

November 15-18, 2010



Santa Clara Marriott
Santa Clara, CA

Security Working Group DMTF Profile Update

Hemal Shah, Broadcom Corporation
Khachatur Papanyan, Dell Inc.

Disclaimer

- 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.





Security Working Group Overview

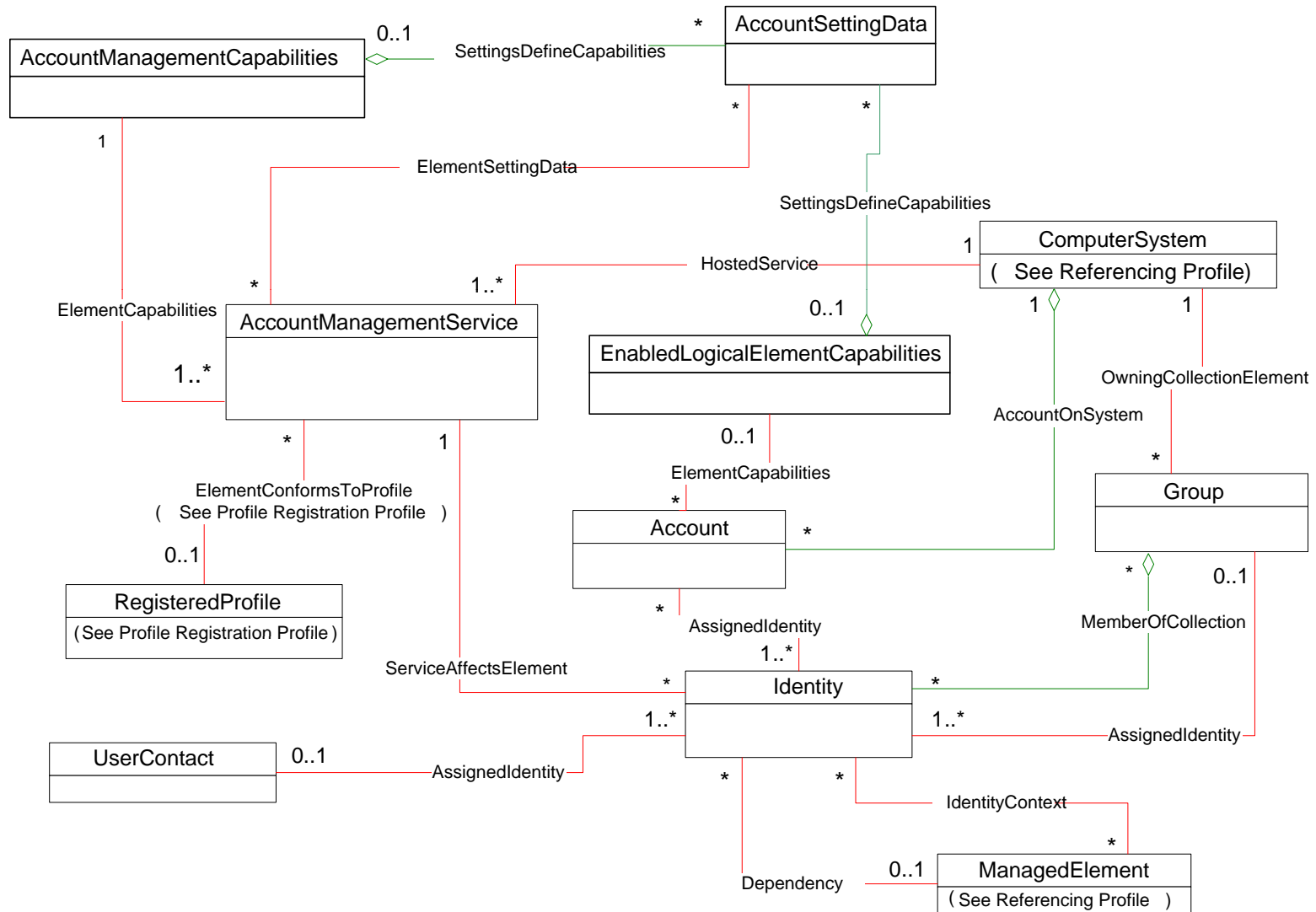
- Development of Interoperable Security Management Interfaces
- Development of CIM models primarily for
 - Authentication,
 - Authorization.
- Development of Profile Specifications
 - Simple Identity Management Profile, 1.0.1 (Standard)
 - Role Based Authorization Profile, 1.0.0 (Standard)
 - Credential Management Profile (Draft)
 - Certificate Management Profile (Draft)
- Out of Scope
 - Development of Security Protocols
 - Operational Security Requirements for Protocols and Management Initiatives
 - Management of the Underlying Security Capabilities Utilized by Protocols and Initiatives



Simple Identity Management Profile (SIMP)

- Manage Security Principal
 - Manage Local Accounts
 - Creation/Deletion/Modification
 - Account State Management
 - Represent Third Party Authenticated Users
 - Represent Ingress Point Based Security
-
- Profile does NOT describe a mechanism for performing the authentication

Class Diagram

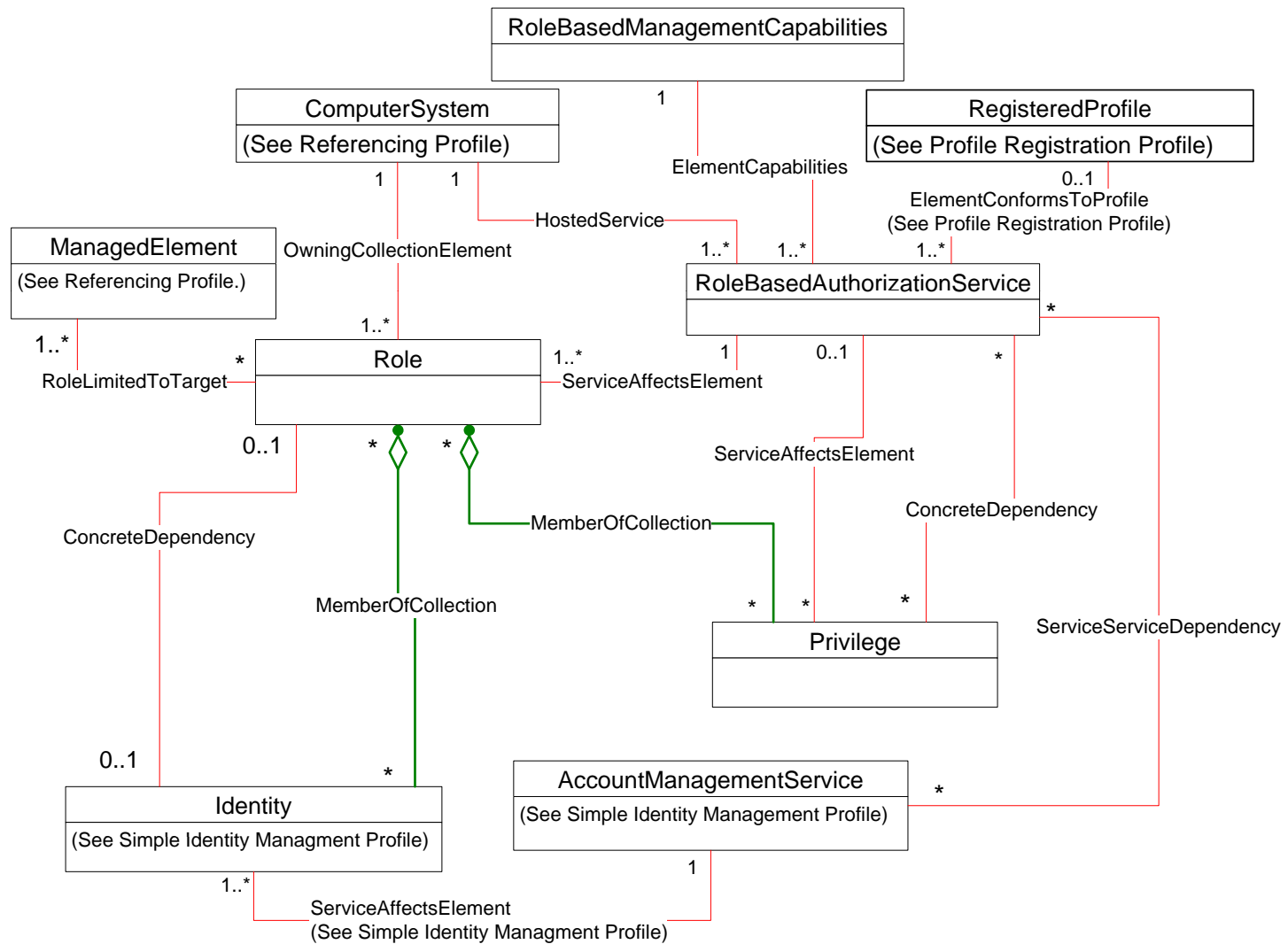




Role Based Authorization Profile (RBAP)

- Representation of Account's Roles and
 - Account Dependent Privileges
 - Access assignment for Accounts
 - Management of Roles and Privileges
-
- Profiles do NOT describe a mechanism for performing the authentication and the authorization.

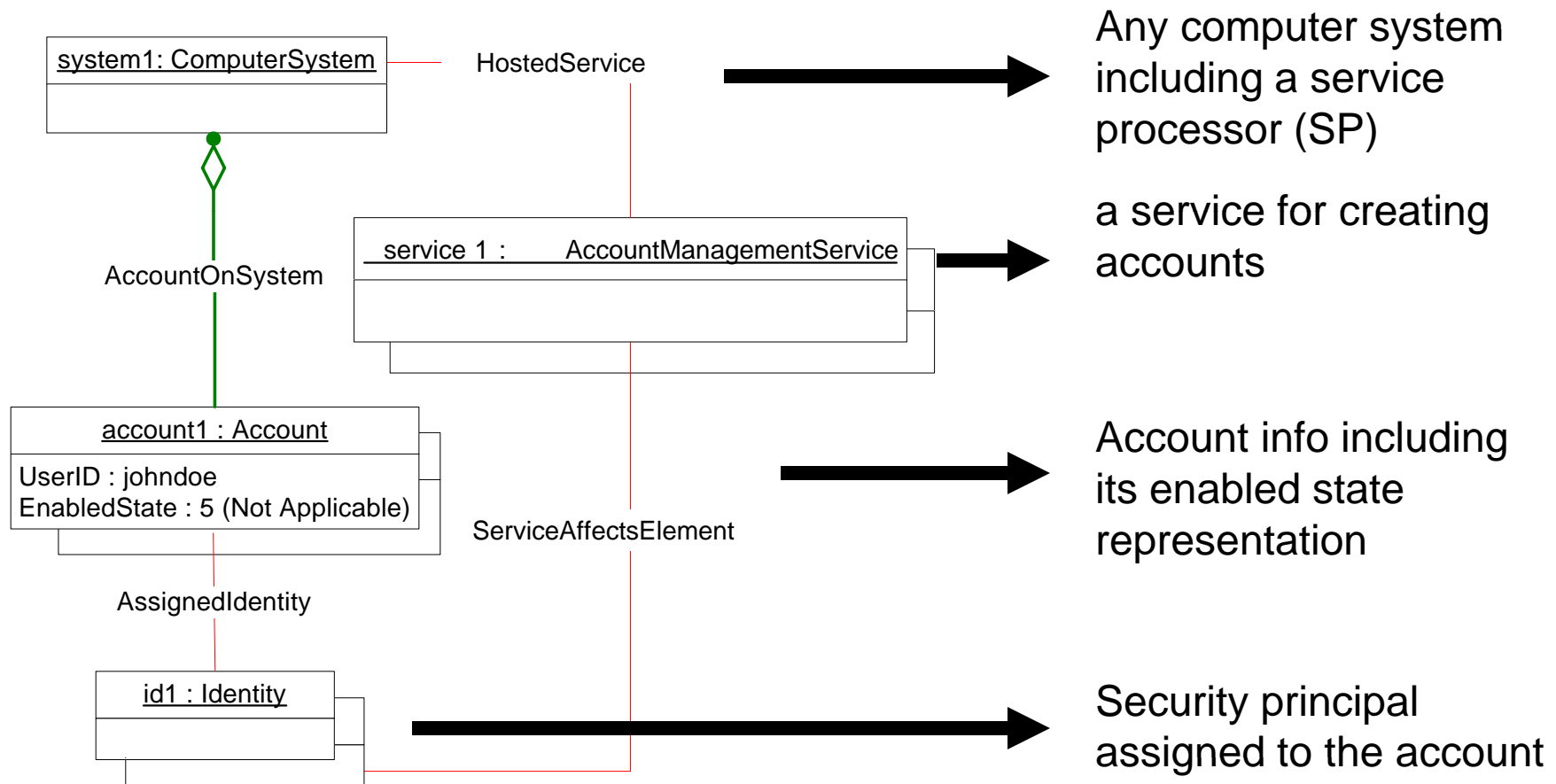
Class Diagram



SIMP and RBAP Use Cases

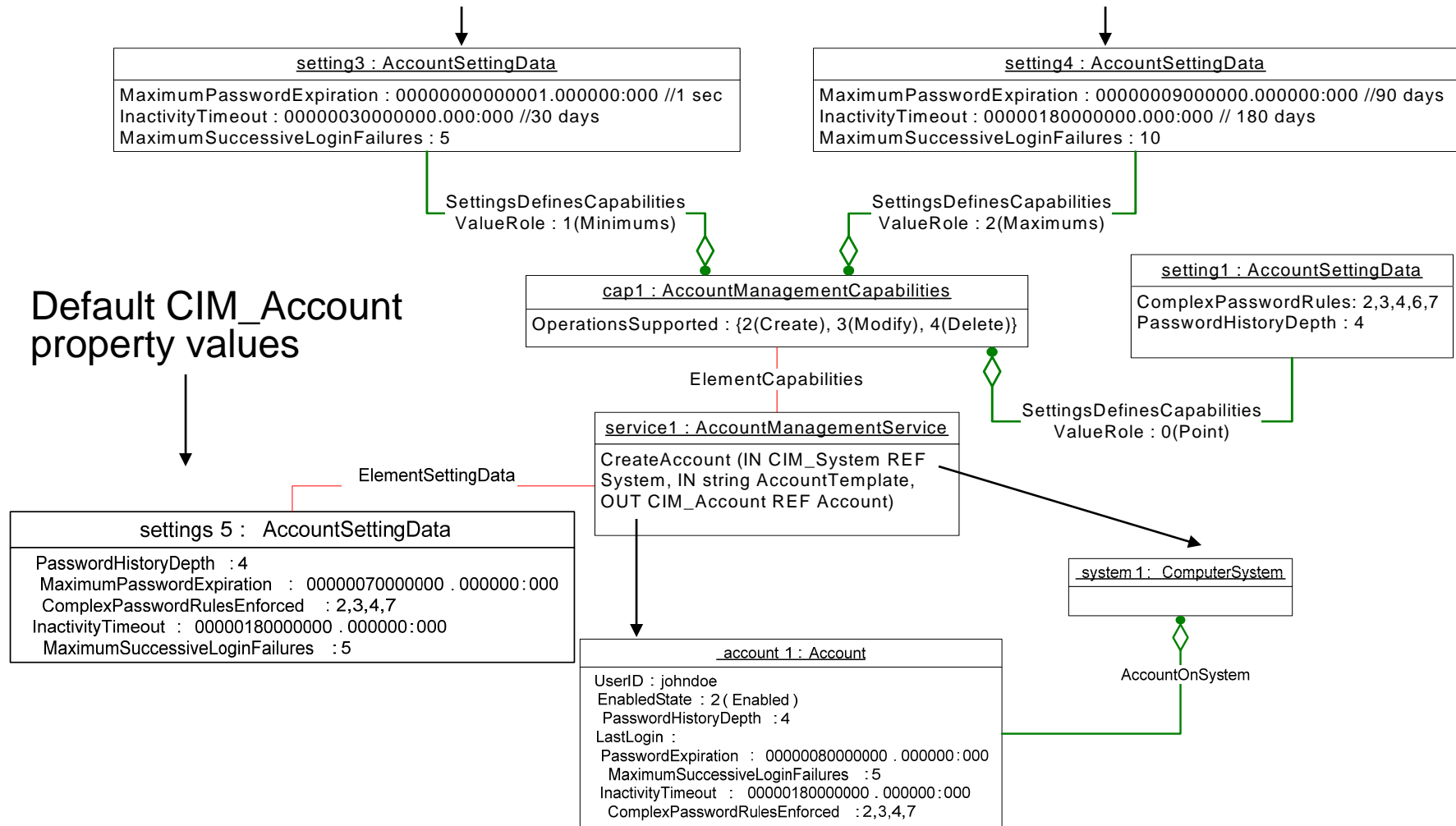
- Show Local Accounts
- Show Third Party Authenticated Users
- Create an Account
- Enable/Offline/Disable an Account
- Show Ingress Point Based Security
- Show Roles
 - Show Opaque Roles
 - Show Roles with Privileges
- Assign Privileges to an Account
- Show Account's Privileges for a Managed Element
- Show Account Dependent Privileges
- Create a Role

Simple SIMP Instantiation



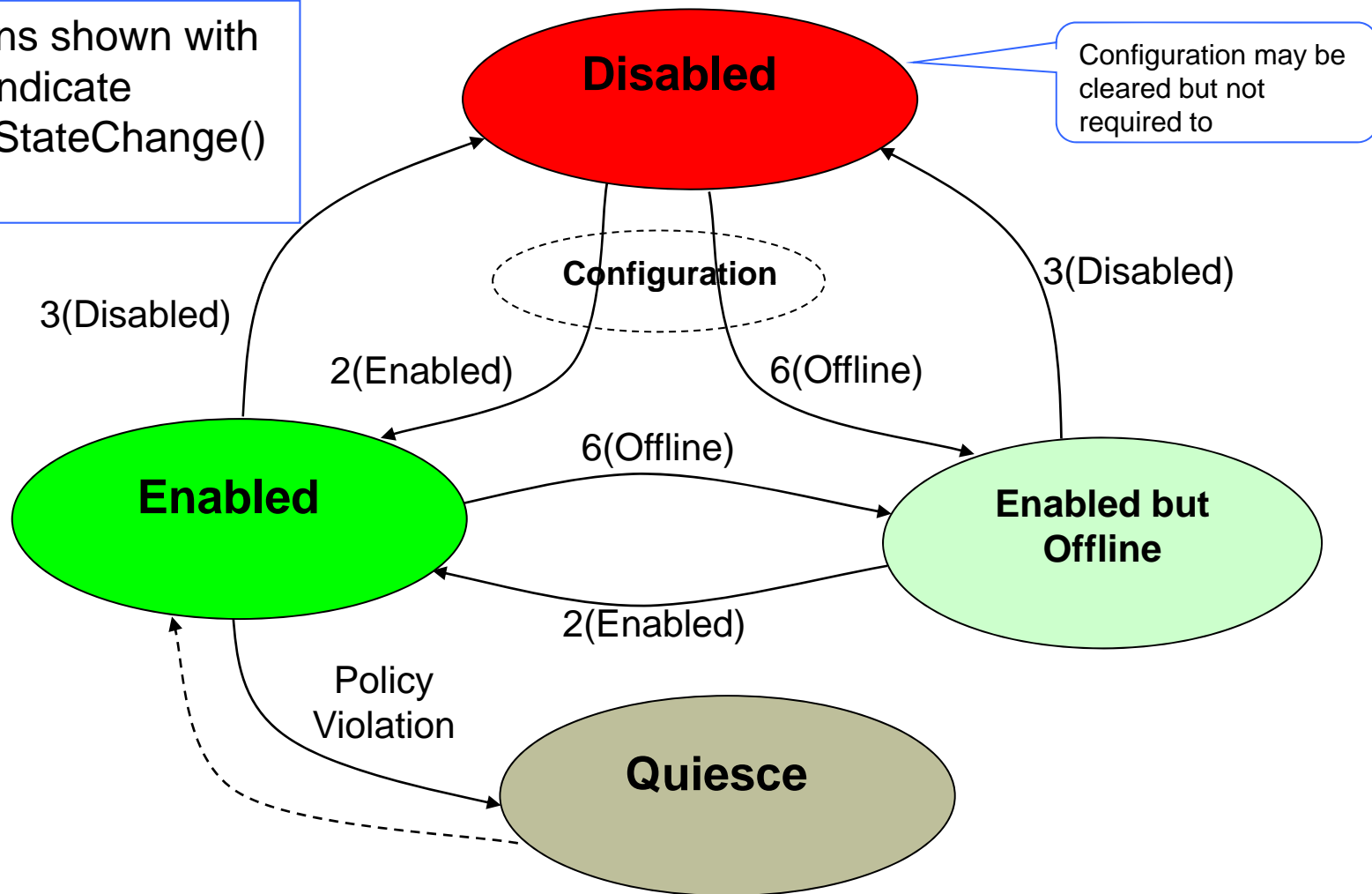
Create an Account

Range of acceptable CIM_Account property values



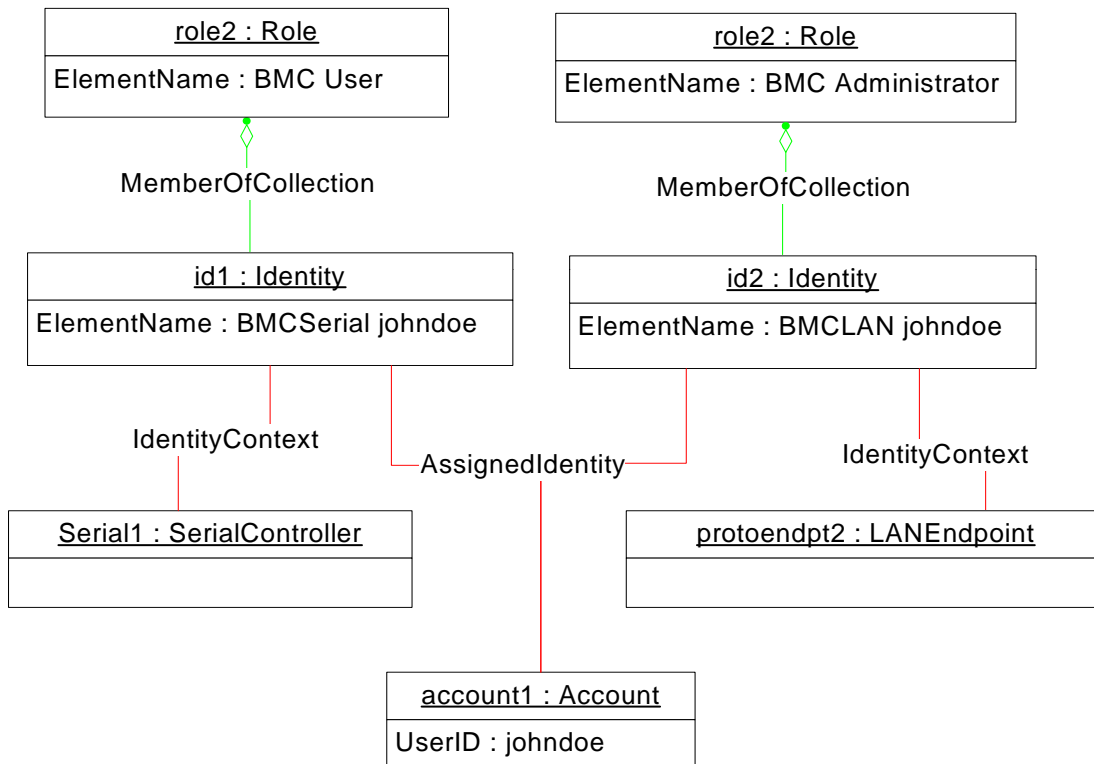
Enable/Offline/Disable an Account (2/2)

All transitions shown with ValueMap indicate RequestedStateChange() behavior



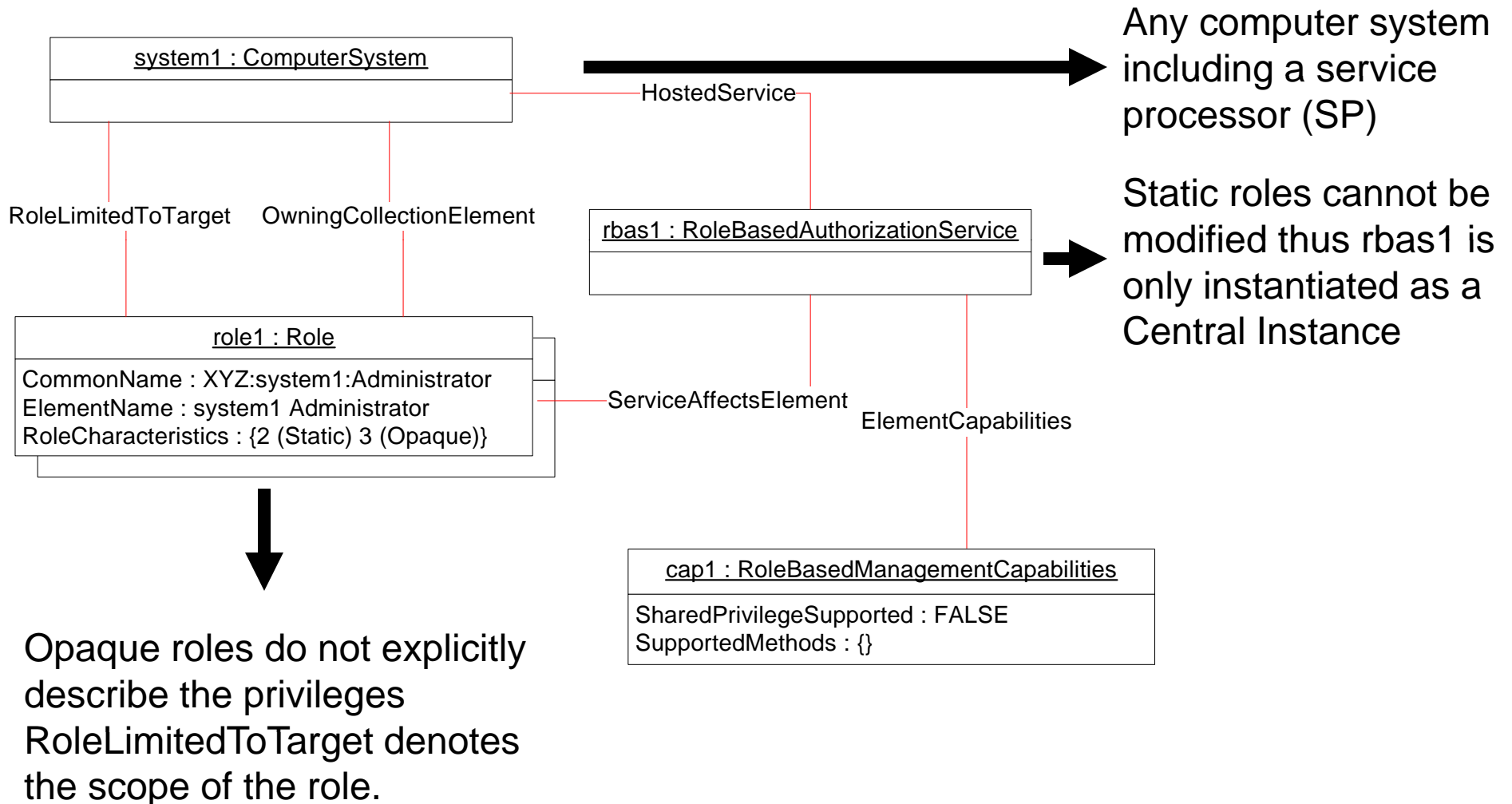
EnabledState values shown within ovals

Show Ingress Point Based Security

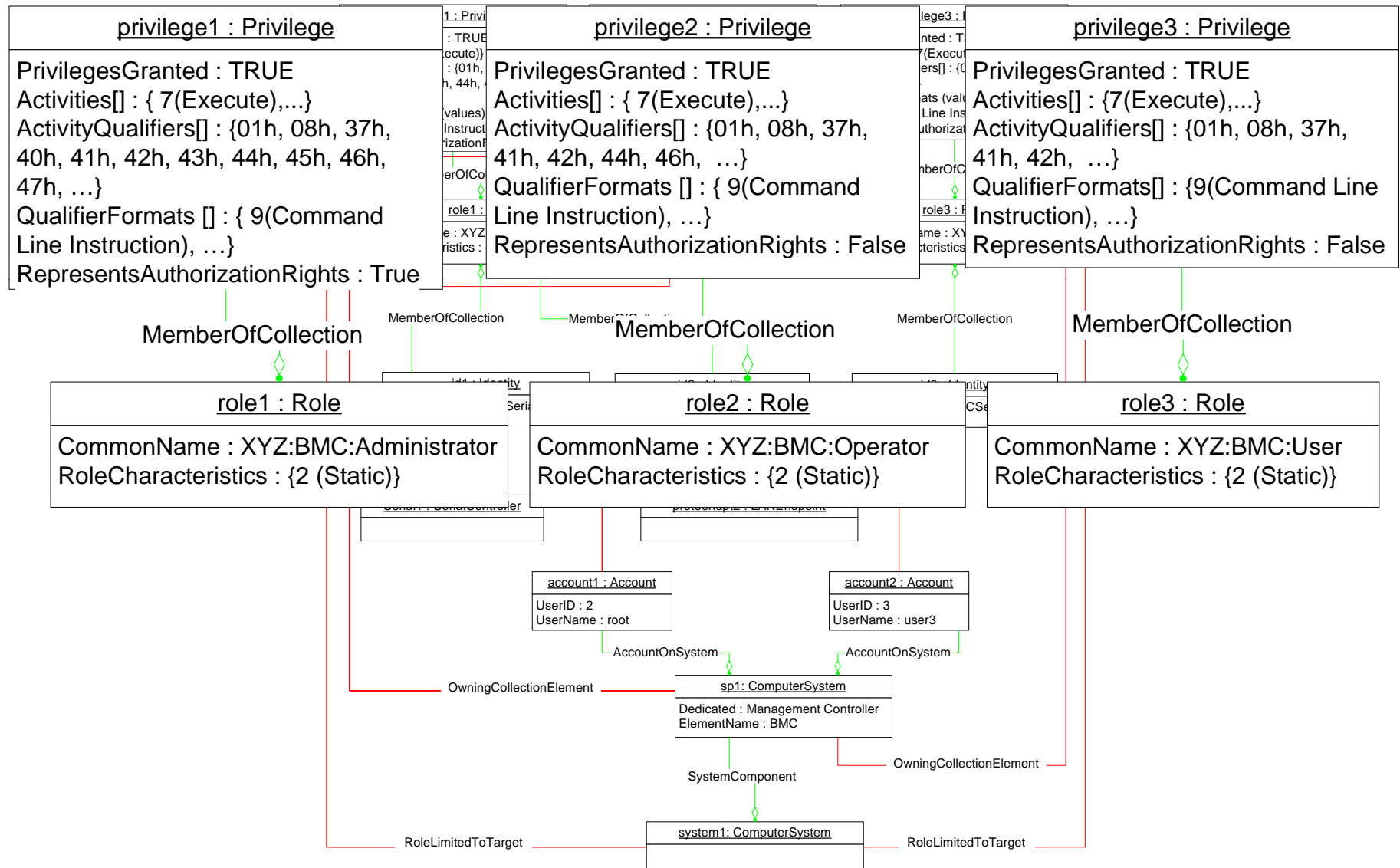


- account1 can have a security principal per the ingress point (LAN vs Serial) of authentication
- Allows account1 to have different authorization based on the ingress point of authentication (Administrator for LAN and User for Serial)

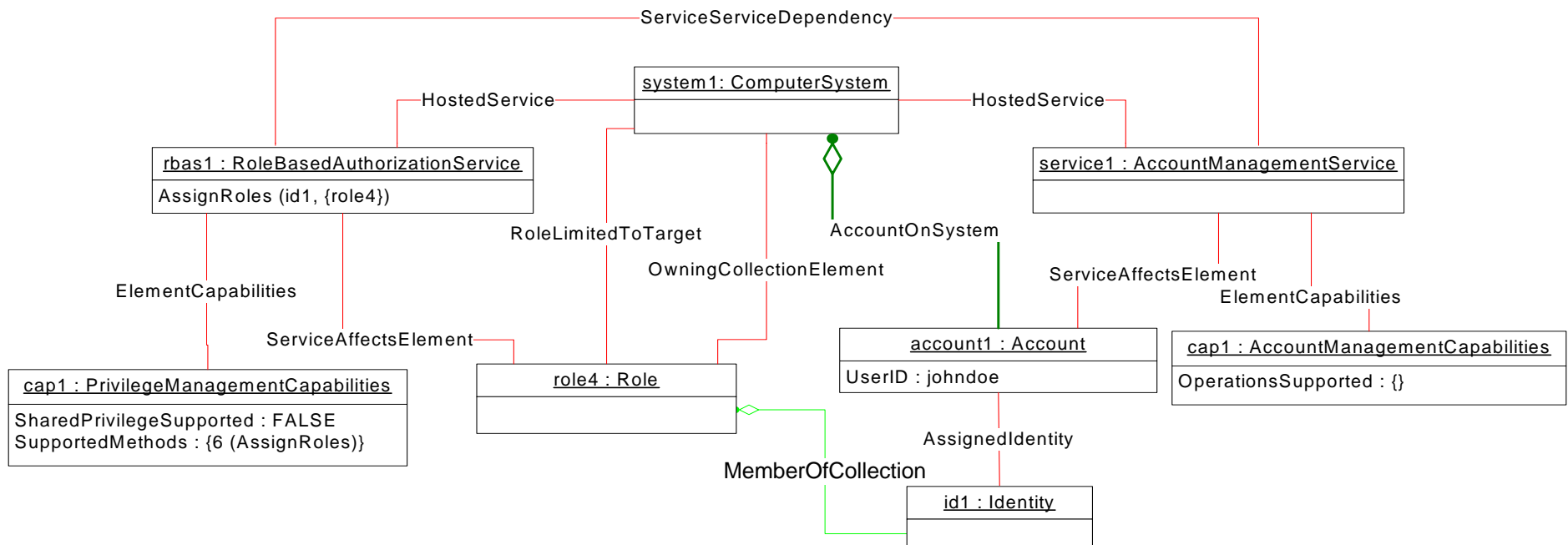
Show Roles



Show Roles with Privileges



Assign a Privileges to an Account





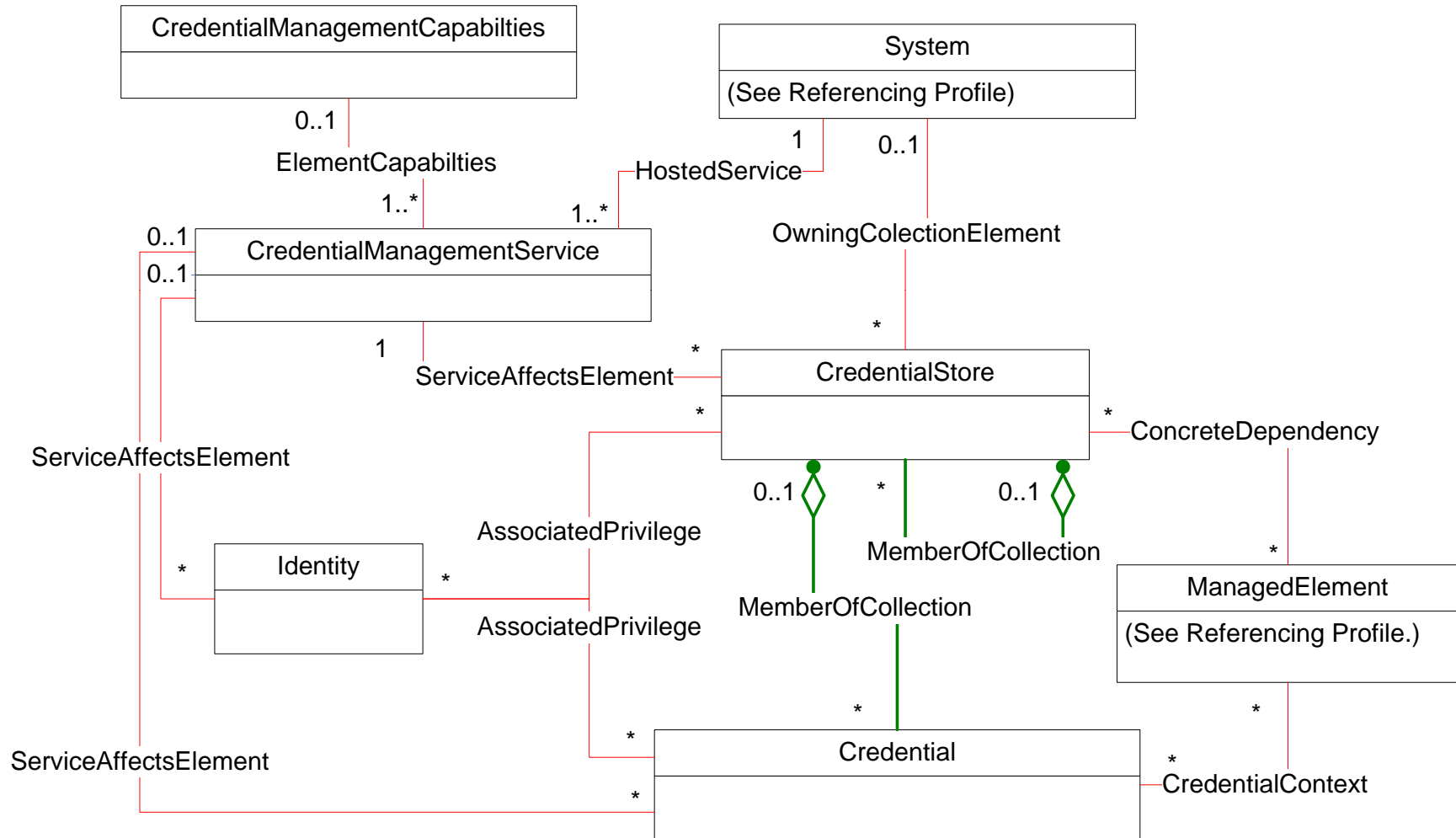
Credential Management Profile

- Credential Management Profile
 - An abstract profile with capability to model credentials including key based credentials like PKI public key infrastructure (PKI), X509 and biometric credentials.
- Features:
 - Provides the base model for the different credential types

Use Cases

- Show credentials in a credential store
- Show authorization model for credential access
- Import a credential as a blob into a credential store.
 - (work in progress)

Class Diagram





Certificate Management Profile

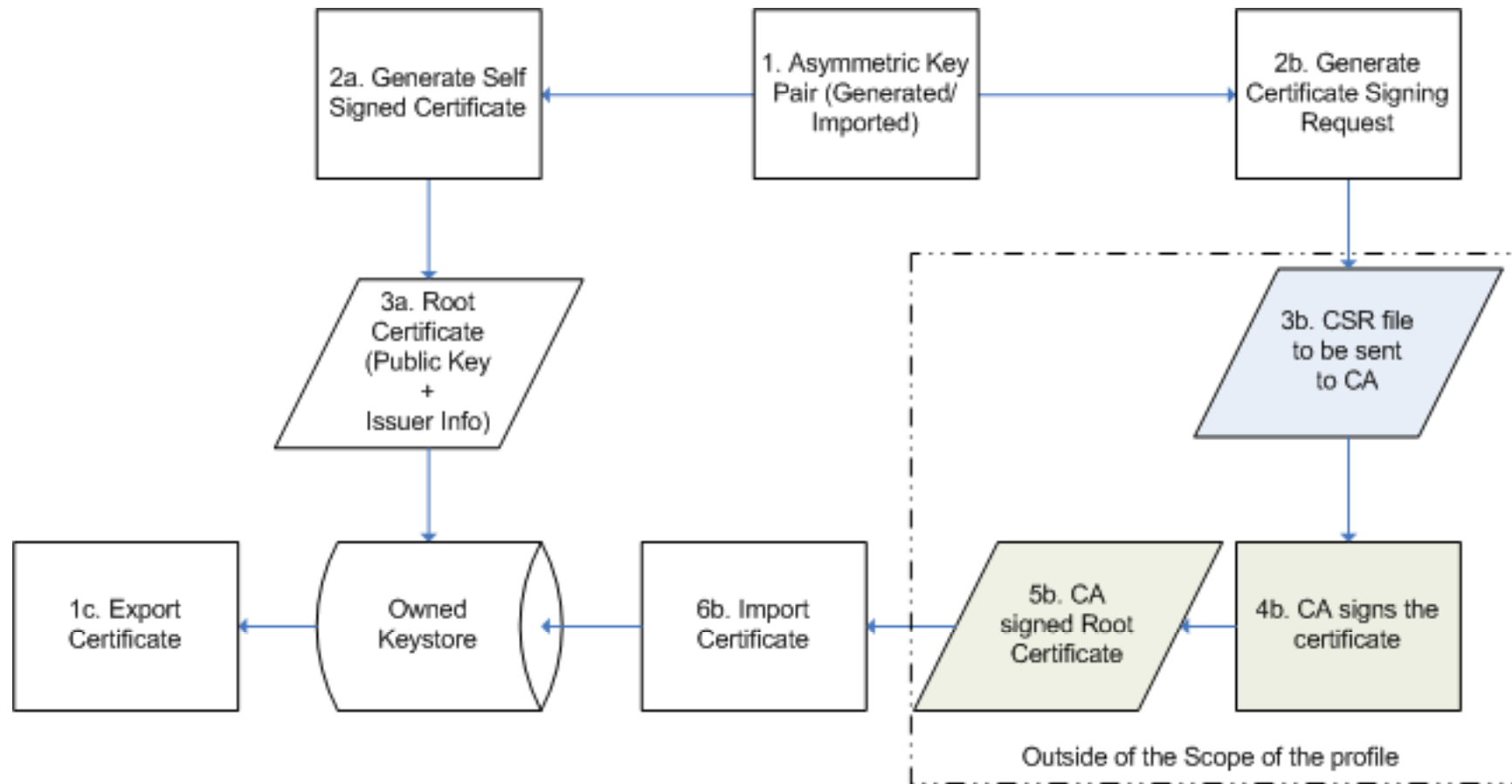
- Certificate Management Profile
 - capability to model and manage key based Certificates used in the identification process such as X509 certificates that utilize public key infrastructure (PKI).
- Profiles do NOT describe a mechanism for the Certificate verification.
- Features:
 - Management of asymmetric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



Certificate Management Use Cases

- Owned Certificate – 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)
- Trusted Certificate – 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
- Managed system can have both trusted and owned certificates.

Owned Certificate Flow Chart





Owned Certificate Use Cases

- Manage owned key store
 - Create a key store
 - Show current certificates
 - Show certificate chain
- 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
- Generate self signed certificate
- Create Certificate Signing Requests
- Import a certificate or a certificate chain
- Export a certificate or a certificate chain



Trusted Certificate Use Cases

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



PKCS#10 CSR & Self-signed X509 Certificate

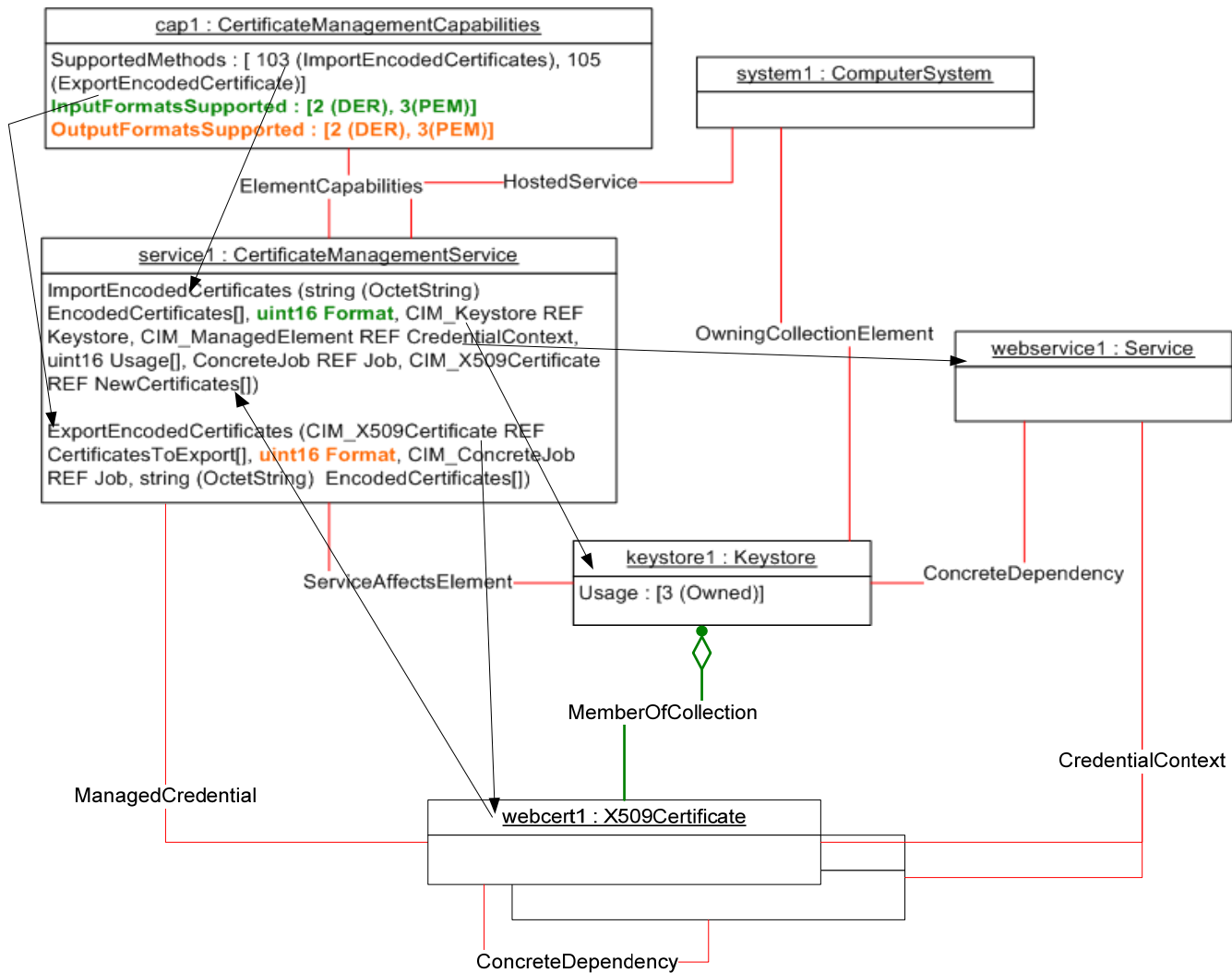
- CIM_X509Certificate represents an X509 certificate such as the self-signed certificate
- Methods to generate CSR and self-signed certificate are based on:
 - previously imported asymmetric key pair represented by CIM_UnsignedCertificate instance and referenced by PublicPrivateKeyPair parameters
- OR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



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.



Questions?

Thank you!