**Document Number: DSP1082**

**Date: 2011-09-16**

**Version: 1.0.0**

# Credential Management Profile

**Document Type: Specification**

**Document Status: DMTF Standard**

**Document Language: en-US**

Copyright notice

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

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

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patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a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

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

33 # Contents

## Figures



## Tables

# Foreword

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

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

## Acknowledgments

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

- Khachatur Papanyan – Dell
- Hemal Shah – Broadcom
- Sharon Smith – Intel
- George Ericson – EMC
- Vincent Perry – Intel
- David Hines – Intel

# Introduction

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

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

## Document conventions

### Typographical conventions

The following typographical conventions are used in this document:

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

### ABNF usage conventions

Format definitions in this document are specified using ABNF (see RFC5234), with the following deviations:

- Literal strings are to be interpreted as case-sensitive Unicode characters, as opposed to the definition in RFC5234 that interprets literal strings as case-insensitive US-ASCII characters.

# Credential Management Profile

## 1 Scope

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

## 2 Normative references

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

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

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

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

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

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

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

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

## 3 Terms and definitions

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

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

The terms "clause," "subclause," "paragraph," and "annex" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 5.

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

The terms defined in DSP0004, DSP0200, and DSP1001 apply to this document. The following additional terms are used in this document.

### 3.1

**Container Credential Store**

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

### 3.2

**Credential Instance**

an instance of a subclass of CIM_Credential

### 3.3

**Owned Credential Store**

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

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

### 3.4

**Trusted Credential Store**

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

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

## 4 Symbols and abbreviated terms

The abbreviations defined in DSP0004, DSP0200, and DSP1001 apply to this document.

## 5 Synopsis

**Profile Name:** Credential Management

**Version:** 1.0.0

**Organization:** DMTF

**CIM schema version:** 2.29

**Central Class:** CIM_CredentialManagementService

**Scoping Class:** CIM_System

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

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

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

Table 1 identifies profiles related to this profile.

**Table 1 – Related profiles**

| Profile Name | Organization | Version | Relationship | Behavior |
|---|---|---|---|---|
| None | | | | |

# 6 Description

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

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

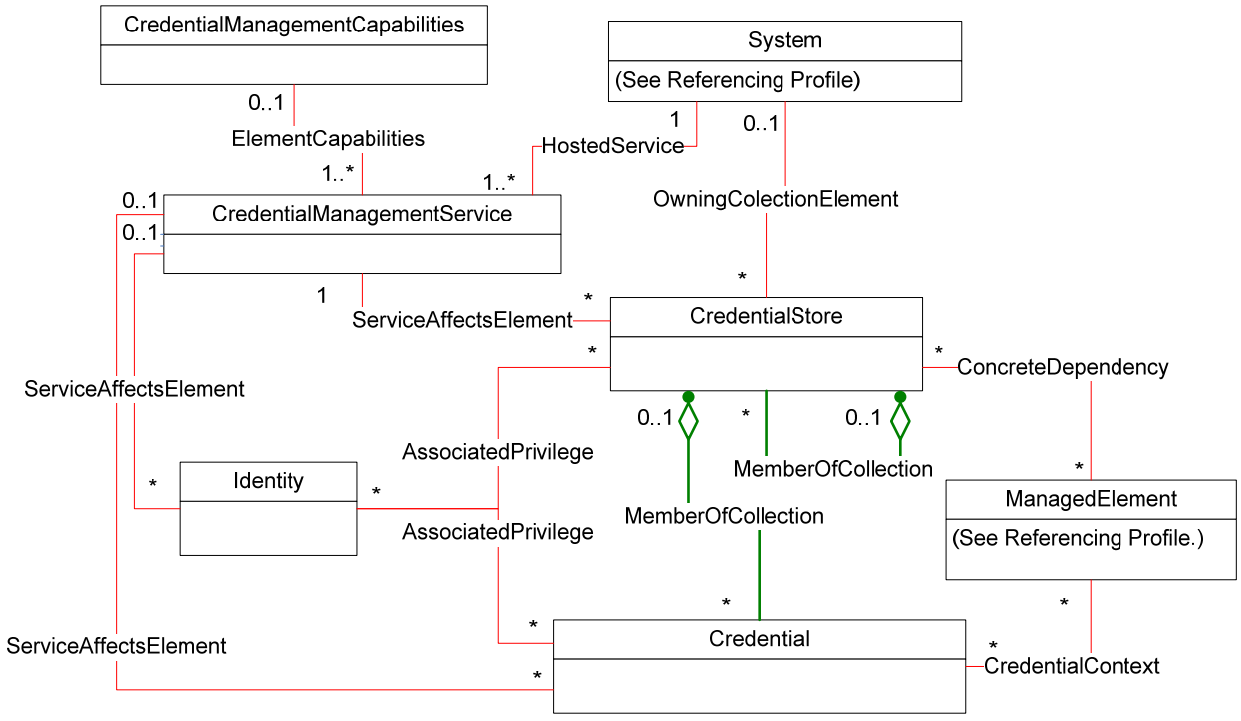


**Figure 1 – Credential Management Profile: Class diagram**

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

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

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

## 6.1 Credential store

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

1) Another entity connects with the managed system service and presents its digital identification for the service to verify. To verify the connected entity's identification, the service looks up a credential store for a matching trusted credential to verify against. In this case, the credential store is identified as a Trusted Credential Store.

2) The managed system's service connects to an entity where the connected entity requires the managed system's service to present its digital identification. The service's digital identification is stored in the credential store identified as an Owned Credential Store.

For example:

1) A web service running on the managed system utilizes an Owned Credential Store for the X509 certificate that is presented to the connecting web client.

2) LDAP client services on the managed system utilize a Trusted Credential Store to store trusted X509 certificates to verify against the certificate presented by the LDAP server, which the managed system connects to in the process of authentication.

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

## 6.2 Credentials

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

## 6.3 Authorization

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

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

1) Collection Privileges Override – The effective credential privileges are the credential store privileges overriding the particular credential privileges.

2) Member Privileges Override – The effective credential privileges are the particular credential privileges overriding the credential store privileges.

3) Collection-Member Privileges Union – The effective credential privilege is the union of the credential store privileges and the particular credential privileges.

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

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

# 7 Implementation

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

## 7.1 Credentials

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

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

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

## 7.2 Credential store

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

### 7.2.1 General requirement

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

### 7.2.2 Credential store hierarchy

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

## 7.3 Utilizing credentials

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

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

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

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

## 7.4 Credential access authorization

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

### 7.4.1 Security principal authorization

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

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

**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 |

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

**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 |

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

### 7.4.2 Credential store and member credential privilege accumulation

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

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

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

# 8 Methods

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

No extrinsic methods have been defined for this profile.

## 8.1 Profile conventions for operations

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

The default list of operations is as follows:

- GetInstance
- Associators
- AssociatorNames
- References
- ReferenceNames
- EnumerateInstances
- EnumerateInstanceNames

## 8.2 CIM_CredentialManagementService

All operations in the default list in 8.1 shall be implemented as defined in DSP0200.

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

## 8.3 CIM_CredentialContext

Table 4 lists implementation requirements for operations. If implemented, these operations shall be implemented as defined in DSP0200. In addition, and unless otherwise stated in Table 4, all operations in the default list in 8.1 shall be implemented as defined in DSP0200.

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

**Table 4 – Operations: CIM_CredentialContext**

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

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

## 8.4 CIM_ConcreteDependency (CIM_CredentialStore)

Table 5 lists implementation requirements for operations. If implemented, these operations shall be implemented as defined in DSP0200. In addition, and unless otherwise stated in Table 5, all operations in the default list in 8.1 shall be implemented as defined in DSP0200.

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

**Table 5 – Operations: CIM_ConcreteDependency**

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

## 8.5 CIM_HostedService

Table 6 lists implementation requirements for operations. If implemented, these operations shall be implemented as defined in DSP0200. In addition, and unless otherwise stated in Table 6, all operations in the default list in 8.1 shall be implemented as defined in DSP0200.

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

**Table 6 – Operations: CIM_HostedService**

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

## 8.6 CIM_CredentialStore

All operations in the default list in 8.1 shall be implemented as defined in DSP0200.

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

## 8.7 CIM_MemberOfCollection (CIM_Credential)

Table 7 lists implementation requirements for operations. If implemented, these operations shall be implemented as defined in DSP0200. In addition, and unless otherwise stated in Table 7, all operations in the default list in 8.1 shall be implemented as defined in DSP0200.

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

# 9 Use cases

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

## 9.1 Profile registration

Figure 2 describes one of the ways that the implementation can advertise the instantiation of the profile specialized from the *Credential Management Profile*. Using the scoping instance methodology as described in the *Profile Registration Profile*, profile2 contains the version information for the *Certificate Management Profile* implementation.

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

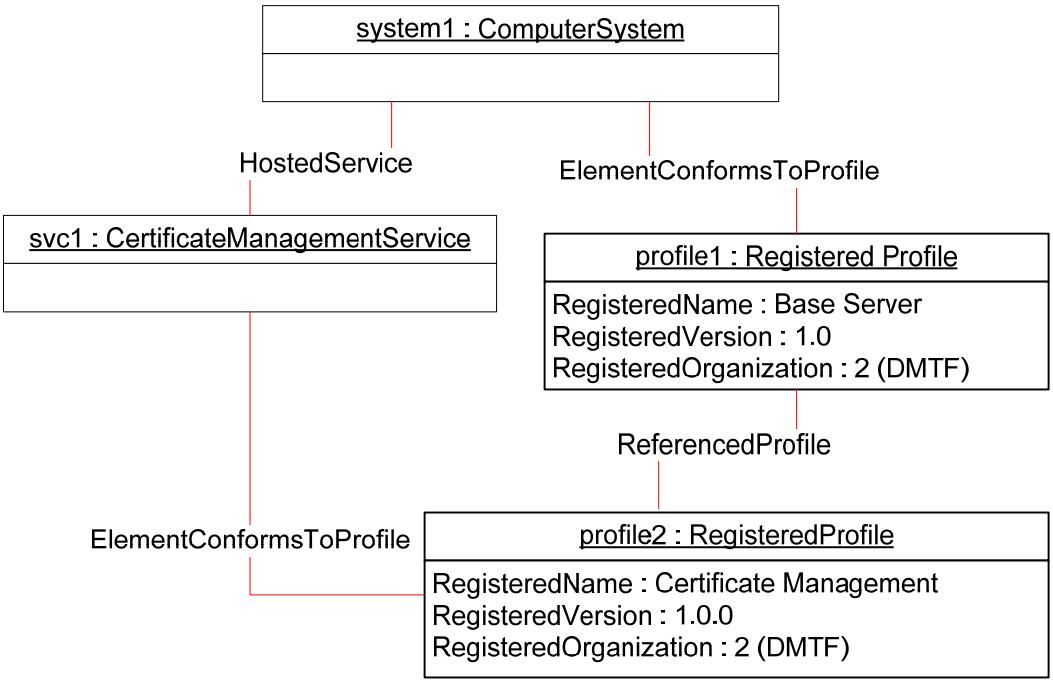


**Figure 2 – Profile registration**

## 9.2 Determining the credential management service for a credential

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

1) Select the instance of CIM_CredentialManagementService associated with the Credential Instance representing the particular credential through the CIM_ServiceAffectsElement association.

2) If the instance of CIM_CredentialManagementService exists, then the selected instance represents the credential management service. Otherwise, select the container credential store of the Credential Instance.

3) Select the instance of CIM_CredentialManagementService associated with the Container Credential Store through the CIM_ServiceAffectsElement association, which represents the credential management service.

4) The selected instance of CIM_CredentialManagementService represents the credential management service.

# 10 CIM elements

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

**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 | | |

## 10.1 CIM_Credential

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

**Table 14 – Class: CIM_Credential**

| Elements | Requirement | Notes |
|---|---|---|
| ElementName | Mandatory | Pattern ".*" |

## 10.2 CIM_CredentialManagementService

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

**Table 15 – Class: CIM_CredentialManagementService**

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

## 10.3 CIM_CredentialContext

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

**Table 16 – Class: CIM_CredentialContext**

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

## 10.4 CIM_ConcreteDependency

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

**Table 17 – Class: CIM_ConcreteDependency**

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

## 10.5 CIM_HostedService

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

**Table 18 – Class: CIM_HostedService**

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

## 10.6 CIM_CredentialStore

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

**Table 19 – Class: CIM_CredentialStore**

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

## 10.7 CIM_MemberOfCollection (CIM_Credential)

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

Table 20 contains the requirements for elements of this class.

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

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

## 10.8 CIM_MemberOfCollection (CIM_CredentialStore)

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

Table 21 provides information about the properties of CIM_MemberOfCollection.

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

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

## 10.9 CIM_OwningCollectionElement

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

Table 22 provides information about the properties of CIM_OwningCollectionElement.

**Table 22 – Class: CIM_OwningCollectionElement**

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

## 10.10 CIM_ServiceAffectsElement (CIM_CredentialStore)

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

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.<br>Cardinality * indicating zero or more references |
| AffectingElement | Mandatory | **Key**: This property shall reference the instance of CIM_CredentialManagementService.<br>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.<br>Cardinality * indicating zero or more references |
| AffectingElement | Mandatory | **Key**: This property shall reference the instance of CIM_CredentialManagementService.<br>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 |
|---|---|---|
| InstanceId | 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.<br>Cardinality * |
| Subject | Mandatory | **Key:** This property shall contain a reference to an instance of CIM_Identity.<br>Cardinality * |
| Activities | Mandatory | See 7.4.1. |

544

545

# ANNEX A
# (informative)

## Change Log

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