)**

501 CIM_MemberOfCollection is used to aggregate the instances of CIM_Credential with the instance of
 502 CIM_CredentialStore.

503 Table 20 contains the requirements for elements of this class.

504 **Table 20 – Class: CIM_MemberOfCollection (CIM_Credential)**

Elements	Requirement	Notes
Collection	Mandatory	Key: This property shall reference an instance of CIM_CredentialStore. Cardinality 1 indicating one and only one reference
Member	Mandatory	Key: This property shall reference a Credential Instance. Cardinality * indicating zero or more references

505 **10.8 CIM_MemberOfCollection (CIM_CredentialStore)**

506 CIM_MemberOfCollection is used to aggregate the instances of CIM_CredentialStore with the instance of
 507 CIM_CredentialStore.

508 Table 21 provides information about the properties of CIM_MemberOfCollection.

509 **Table 21 – Class: CIM_MemberOfCollection (CIM_CredentialStore)**

Properties	Requirement	Notes
Collection	Mandatory	Key: This property shall reference an instance of CIM_CredentialStore. Cardinality 0..1 indicating one and only one reference
Member	Mandatory	Key: This property shall reference an instance of CIM_CredentialStore. Cardinality * indicating zero or more references

510 **10.9 CIM_OwningCollectionElement**

511 CIM_OwningCollectionElement is used to associate a CIM_CredentialStore instance with its scoping
 512 CIM_System instance. If the CIM_CredentialStore instance exists, the CIM_OwningCollectionElement
 513 shall be implemented.

514 Table 22 provides information about the properties of CIM_OwningCollectionElement.

515 **Table 22 – Class: CIM_OwningCollectionElement**

Properties	Requirement	Notes
OwningElement	Mandatory	Key: This property shall reference the Scoping Instance of this profile. Cardinality 0..1 indicating at most one reference
OwnedElement	Mandatory	Key: This property shall be an instance of CIM_CredentialStore. Cardinality * indicating zero or more references

516 **10.10 CIM_ServiceAffectsElement (CIM_CredentialStore)**

517 CIM_ServiceAffectsElement is used to associate an instance of CIM_CredentialManagementService with
 518 an instance of CIM_CredentialStore that represents a credential store that could be managed using the
 519 service. If the CIM_CredentialStore instance exists, CIM_ServiceAffectsElement shall be implemented.

520 Table 23 contains the requirements for elements of this class.

521 **Table 23 – Class: CIM_ServiceAffectsElement (CIM_CredentialStore)**

Elements	Requirement	Notes
AffectedElement	Mandatory	Key: This property shall reference the instance of CIM_CredentialStore. Cardinality * indicating zero or more references
AffectingElement	Mandatory	Key: This property shall reference the instance of CIM_CredentialManagementService. Cardinality 1 indicating one reference
ElementEffects	Mandatory	Matches 5 (Manages)

522 **10.11 CIM_ServiceAffectsElement (CIM_Credential)**

523 CIM_ServiceAffectsElement is used to associate an instance of CIM_CredentialManagementService with
524 a Credential Instance. If the credential store is not implemented, CIM_ServiceAffectsElement shall be
525 implemented.

526 Table 24 contains the requirements for elements of this class.

527 **Table 24 – Class: CIM_ServiceAffectsElement (CIM_Credential)**

Elements	Requirement	Notes
AffectedElement	Mandatory	Key: This property shall reference the instance of CIM_Credential. Cardinality * indicating zero or more references
AffectingElement	Mandatory	Key: This property shall reference the instance of CIM_CredentialManagementService. Cardinality 0..1 indicating zero or one reference
ElementEffects	Mandatory	Matches 5 (Manages)

528 **10.12 CIM_CredentialManagementCapabilities**

529 CIM_CredentialManagementCapabilities is used to represent the management capabilities for
530 credentials.

531 Table 25 details the requirements for instances of CIM_CredentialManagementCapabilities.

532 **Table 25 – Class: CIM_CredentialManagementCapabilities**

Elements	Requirement	Notes
InstanceID	Mandatory	None
SupportedMethods	Mandatory	None
CumulativePrivilegeMethodology	Optional	See 7.4.2.

533 **10.13 CIM_Identity**

534 CIM_Identity is used to represent the security principal of an account that has access authorization to
535 credentials or credential stores.

536 Table 26 details the requirements for instances of CIM_Identity.

537

Table 26 – Class: CIM_Identity

Elements	Requirement	Notes
Instanceld	Mandatory	Key
ElementName	Mandatory	pattern ".*"

538 **10.14 CIM_AssociatedPrivilege**

539 CIM_AssociatedPrivilege is used to associate the security principal with the credential or credential store
 540 to which the security principal has access authorization.

541 CIM_AssociatedPrivilege is conditional and shall be implemented if CIM_Identity is implemented.

542 Table 27 contains the requirements for elements of CIM_AssociatedPrivilege.

543

Table 27 – Class: CIM_AssociatedPrivilege

Elements	Requirement	Notes
Target	Mandatory	Key: This property shall contain a reference to an instance of CIM_Credential or CIM_CredentialStore. Cardinality *
Subject	Mandatory	Key: This property shall contain a reference to an instance of CIM_Identity. Cardinality *
Activities	Mandatory	See 7.4.1.

544

545

546
547
548
549
550

ANNEX A (informative)

Change Log

Version	Date	Description
1.0.0	2011-09-16	DMTF Standard released

551
552