

Security Credential Modeling in DMTF Security Working Group

Jon Hass
Dell Inc.

August 2008



Disclaimer



The DMTF was formed to lead the development, adoption and unification of management standards and initiatives for desktop, enterprise and internet environments

- The information in this presentation represents a snapshot of work in progress within the DMTF.
- This information is subject to change. The Standard Specifications remain the normative reference for all information.
- For additional information, see the Distributed Management Task Force (DMTF) Web site.
<http://www.dmtf.org>.

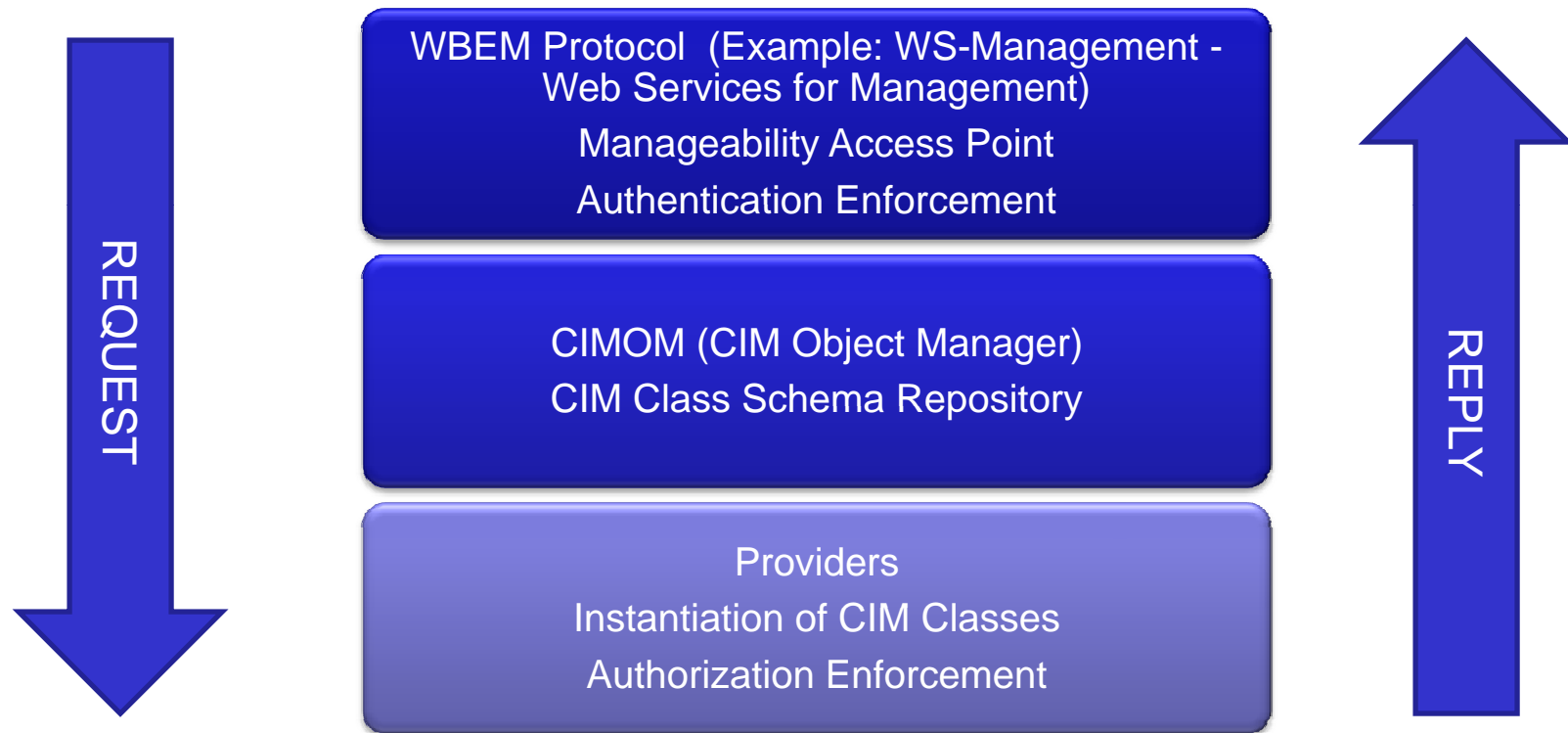
Agenda

- Introduction to CIM and DMTF
- Architecture for CIM Implementations
- Security Credential Class Schemas
- Security Credential Profiles
- Future Work
- Additional Materials

Introduction to CIM

- CIM (Common Information Model) is a model for describing overall management information in a network/enterprise environment
 - Object Oriented class definitions (properties and methods)
 - Association classes interlink object class definitions
 - Classes derived through inheritance hierarchy
 - Starts with CIM_ManagedElement
 - Over 1200 classes in Core Schema
- CIM is the most comprehensive public data model available
 - Covers hardware, software, applications, policies, security, eventing
 - Extensible and flexible
- Provides basis for a consistent data model for across products
 - Applicable to Systems, Components, Devices, Networks, and Software
- Enables standardization of the CONTENT of product management interfaces

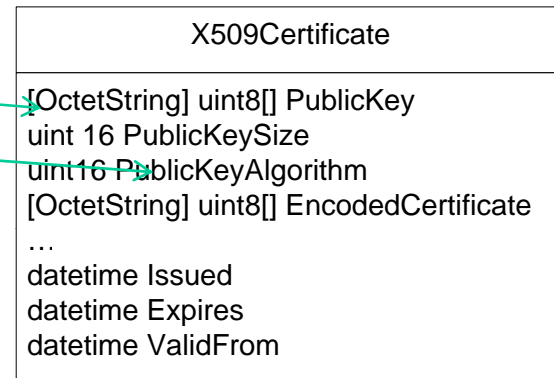
Layers of CIM Instrumentation



CIM Class Attributes and Operations

Class Attributes

- Qualifiers
- Properties
- Methods



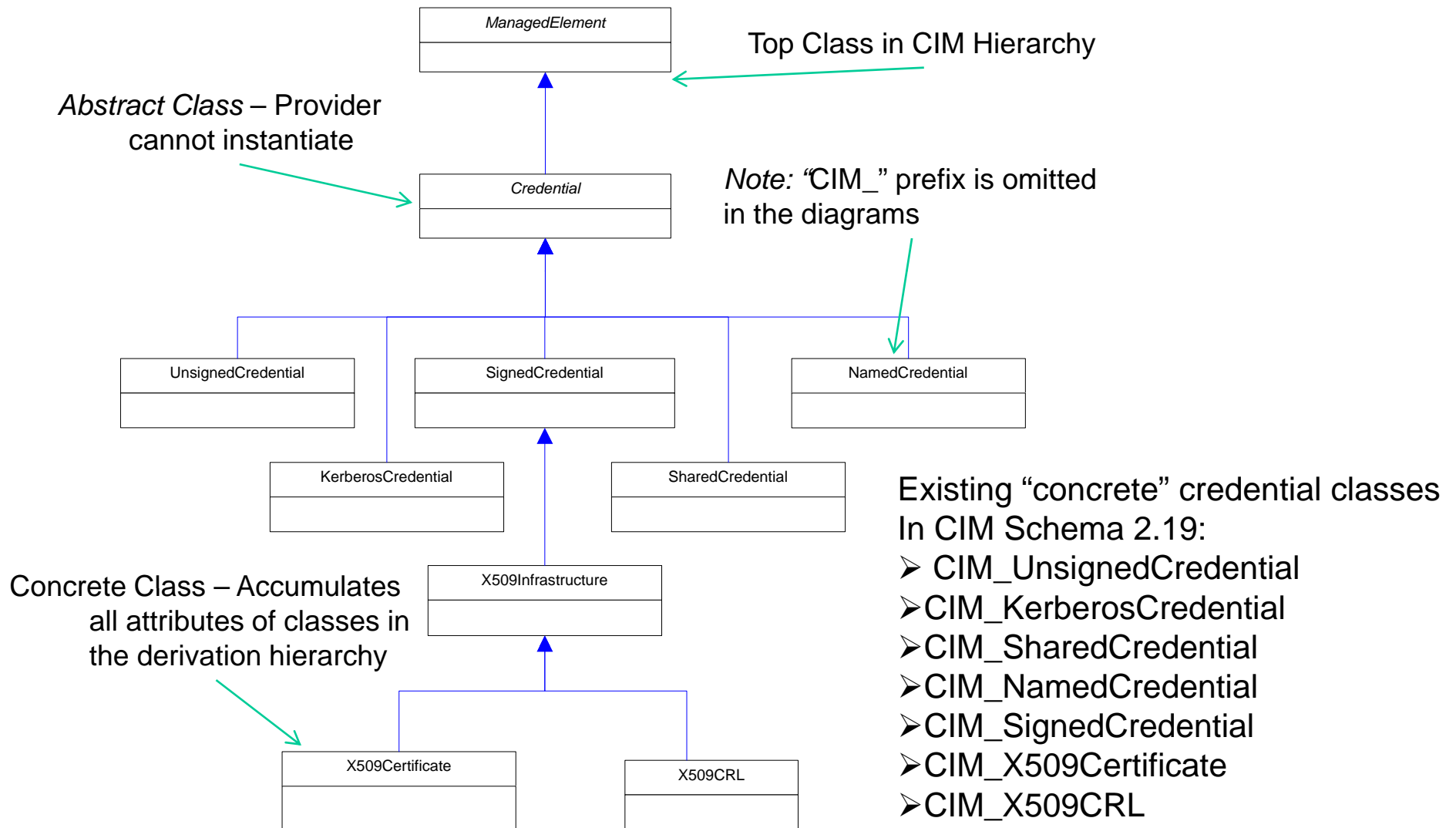
Instance Operations

- Intrinsic: common methods shared by all instances
 - GetInstance
 - EnumerateInstances
 - ModifyInstance
 - CreateInstance
 - DeleteInstance
 - Associators
- Extrinsic: specific methods defined in related service classes or in individual classes

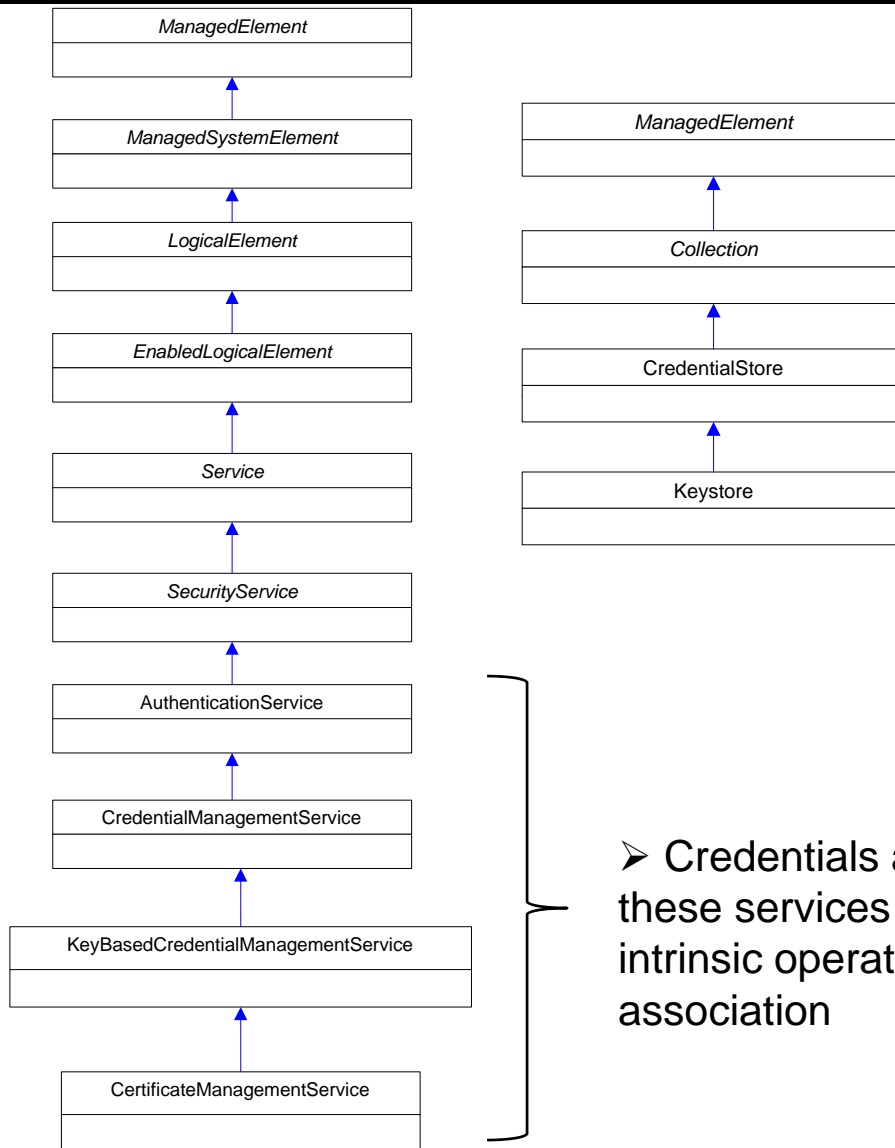




Security Credential CIM Schema



Credential Service and Store CIM Schema Derivation



➤ Credentials stored in a CredentialStore can be listed using the Associators intrinsic operation filtered on MemberOfCollection with proper authorization

➤ Resources (represented by ManagedElements) that have associated credential stores can be listed using the Associators intrinsic operation filtered on ConcreteDependency

➤ Credentials and CredentialStores that are managed by these services can be listed by using the Associators intrinsic operation filtered on ServiceAffectsElement association



Credential Profiles Work in DMTF Security WG

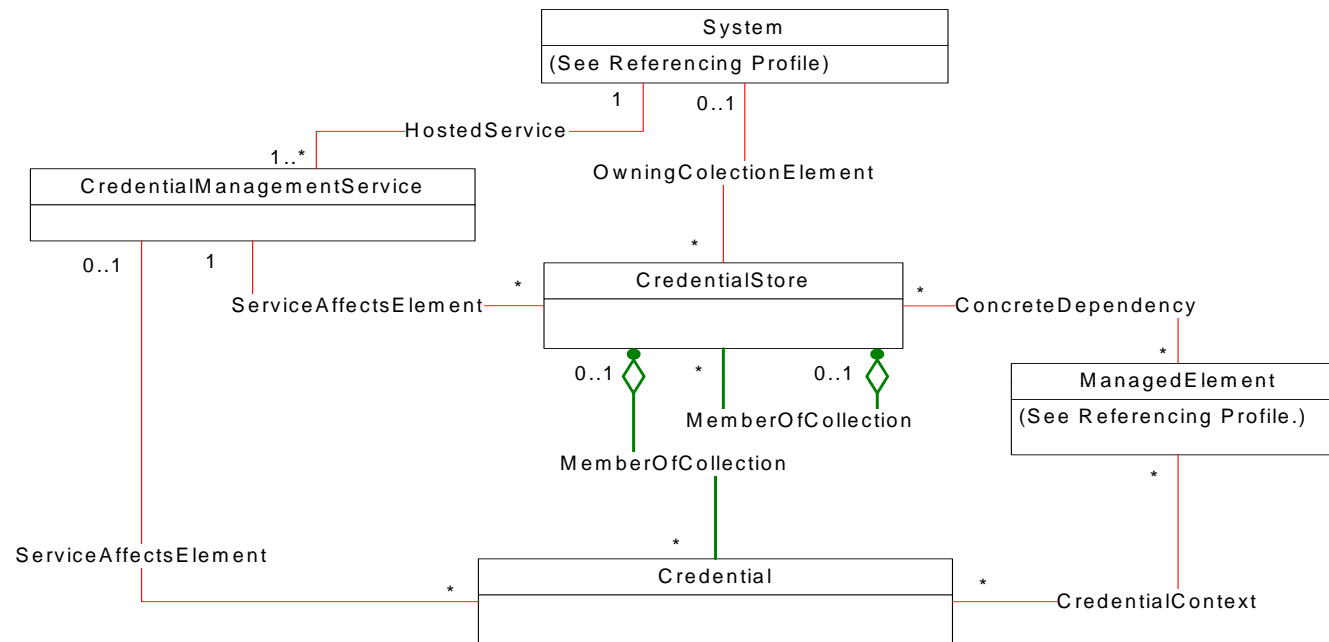
- What is a Profile?
 - A specification that normatively defines the data model interface between a WBEM Server and a WBEM Client.
 - Leverages CIM schema
 - Defines the behavioral relationships
 - Requirements are only for the WBEM Server
 - Scoped to a specific management domain
- Includes Abstract and Specialized Profiles
 - Abstract Profile – Includes common modeling definitions and behavior that will be equivalent across Specialized Profiles that derive from it
 - Specialized Profile – Inherits from an Abstract Profile where appropriate and targets specifying the model behavior for a specific management domain. In this case a particular type of credential.
- DMTF Security WG is developing a Profile specification per security credential type



Security Credential Profiles - Works in Progress

- DSP1082 Credential Management Profile (Abstract)
 - Provides capability to represent and manage credentials in a managed system.
 - Use case
 - Definition for the generic CIM model for managing different credentials
- DSP1 096 Certificate Management Profile (Specialized)
 - Provides capability to represent and manage X509 certificates
 - Use cases:
 - Import/management of asymmetric keys
 - Management of key stores
 - Request for PKCS#10 certificate signing requests (CSR) generation
 - Export/import/management of X509 certificates and certificate revocation lists (CRL)

Credential Management Profile (Work in Progress)



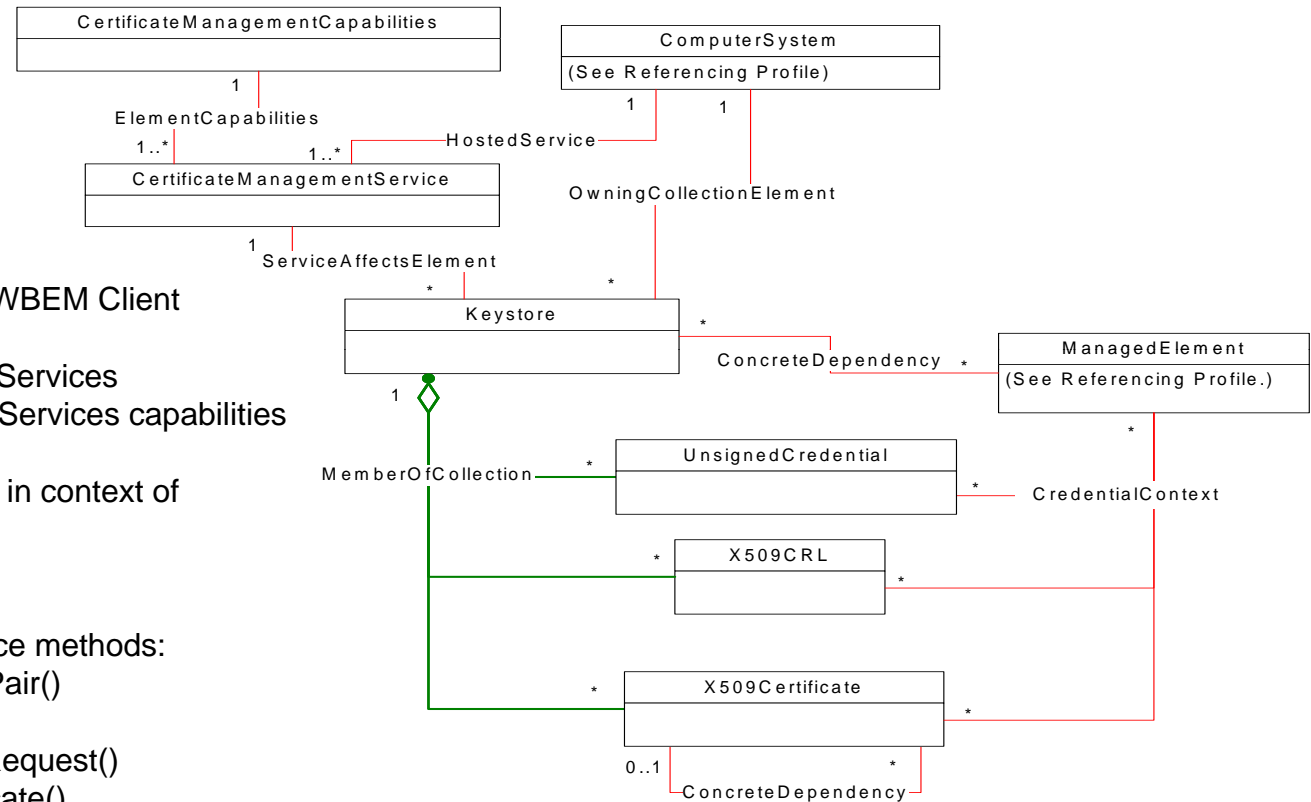
Management Interfaces presented to WBEM Client

- List Credential Management Services (of System)
- List managed Credentials
- List managed Credential Stores (of System, of Service)
- List Credentials (of CredentialStore)
- List Credential Stores (of CredentialStore)

- Extrinsic methods of particular types of credential management services and stores



Certificate Management Profile (Work in Progress)



Management Interfaces presented to WBEM Client

Intrinsic:

- List Certificate Management Services
- Get Certificate Management Services capabilities
- List managed Keystores
- List Certificates (of Keystore, in context of ManagedElement)

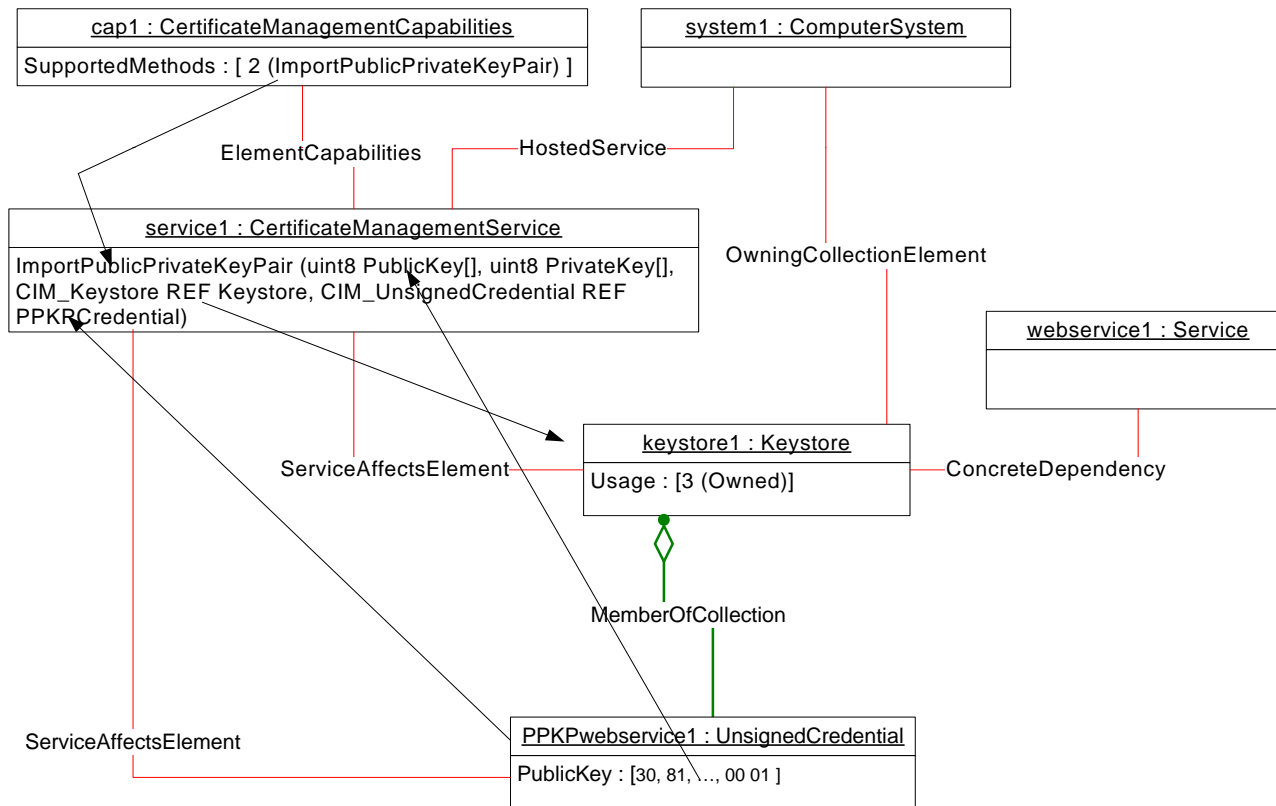
Extrinsic:

- CertificateManagementService methods:
 - ImportPublicPrivateKeyPair()
 - CreateKeystore()
 - CreatCertificateSigningRequest()
 - CreateSelfSignedCertificate()
 - ImportEncodedCertificates()
 - ImportCertificates()
 - ExportEncodedCertificate()
 - ApplyCRL()



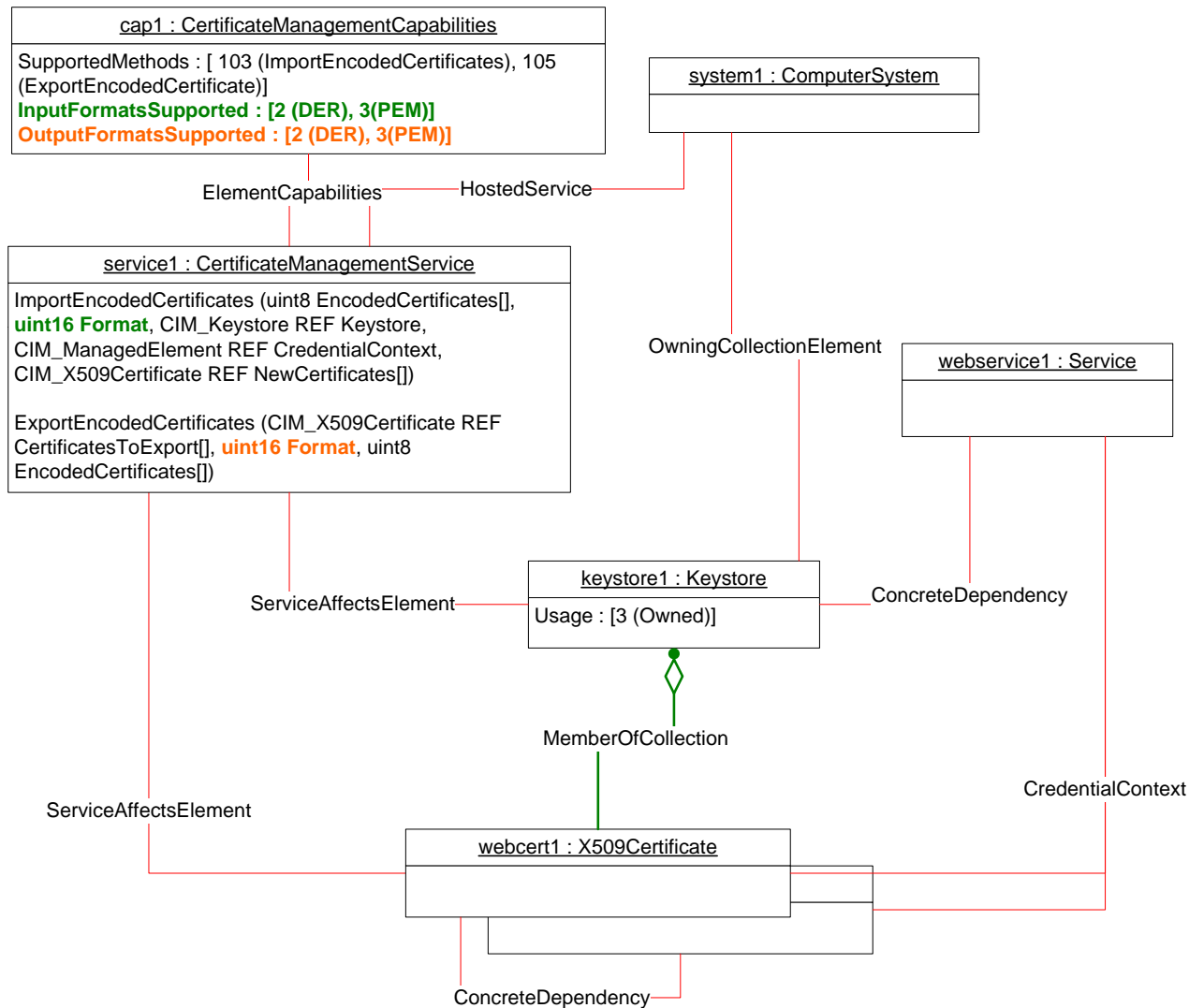
Example: Import Asymmetric Key to Keystore

In this example a CIM_UnsignedCredential instance represents the asymmetric key pair Imported using the ImportPublicPrivateKeyPair() method of the Certificate Management Service.





Example: Import & Export X509 Certificates



In this Example:

- CIM_X509Certificate class represents X509 certificates for an application represented by webservice1 instance of a service class
- CIM_Keystore instance keystore1 represents the application certificate cache
- CIM_CertificateManagementCapabilities advertises the supported configurations
- Methods support importing and exporting of certificates based on different formats including importing in CIM embedded instance(s) format.
- Certificate chains are modeled using the CIM_ConcreteDependency association



Future DMTF Security WG Activities

- CIM Schema Classes for
 - Symmetric keys
 - Biometric credentials
 - Other security credentials
- Profiles for management of
 - Symmetric keys, biometric and other security credentials
 - Credential store authorization
 - Ties into DMTF DSP1039 Role Based Authorization Profile

Additional Material

CIM Schema – <http://www.dmtf.org/standards/cim>

- DSP0004 – CIM Infrastructure Specification
- CIM v. 2.19 – CIM Schema

WS-Man – <http://www.dmtf.org/standards/wsman/>

- DSP0226, 1.0.0 – WS Management
- DSP0227, 1.0.0b – WS-Management CIM Binding
- DSP0230, 1.0.0 – WS-CIM Mapping

Profiles (available to DMTF members only)

- DSP1082 – Credential Management
- DSP1096 – Certificate Management

Contact Information

Jon Hass, Dell – Jon_Hass@Dell.com

Khachatur Papanyan, Dell – Security WG Co-Chair –
khachatur_papanyan@dell.com

George Ericson, EMC – Security WG Co-Chair - ericson_george@emc.com

Q/A Session



Thank You !

