



December 3-6, 2007, Santa Clara Marriott, Santa Clara, CA

Credential Management Profile

Khachatur Papanyan
Dell Inc.

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>.

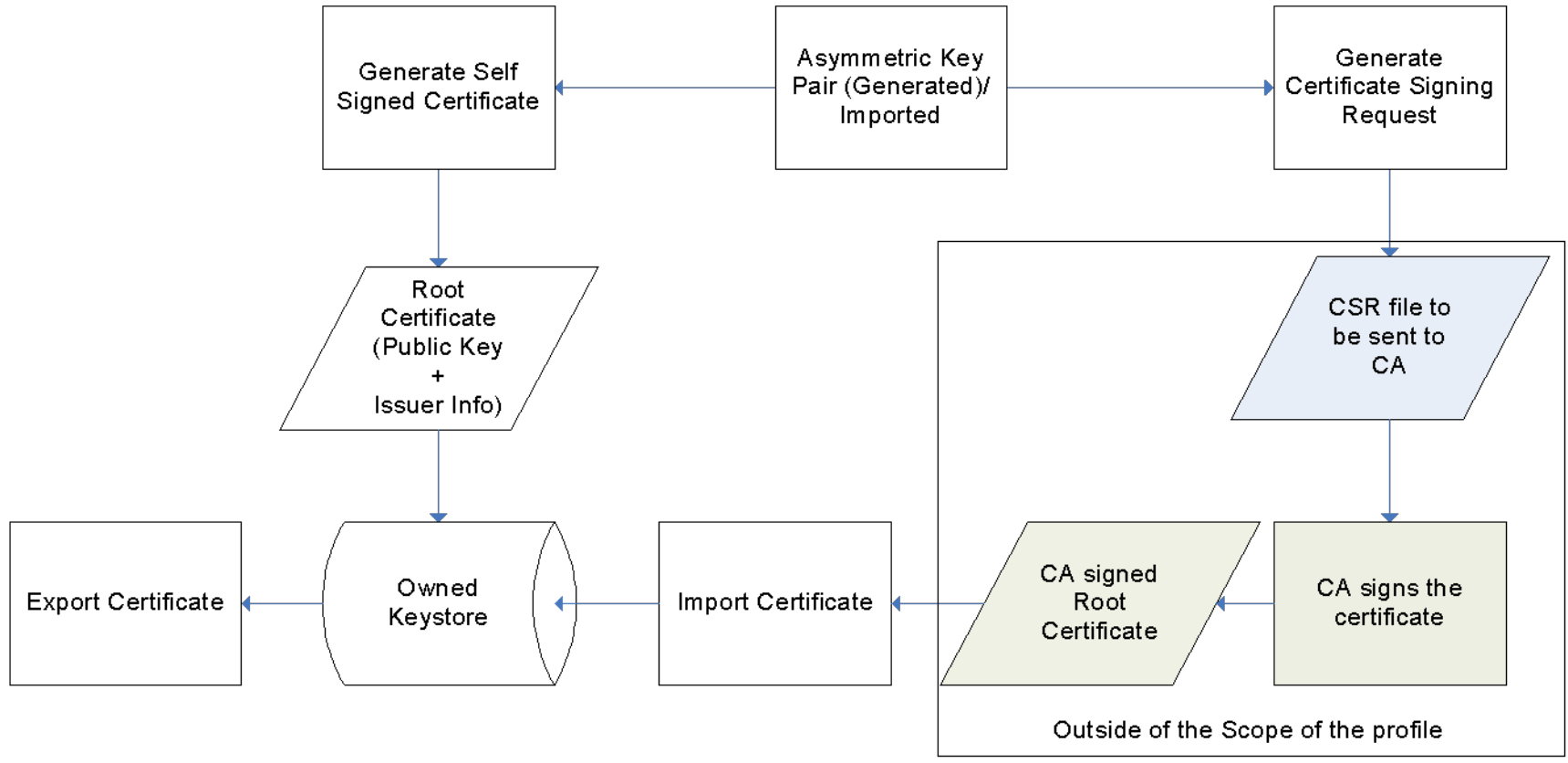
Scope of the Profiles

- Credential Management Profile
 - capability to model and manage key based credentials used in the identification process such as X509 certificates that utilize public key infrastructure (PKI).
- Profiles do NOT describe a mechanism for the credential verification.
- Features:
 - Management of asymmetric keys
 - Management X509 certificates and certificate revocation lists (CRL)
 - Management of key stores
 - Generating PKCS#10 certificate signing requests

Credential Management Use Cases

- Server Side (Role) – Managed system serves up a certificate for the client to authenticate the identity of the server.
 - Ex: Web servers supporting HTTPs (includes managed systems that use TLS based authentication for WS-Man)
- Client Side (Role) – Managed system verifies the certificates served up against its chain of certificates in the trusted list and CRL
 - Ex: Managed system connecting to an LDAP/Active Directory server for authentication
 - Ex: Mutual TLS authentication

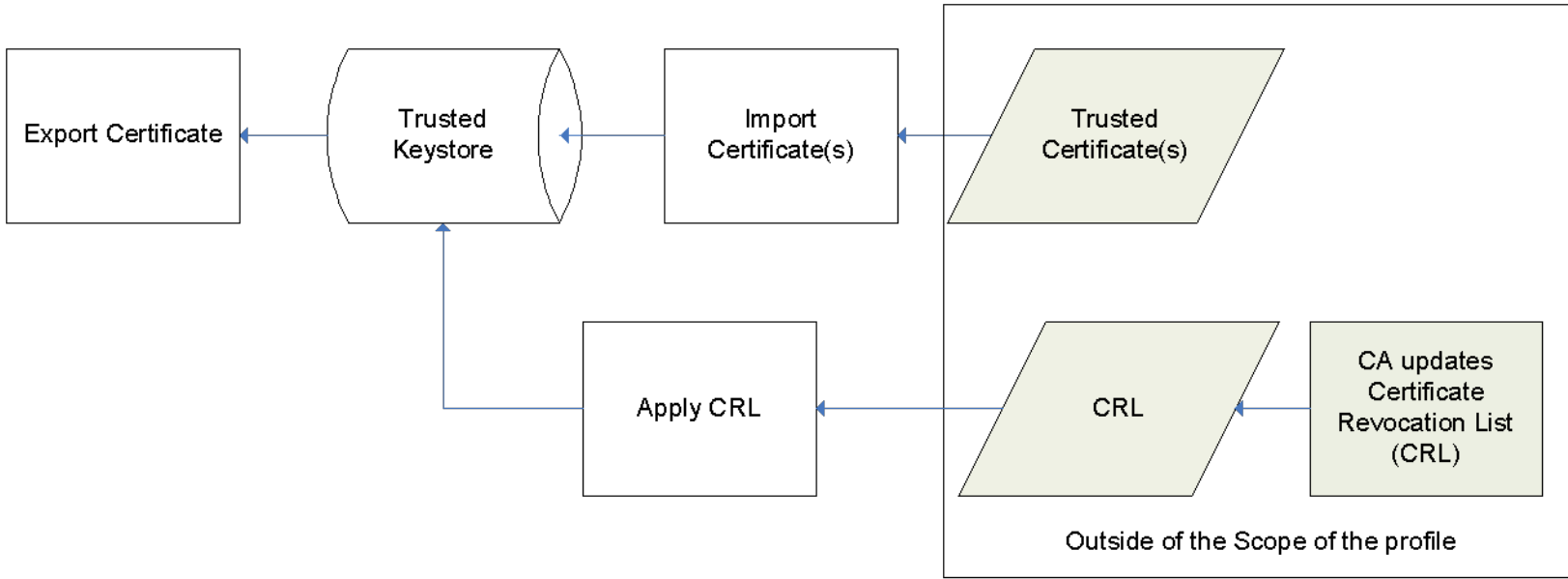
Server Side Flow Chart



Server Side Use Cases

- Management of the server side key store
- Import asymmetric keys (public/private key pair)
 - Due to the constraints of the implementation the key pair may not be generated locally but uploaded to the system
- Generating self signed certificate
- Create CSR
- Import a root certificate
- Import a certificate chain
- Export certificates
- Represent current root certificate
- Represent current root certificate chain

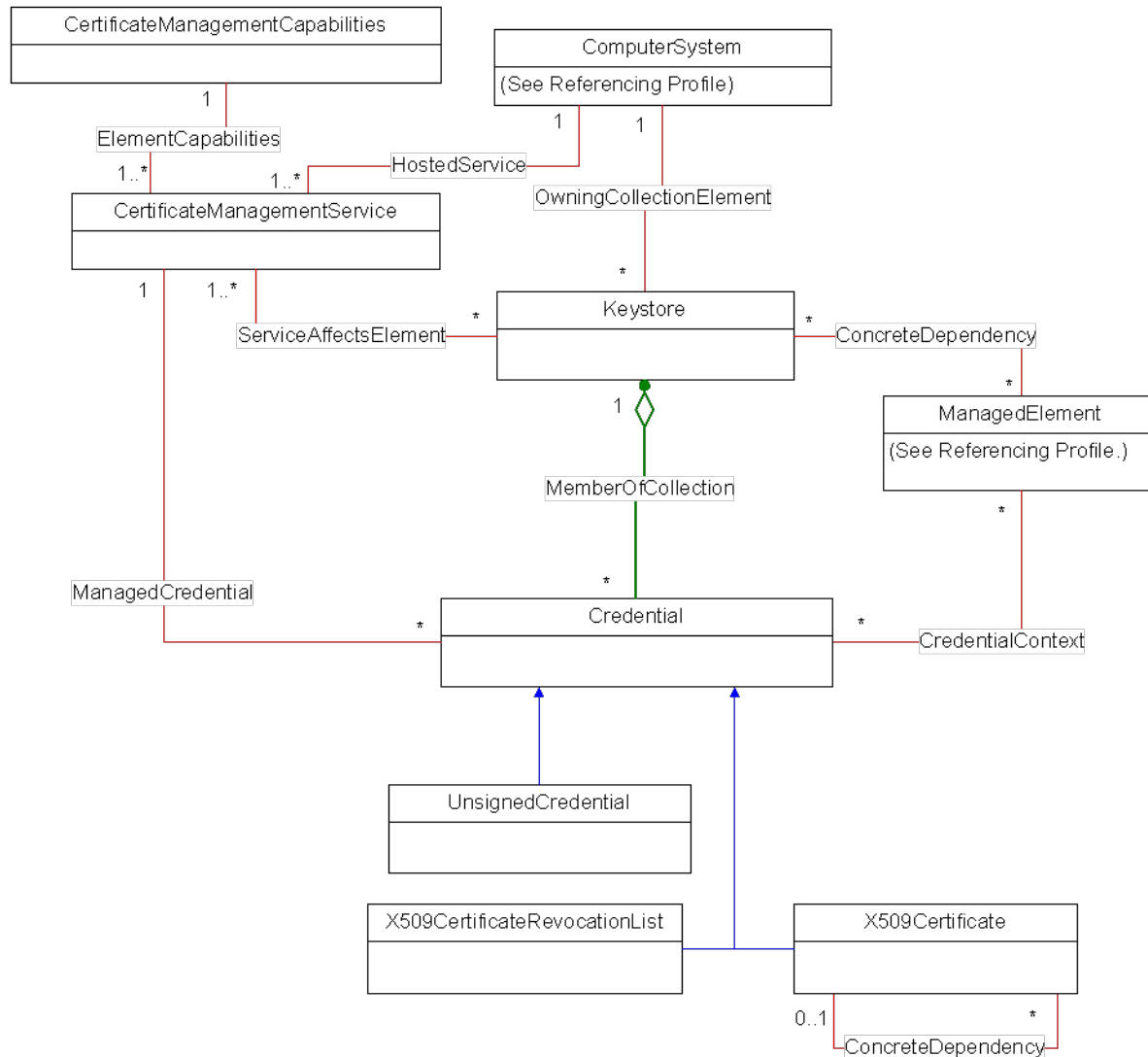
Client Side Flow Chart



Client Side Use Cases

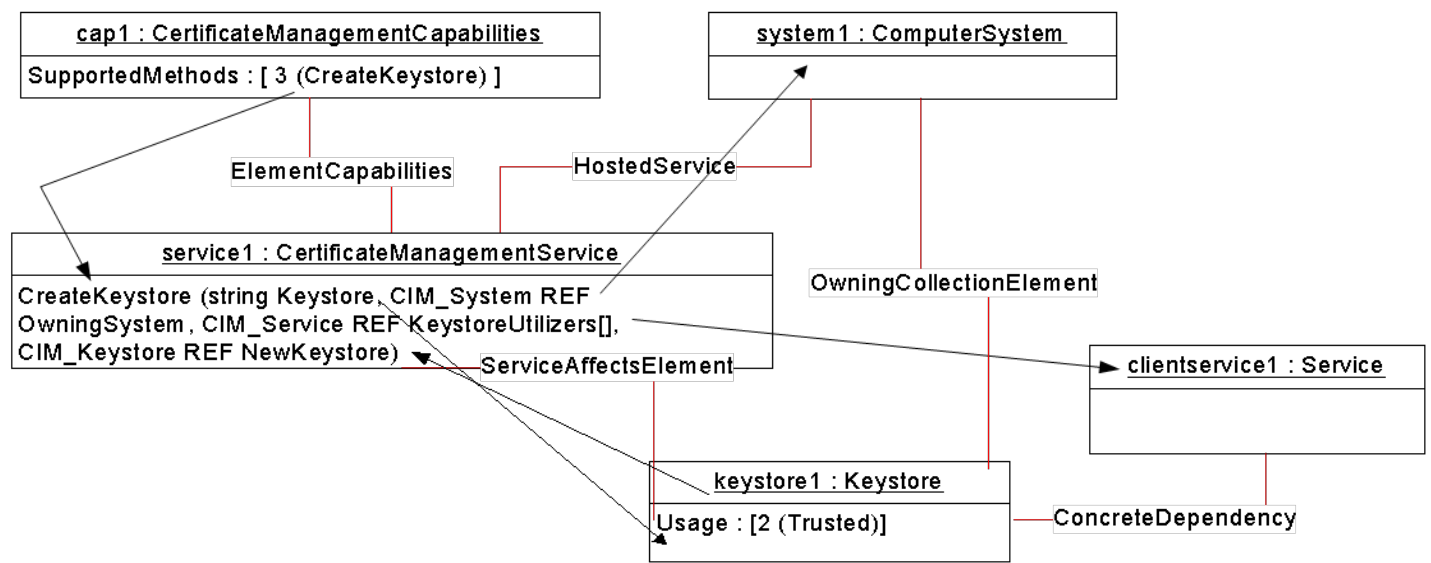
- Management of the client side key store
- Representation of a certificate chain
- Import certificate/certificate chain
- Export certificate/certificate chain
- Management of CRL

Proposed Class Diagram



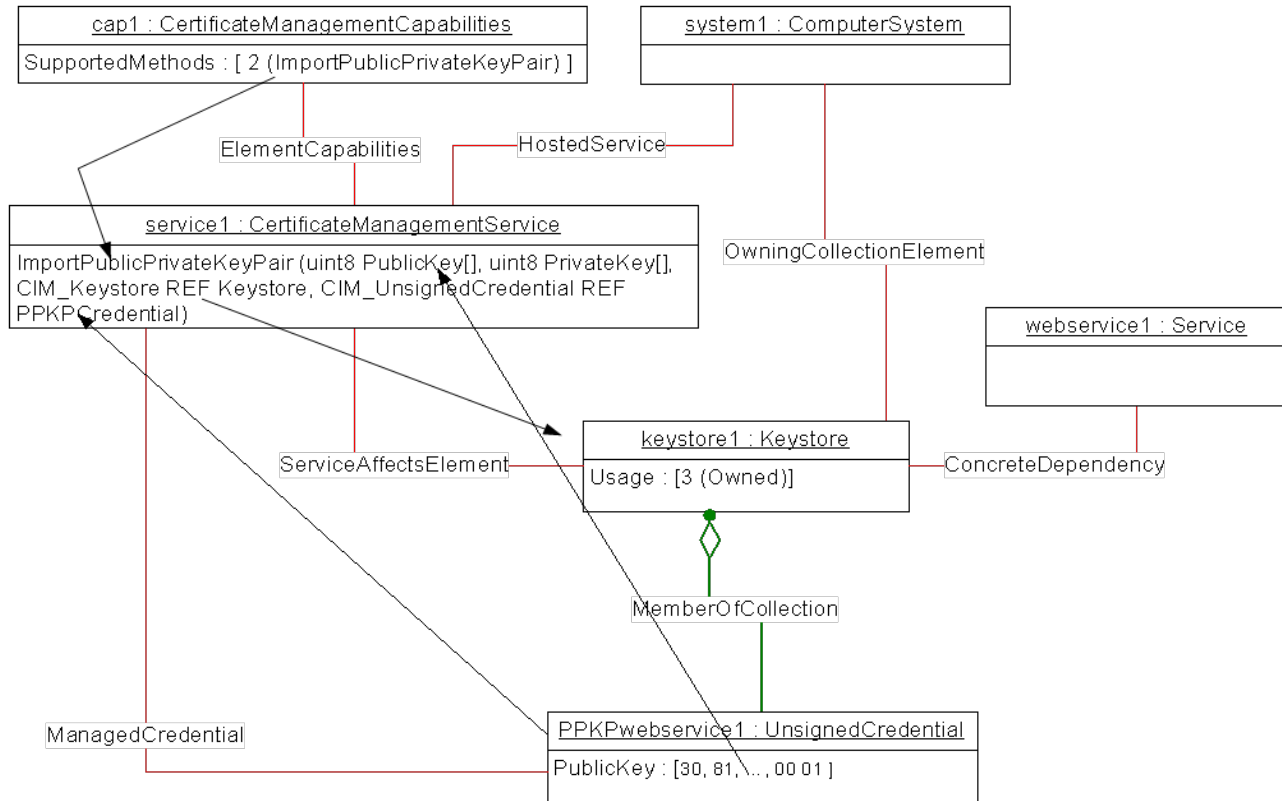
CIM_Keystore

- CIM_Keystore represents the aggregation of key-based credentials
 - Properties
 - Usage: denotes keystore usage, trusted (client side role) vs owned (server side role)
 - ElementName: user-friendly name of the key store
 - Created either by the CreatKeystore method or instantiated by the instrumentation
 - Any key based credential needs to belong to a particular key store



Import Asymmetric Key

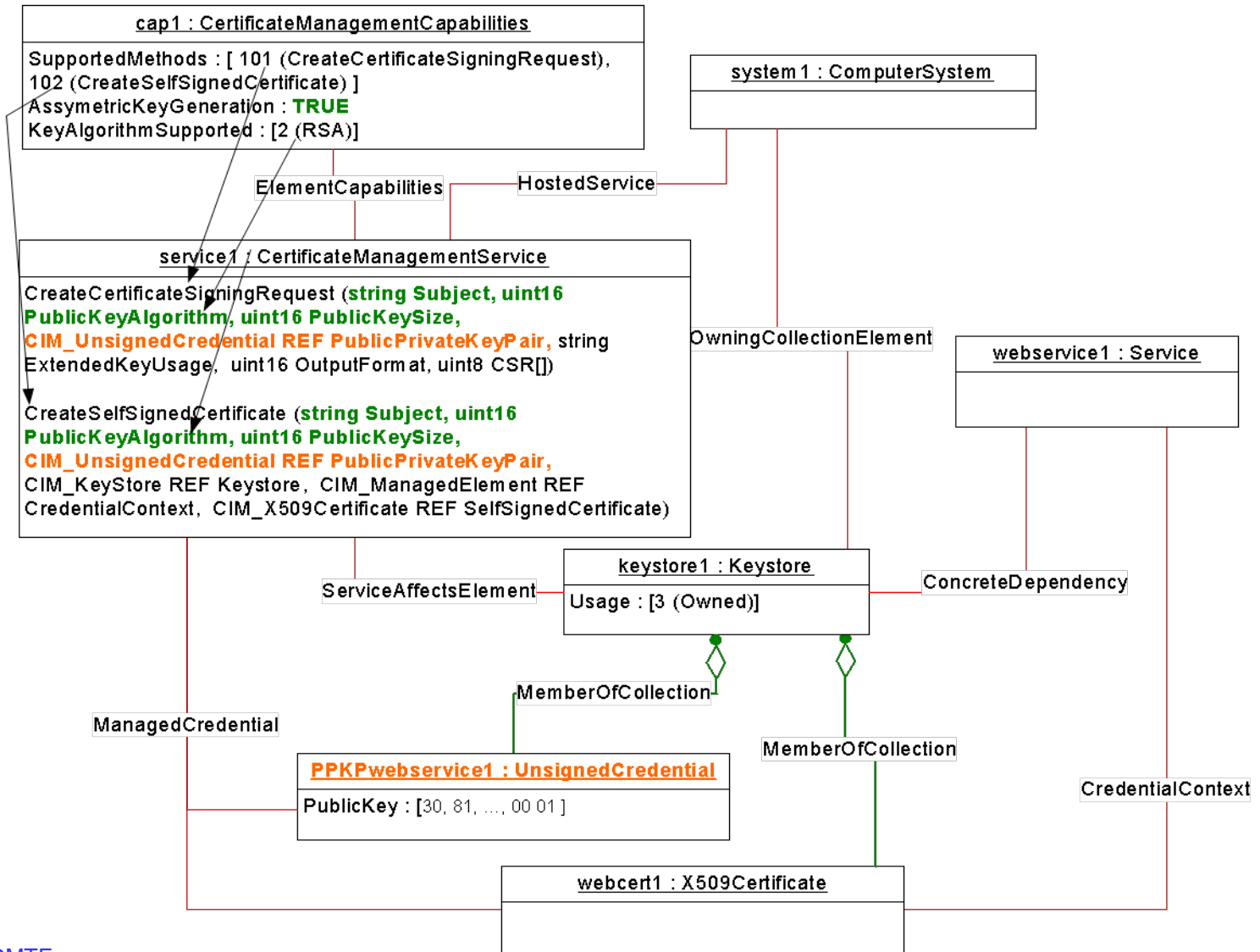
- CIM_UnsignedCredential represents the asymmetric key pair
 - Imported using the ImportPublicPrivateKeyPair() method



PKCS#10 CSR & Self-signed X509 Certificate

- CIM_X509Certificate represents an X509 certificate such as the self-signed certificate
- Methods to generate CSR and self-signed certificate are based on:
 - previously imported asymmetric key pair represented by CIM_UnsignedCredential instance and referenced by PublicPrivateKeyPair parameters
- OR
- subject (RFC 1485), PublicKeyAlgorithm, PublicKeySize parameters
- CIM_CertificateManagementCapabilities advertises the supported configurations

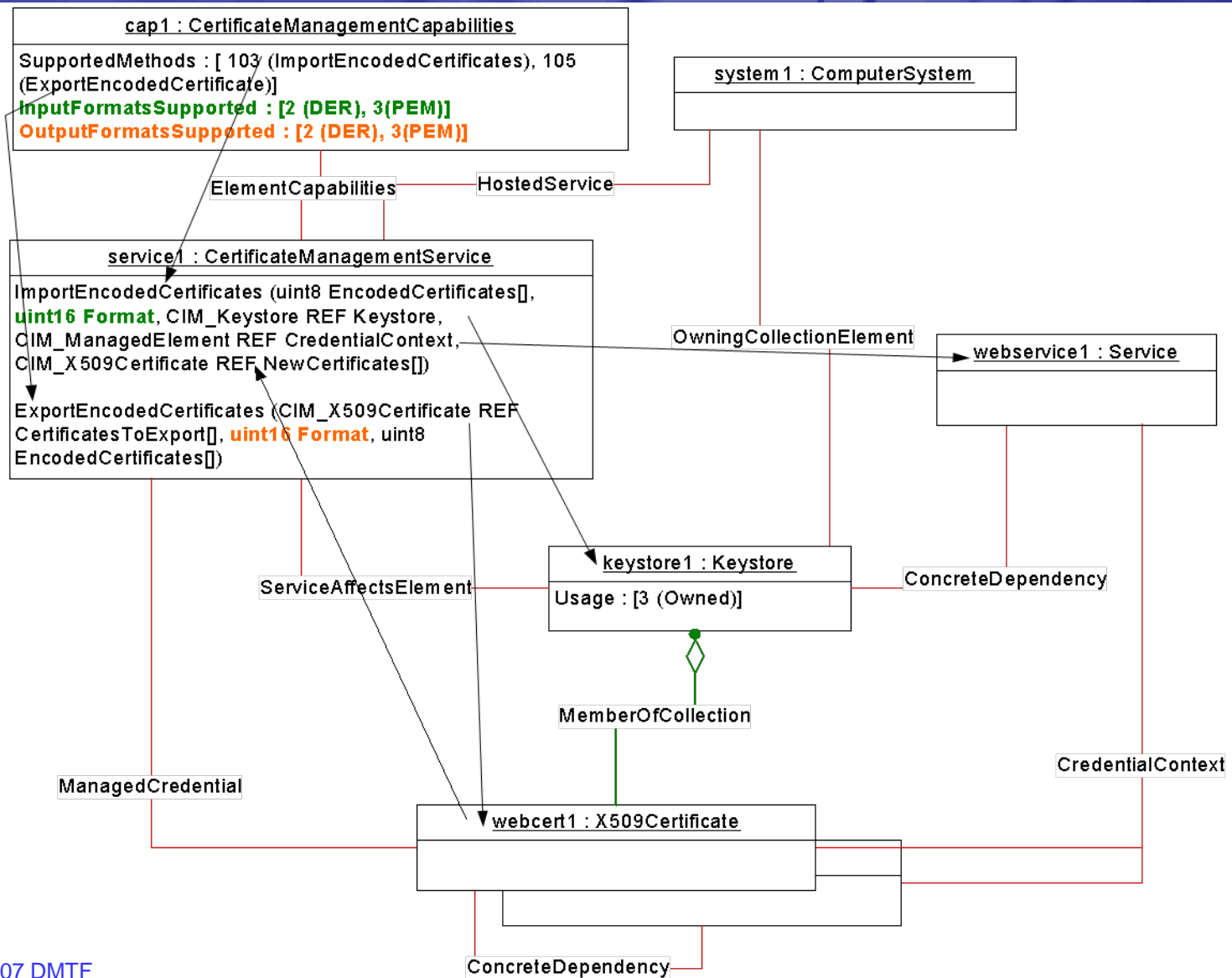
PKCS#10 CSR & Self-signed X509 Certificate Methods



Import & Export of X509 Certificates

- CIM_X509Certificate class represents X509 certificates
- 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

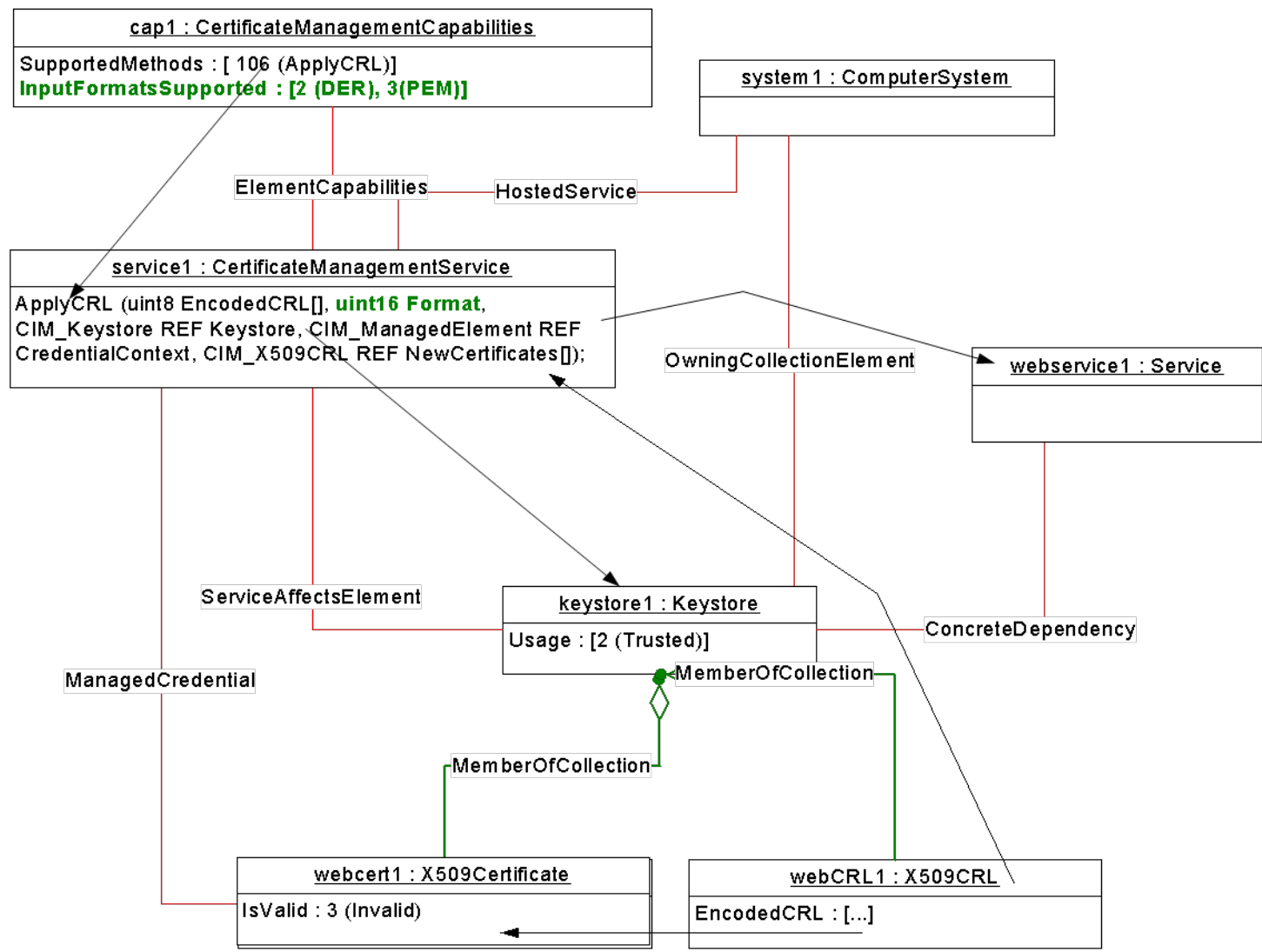
Import & Export X509 Certificates Methods



X509 CRL

- CIM_X509CRL class represents the CRL applied to the key store. Following are important properties:
 - Issued – thisUpdate of X509 CRL based on RFC 3280
 - NextUpdate – nextUpdate of X509 CRL based on RFC 3280
- Execution of the ApplyCRL() methods triggers application of the CRL to the key store resulting in the invalidation of the certificates contained in the CRL or

Application of X509 CRL





December 3-6, 2007, Santa Clara Marriott, Santa Clara, CA

Q/A Session



December 3-6, 2007, Santa Clara Marriott, Santa Clara, CA

Thank You !