



Specification

DSP0121

STATUS: Preliminary

Copyright © “2001” 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. DMTF specifications and documents may be reproduced for uses consistent with this purpose by members and non-members, if correct attribution is given. As DMTF specifications may be revised from time to time, the particular version and release cited should always be noted.”

DMTF LDAP Schema for the CIM v2.5 User Information Model Jan 11, 2002

Abstract

This document presents an LDAP schema for the CIM version 2.5 User Information Model [1].

Table of Contents

1	INTRODUCTION.....	3
2	LDAP MAPPING CONSIDERATIONS	3
2.1	EXISTING LDAP CLASSES AND ATTRIBUTES	3
2.1.1	<i>d1m1PersonInfoAuxClass</i>	5
2.1.2	<i>d1m1OrganizationInfoAuxClass</i>	5
2.1.3	<i>d1m1RoleInfoAuxClass</i>	6
2.1.4	<i>d1m1CimLDAPInfoAuxClass</i>	6
2.2	MAPPING ASSOCIATIONS	6
2.2.1	<i>No Additional Properties</i>	7
2.2.2	<i>Additional Properties, 1-to-1 or 1-to-many</i>	8
2.2.3	<i>Additional Properties, many-to-many</i>	9
3	CLASS DEFINITIONS	10
3.1	SECURITYSERVICE	10
3.2	ACCOUNTMANAGEMENTSERVICE CLASSES	10
3.3	AUTHENTICATIONSERVICE CLASSES	12
3.4	VERIFICATIONSERVICE CLASSES	13
3.5	CREDENTIALMANAGEMENTSERVICE CLASSES	15

3.6	CERTIFICATEAUTHORITY CLASSES.....	16
3.7	KERBEROSKEYDISTRIBUTIONCENTER CLASSES.....	19
3.8	NOTARYINSTANCE CLASSES.....	20
3.9	LOCALCREDENTIALMANAGEMENTSERVICE CLASSES.....	22
3.10	SHAREDSECRETSERVICE CLASSES.....	24
3.11	PUBLICKEYMANAGEMENTSERVICE CLASSES.....	25
3.12	AUTHORIZATIONSERVICE CLASSES.....	27
3.13	CREDENTIALMANAGEMENTSAP.....	28
3.14	AUTHENTICATIONREQUIREMENT CLASSES.....	29
3.15	ACCESSCONTROLINFORMATION CLASSES.....	31
3.16	ORGANIZATIONALENTITY.....	33
3.17	USERENTITY.....	33
3.18	USERSACCESS CLASSES.....	33
3.19	CREDENTIAL.....	35
3.20	PUBLICKEYCERTIFICATE CLASSES.....	36
3.21	UNSIGNEDPUBLICKEY CLASSES.....	38
3.22	KERBEROSTICKET CLASSES.....	39
3.23	SHAREDSECRET CLASSES.....	41
3.24	NAMEDSHAREDIKESECRET CLASSES.....	43
3.25	SERVICEUSESSECURITYSERVICE CLASSES.....	44
3.26	SECURITYSERVICEFORSYSTEM CLASSES.....	46
3.27	MANAGESACCOUNTONSYSTEM CLASSES.....	46
3.28	ELEMENTASUSER CLASSES.....	47
3.29	SYSTEMADMINISTRATOR CLASSES.....	48
3.30	SYSTEMADMINISTRATORGROUP CLASSES.....	49
3.31	SYSTEMADMINISTRATORROLE CLASSES.....	49
3.32	USERACCOUNT CLASSES.....	50
3.33	SECURITYSERVICEUSESACCOUNT CLASSES.....	51
3.34	MANAGESACCOUNT CLASSES.....	51
3.35	TRUSTHIERARCHY CLASSES.....	52
3.36	USERSCREDENTIAL CLASSES.....	53
3.37	PUBLICPRIVATEKEYPAIR CLASSES.....	53
3.38	CAHASPUBLICCERTIFICATE CLASSES.....	55
3.39	MANAGEDCREDENTIAL CLASSES.....	56
3.40	CASIGNSPUBLICKEYCERTIFICATE CLASSES.....	56
3.41	LOCALLYMANAGEDPUBLICKEY CLASSES.....	57
3.42	SHAREDSECRETISSHARED CLASSES.....	58
3.43	IKESCRETISNAMED CLASSES.....	58
3.44	KDCISSUESKERBEROSTICKET CLASSES.....	59
3.45	NOTARYVERIFIESBIOMETRIC CLASSES.....	60
3.46	HOSTEDAUTHENTICATIONREQUIREMENT CLASSES.....	60
3.47	AUTHENTICATEFORUSE CLASSES.....	61
3.48	REQUIRECREDENTIALSFROM CLASSES.....	62
3.49	AUTHENTICATIONTARGET CLASSES.....	63
3.50	HOSTEDACI CLASSES.....	63
3.51	AUTHENTICATIONUSE CLASSES.....	64
3.52	AUTHORIZATIONSUBJECT CLASSES.....	65
3.53	AUTHORIZATIONTARGET CLASSES.....	66
3.54	MEMBERPRINCIPAL CLASSES.....	66
3.55	ACCOUNTONSYSTEM CLASSES.....	68
3.56	ORGSTRUCTURE CLASSES.....	69
3.57	COLLECTIONINORGANIZATION CLASSES.....	70
3.58	COLLECTIONINSYSTEM CLASSES.....	70
4	REFERENCES.....	71

A.	STRUCTURE RULE DEFINITIONS.....	72
B.	OID ASSIGNMENTS.....	73
B.1	OBJECT CLASSES	73
B.2	ATTRIBUTES.....	77
B.3	NAMEFORMS.....	80

1 Introduction

This document presents an LDAPv3 [2, 3, 6] schema for the DMTF CIM User 2.5 Model [1]. This mapping follows the methodology used for the Core Mapping document [4] except as noted below in that abstract CIM classes are mapped to abstract LDAP classes. Concrete CIM classes are mapped to structural and auxiliary LDAP classes. CIM associations are mapped using a combination of auxiliary classes and structural LDAP classes.

The content, naming and structure rules provided here are suggestions and may be modified as needed to support a particular directory structure. In addition, the attribute and object class descriptive fields are provided for human clarity. Directory administrators do not need to subclass/instantiate everything in this schema verbatim. They are free to choose the subset that meets their particular needs. In particular, this means:

- If your directory implementation does not support content, naming or structure rules, comment them out.
- If your directory implementation does not support description fields of greater than some length, those may be commented out.
- If your directory implementation requires a certain ordering of classes and attributes (e.g. to avoid forward references) feel free to re-order as necessary.
- If your directory implementation and application can make use of substring matching, feel free to add substring matching clauses as appropriate.

While this document discusses X.509 certificates, it does not address any interworking between directory object classes as described in X.509 and the classes in this mapping. This is a topic for future work. This document is a product of the DMTF User & Security and LDAP Mapping WGs.

2 LDAP Mapping Considerations

2.1 Existing LDAP classes and attributes

As the CIM User Model is actually a mapping of existing LDAP classes, these CIM classes should revert back to the source LDAP classes when mapping back to LDAP. The following table states the mapping between CIM and LDAP classes along with the reference for the definition of that particular LDAP class.

CIM class	LDAP class
CIM_Person, CIM_OtherPersonInformation	inetOrgPerson [5] and d1m1PersonInfoAuxClass
CIM_Group, CIM_OtherGroupInformation	groupOfNames [6]
CIM_Organization, CIM_OtherOrganizationInformation	organization [6] and d1m1OrganizationInfoAuxClass
CIM_OrgUnit, CIM_OtherOrgUnitInformation	organizationalUnit [6]
CIM_Role, CIM_OtherRoleInformation	organizationalRole [6] and d1m1RoleInfoAuxClass
CIM_Account	account [7]

In addition the following table states the mapping between CIM properties and LDAP attributes along with the reference for the definition of those particular LDAP attributes.

URL	LabeledURI [5]
-----	----------------

If these attributes and classes are not native to a directory implementation, they can be found within the referenced documents [5, 6, 7]. This document does not redefine them. Although many of the source LDAP classes and attributes originate in X.500, they are not identical. When they differ, or are not present in an X.500 implementation, the alias, X.500 originating name, or definition that most closely resembles the definition in [6] should be used.

The hierarchy of classes from which these CIM classes derive does not directly correspond to the superior classes of the source LDAP. Therefore, the conceptual abstract classes CIM_UserEntity, CIM_OrganizationalEntity and CIM_Collection are not mapped. The mapped attributes from CIM_ManagedElement, d1m1Caption and d1m1Description, are included in an auxiliary class, d1m1CimLDAPInfoAuxClass. This allows properties from CIM originating instances to be fully mapped back into their LDAP entries.

By convention, the CIM property Name, although a key property, does not have to be mapped onto a source LDAP class when it serves as a DN hint to the LDAP object. Also, the non-mapped attribute orderedCimKeys may not be needed for CIM classes of LDAP origin, as the RDN may already be defined. Nevertheless, these attributes are available via d1m1CimLDAPInfoAuxClass that is defined with the abstract class d1m1ManagedElement as its superior. The propagated key properties SystemName and SystemCreationClassName from CIM_Account are not required when weakly associated instances are mapped as subordinate LDAP entries.

Finally, the attributes member (from groupOfNames) and roleOccupant (from organizationalRole) are captured in CIM's MemberofCollection association attached to

CIM_Group and CIM_Role. Thus, when converting to LDAP, associations of this type should be examined to appropriately populate these attributes.

2.1.1 dlm1PersonInfoAuxClass

To support mapping of those properties of CIM_Person and CIM_OtherPersonInformation that are not part of the inetOrgPerson class, and to support directory installations that do not use inetOrgPerson, the following auxiliary class is defined to allow CIM_Person and CIM_OtherPersonInformation properties to be mapped.

```
( 1.3.6.1.4.1.412.100.4.1.1.1 NAME 'dlm1PersonInfoAuxClass'
DESC 'This auxiliary class allows CIM_Person properties to be
      mapped to directory installations that may or may not use
      inetOrgPerson'
SUP top AUXILIARY
MAY ( objectClass $ audio $ businessCategory $ carLicense $
      commonName $ countryName $ departmentNumber $ description $
      destinationIndicator $ displayName $ employeeNumber $
      employeeType $ facsimileTelephoneNumber $ generationQualifier $
      givenName $ homeFax $ homePhone $ homePostalAddress $
      initials $ internationaliSDNNumber $ jpegPhoto $ labeledURI $
      localityName $ mail $ manager $ middleName $ mobile $
      organizationName $ organizationalStatus $ otherMailbox $ ou $
      pager $ personalTitle $ photo $ physicalDeliveryOfficeName $
      postalAddress $ postalCode $ postOfficeBox $
      preferredDeliveryMethod $ preferredLanguage $
      registeredAddress $ roomNumber $ secretary $ seeAlso $
      stateOrProvince $ street $ surname $ telephoneNumber $
      teletexTerminalIdentifier $ telexNumber $ thumbnailLogo $
      thumbnailPhoto $ title $ userID $ uniqueIdentifier $
      userCertificate $ userPassword $ userPKCS12 $
      userSMIMECertificate $ x121Address $ x500UniqueIdentifier )
)
```

2.1.2 dlm1OrganizationInfoAuxClass

To support mapping of those properties of CIM_Organization and CIM_OtherOrganizationInformation that are not part of the organization class, and to support directory installations that do not use organization, the following auxiliary class is defined to allow CIM_Organization and CIM_OtherOrganizationInformation properties to be mapped.

```
( 1.3.6.1.4.1.412.100.4.1.1.2 NAME 'dlm1OrganizationInfoAuxClass'
DESC 'This auxiliary class allows CIM_Organization properties to be
      mapped to directory installations that may or may not use
      organization.'
SUP top AUXILIARY
MAY ( objectClass $ businessCategory $ description $
      destinationIndicator $ facsimileTelephoneNumber $
      internationaliSDNNumber $ labeledURI $ localityName $ mail $
      manager $ organizationName $ otherMailbox $
      physicalDeliveryOfficeName $ postalAddress $ postalCode $
      postOfficeBox $ preferredDeliveryMethod $ registeredAddress $
```

```

searchGuide $ seeAlso $ stateOrProvince $ street $
telephoneNumber $ teletexTerminalIdentifier $ telexNumber $
thumbnailLogo $ uniqueIdentifier $ userPassword $ x121Address )
)

```

2.1.3 dlm1RoleInfoAuxClass

To support mapping of those properties of CIM_Role and CIM_OtherRoleInformation that are not part of the organizationalRole class, and to support directory installations that do not use organizationalRole, the following auxiliary class is defined to allow CIM_Role and CIM_OtherRoleInformation properties to be mapped.

```

( 1.3.6.1.4.1.412.100.4.1.1.3 NAME 'dlm1RoleInfoAuxClass'
DESC 'This auxiliary class allows CIM_Role properties to be
      mapped to directory installations that may or may not use
      organizationalRole.'
SUP top AUXILIARY
MAY ( objectClass $ businessCategory $ cn $ description $
      destinationIndicator $ facsimileTelephoneNumber $
      internationaliSDNNNumber $ ou $ physicalDeliveryOfficeName $
      postalAddress $ postalCode $ postOfficeBox $
      preferredDeliveryMethod $ registeredAddress $seeAlso $
      stateOrProvince $ street $ telephoneNumber $
      teletexTerminalIdentifier $ telexNumber $ x121Address )
)

```

2.1.4 dlm1CimLDAPInfoAuxClass

To support mapping of those properties that originate in CIM classes that correspond to native LDAP objects, but do not exist in their attribute sets, the following auxiliary class is defined to allow those properties to be mapped. These attributes may be useful if complete bi-directional mapping is needed.

```

( 1.3.6.1.4.1.412.100.4.1.1.139 NAME 'dlm1CimLDAPInfoAuxClass'
DESC 'This auxiliary class allows CIM properties to be
      mapped to directory entries that are the basis for their
      corresponding CIM classes.'
SUP top dlm1ManagedElement
MAY ( objectClass $ dlmCreationClassName $ dlmName )
)

```

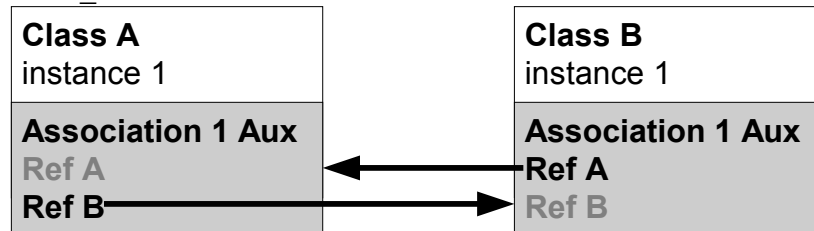
2.2 Mapping Associations

For ease of reference, the following text has been copied from 2.6.2 of the Core Mapping document:

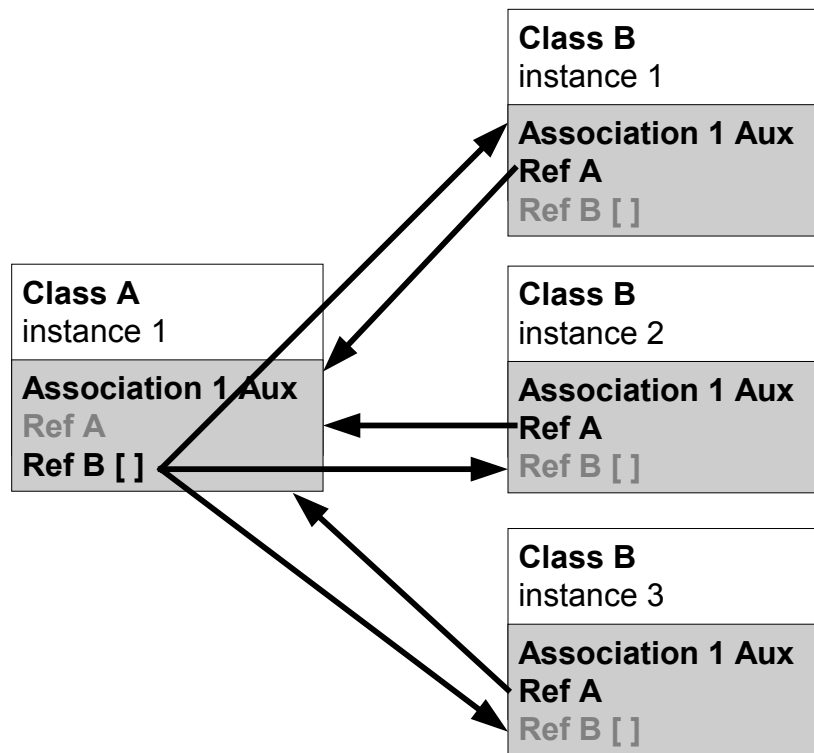
There are three distinct models used for mapping non-abstract associations in this document. Each has its own conventions for how such associations are not only mapped, but also implemented in the directory. The following sections discuss these conventions. Since all associations have referential properties, the term “additional properties” in the remainder of this section refers to non-referential properties. The approach in Section 2.2.3 may also be used to map associations with no additional properties and 1-to-1 or 1-to-many associations with additional properties if necessary.

2.2.1 No Additional Properties

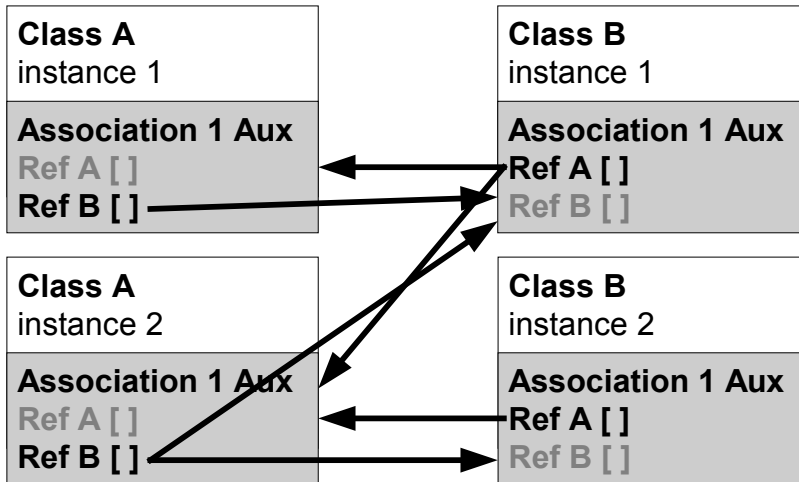
If a non-abstract association has no additional properties, then it is mapped as an auxiliary class that contains both referential properties as optional DN attributes. This class is attached to all structural objects that participate in the association, with the proper attribute being populated for that particular structural object. An example of this type of association is CIM_HostedService.



One-to-One



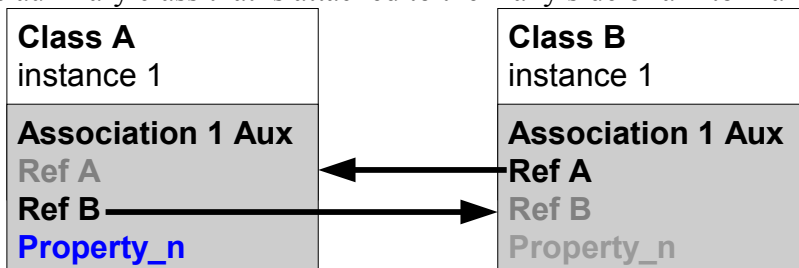
One-to-many



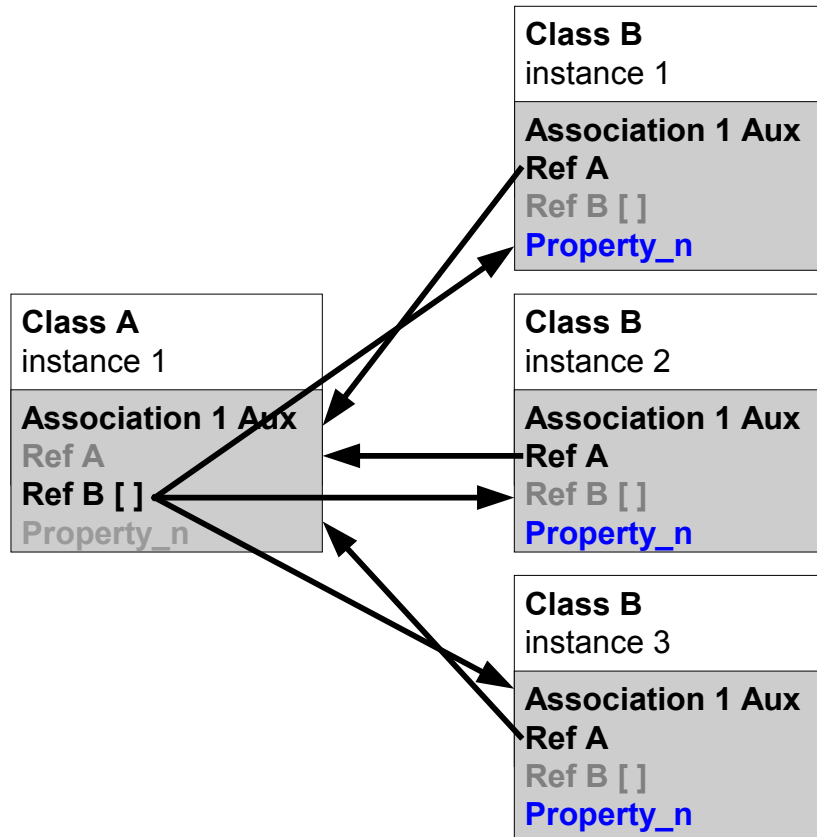
Many-to-Many

2.2.2 Additional Properties, 1-to-1 or 1-to-many

If a non-abstract association has additional properties, then the mapping is determined by the cardinality of the referential properties. In the case of a 1-to-1 or 1-to-many cardinality, the association is mapped as an auxiliary class with all properties mapped as optional attributes. The auxiliary class is attached to all structural objects participating in the association, with the referential attribute set appropriately. The additional properties are set for the auxiliary class that is attached to the many side of a 1-to-many association.



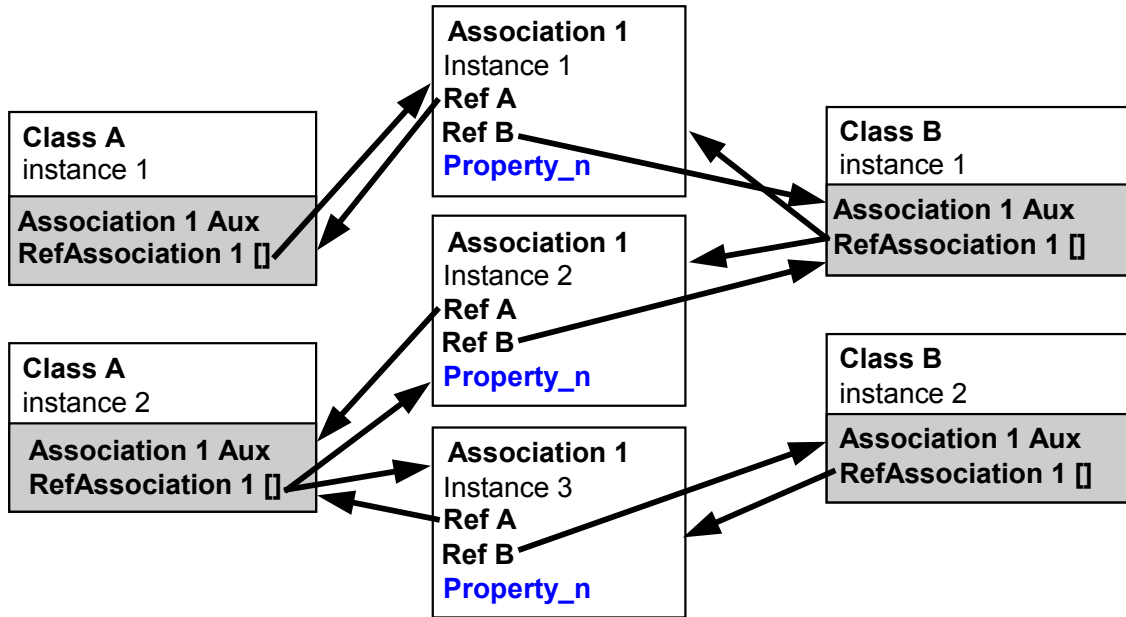
One-to-one with properties



One-to-many with properties

2.2.3 Additional Properties, many-to-many

For a non-abstract association with additional properties and a many-to-many cardinality, the most flexible mapping is to use a structural LDAP class that contains all properties of the association as optional attributes. Since this is a separate object in the directory, helper auxiliary classes are provided that are attached to the structural objects in the directory participating in the association. These helper classes contain a single optional attribute that points to the particular instance of the association that this object participates in. There is an instance of the structural class for every instance of the association. An example of this type of association is `CIM_ServiceServiceDependency`.



Many-to-many with properties

This approach may also be used to map associations with no additional properties and 1-to-1 or 1-to-many associations with additional properties if necessary.

3 Class Definitions

For efficiency in the LDAP representation, associations are specified as a combination of auxiliary classes and DIT structure rules. Attribute definitions for each class are presented with the object class. Other definitions are also provided when necessary.

While this approach was chosen to minimize the number of DN pointers stored in the schema, some pointer dereferencing may be necessary.

3.1 SecurityService

This class provides a super-class for security services. Being abstract, it cannot be instantiated in a directory.

```
( 1.3.6.1.4.1.412.100.4.1.1.4 NAME 'd1m1SecurityService'
  DESC 'SecurityService ...'
  SUP d1m1Service ABSTRACT
)
```

3.2 AccountManagementService Classes

These classes handle mapping of AccountManagementService, which creates, manages, and destroys account entries on behalf of other SecurityServices.

```
( 1.3.6.1.4.1.412.100.4.1.1.5 NAME 'd1m1AccountManagementService'
  DESC 'AccountManagementService creates, manages, and if
        necessary destroys Accounts on behalf of other
        SecurityServices.'
  SUP d1m1SecurityService ABSTRACT
```

```

)

( 1.3.6.1.4.1.412.100.4.1.1.6 NAME
'dlmlAccountManagementServiceAuxClass'
  DESC 'AccountManagementService creates, manages, and if
        necessary destroys Accounts on behalf of other
        SecurityServices.'
  SUP dlmlAccountManagementService AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.7 NAME
'dlmlAccountManagementServiceInstance'
  DESC 'AccountManagementService creates, manages, and if
        necessary destroys Accounts on behalf of other
        SecurityServices.'
  SUP dlmlAccountManagementService
)

( 1.3.6.1.4.1.412.100.4.3.1.1 NAME
'dlmlAccountManagementServiceInstanceNameForm1'
  OC dlmlAccountManagementServiceInstance
  MUST ( orderedCimKeys )
)

( <user-sr-1 NAME
'dlmlAccountManagementServiceInstanceStructureRule1'
  Form dlmlAccountManagementServiceInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to dlmlAccountManagementServiceInstance.

```

( 1.3.6.1.4.1.412.100.4.1.1.7 NAME
'dlmlAccountManagementServiceInstanceContentRule'
  DESC 'Aux classes that can attach to
        dlmlAccountManagementServiceInstance.'
  AUX ( dlmlManagesAccountAuxClass $
        dlmlManagesAccountOnSystemAuxClass $
        dlmlSecurityServiceUsesAccountAuxClass $
        dlmlServiceUsesSecurityServiceHelperAuxClass $
        dlmlSecurityServiceForSystemAuxClass $
        dlmlServiceAccessBySAPAuxClass $
        dlmlProvidesServiceToElementAuxClass $
        dlmlServiceServiceDependencyHelperAuxClass $
        dlmlServiceSAPDependencyAuxClass $
        dlmlLogicalIdentityAuxClass $
        dlmlSynchronizedHelperAuxClass $
        dlmlElementConfigurationAuxClass $
        dlmlElementSettingAuxClass $
        dlmlDefaultSettingAuxClass $ dlmlDependencyAuxClass $
        dlmlElementAsUserAuxClass $
        dlmlAuthenticationTargetAuxClass $
        dlmlAuthorizationSubjectAuxClass $
        dlmlAuthorizationTargetAuxClass $
        dlmlServiceComponentAuxClass $
        dlmlCollectedMSEsAuxClass $ dlmlComponentAuxClass $

```

```

        dlmlSystemComponentAuxClass $
        dlmlMemberOfCollectionAuxClass $
        dlmlMemberPrincipalHelperAuxClass )
    )

```

3.3 AuthenticationService Classes

These classes map AuthenticationService, which verifies the identity of users. Subclasses of this superclass include providing credentials to users and verification of the validity of a credential. An account entry for a particular UserAccess entry is used to store the persistent state information that is kept across verifications of credentials.

```

    ( 1.3.6.1.4.1.412.100.4.1.1.8 NAME 'dlmlAuthenticationService'
      DESC 'AuthenticationService verifies users" identities
        through some means. These services are decomposed
        into a subclass that provides credentials to users and
        a subclass that provides for the verification of the
        validity of a credential and, perhaps, the
        appropriateness of its use for access to target
        resources. The persistent state information used from
        one such verification to another is maintained in an
        Account for that Users Access on that
        AuthenticationService.'
      SUP dlmlSecurityService ABSTRACT
    )

    ( 1.3.6.1.4.1.412.100.4.1.1.9 NAME
'dlmlAuthenticationServiceAuxClass'
      DESC 'AuthenticationService verifies users" identities
        through some means. These services are decomposed
        into a subclass that provides credentials to users and
        a subclass that provides for the verification of the
        validity of a credential and, perhaps, the
        appropriateness of its use for access to target
        resources. The persistent state information used from
        one such verification to another is maintained in an
        Account for that Users Access on that
        AuthenticationService.'
      SUP dlmlAuthenticationService AUXILIARY
    )

    ( 1.3.6.1.4.1.412.100.4.1.1.10 NAME
'dlmlAuthenticationServiceInstance'
      DESC 'AuthenticationService verifies users" identities
        through some means. These services are decomposed
        into a subclass that provides credentials to users and
        a subclass that provides for the verification of the
        validity of a credential and, perhaps, the
        appropriateness of its use for access to target
        resources. The persistent state information used from
        one such verification to another is maintained in an
        Account for that Users Access on that
        AuthenticationService.'
      SUP dlmlAuthenticationService
    )

```

```

( <.3.6.1.4.1.412.100.4.3.1.2 NAME
'dlmlAuthenticationServiceInstanceNameForm1'
  OC dlmlAuthenticationServiceInstance
  MUST ( orderedCimKeys )
)

( <user-sr-2 NAME 'dlmlAuthenticationServiceInstanceStructureRule1'
  Form dlmlAuthenticationServiceInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to dlmlAuthenticationServiceInstance.

```

( 1.3.6.1.4.1.412.100.4.1.1.10 NAME
'dlmlAuthenticationServiceInstanceContentRule'
  DESC 'Aux classes that can attach to
  dlmlAuthenticationServiceInstance.'
  AUX ( dlmlAuthenticateForUseAuxClass $
  dlmlSecurityServiceUsesAccountAuxClass $
  dlmlServiceUsesSecurityServiceHelperAuxClass $
  dlmlSecurityServiceForSystemAuxClass $
  dlmlServiceAccessBySAPAuxClass $
  dlmlProvidesServiceToElementAuxClass $
  dlmlServiceServiceDependencyHelperAuxClass $
  dlmlServiceSAPDependencyAuxClass $
  dlmlLogicalIdentityAuxClass $
  dlmlSynchronizedHelperAuxClass $
  dlmlElementConfigurationAuxClass $
  dlmlElementSettingAuxClass $
  dlmlDefaultSettingAuxClass $ dlmlDependencyAuxClass $
  dlmlElementAsUserAuxClass $
  dlmlAuthenticationTargetAuxClass $
  dlmlAuthorizationSubjectAuxClass $
  dlmlAuthorizationTargetAuxClass $
  dlmlServiceComponentAuxClass $
  dlmlCollectedMSEsAuxClass $ dlmlComponentAuxClass $
  dlmlSystemComponentAuxClass $
  dlmlMemberOfCollectionAuxClass $
  dlmlMemberPrincipalHelperAuxClass )
)

```

3.4 VerificationService Classes

These classes map VerificationService, the subclass of AuthenticationService that verifies a credential for use. Optionally, it may also verify whether the credential is appropriate for accessing a particular target resource.

```

( 1.3.6.1.4.1.412.100.4.1.1.11 NAME 'dlmlVerificationService'
  DESC 'VerificationService is the authentication service
  that verifies a credential for use and may also verify
  the appropriateness of a particular credential in
  conjunction with a particular target resource.'
  SUP dlmlAuthenticationService ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.1.1.12 NAME 'dlmlVerificationServiceAuxClass'

```

```

DESC 'VerificationService is the authentication service
      that verifies a credential for use and may also verify
      the appropriateness of a particular credential in
      conjunction with a particular target resource.'
SUP dlm1VerificationService AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.13 NAME 'dlm1VerificationServiceInstance'
  DESC 'VerificationService is the authentication service
        that verifies a credential for use and may also verify
        the appropriateness of a particular credential in
        conjunction with a particular target resource.'
  SUP dlm1VerificationService
)

( 1.3.6.1.4.1.412.100.4.3.1.3 NAME
'dlm1VerificationServiceInstanceNameForm1'
  OC dlm1VerificationServiceInstance
  MUST ( orderedCimKeys )
)

( <user-sr-3 NAME 'dlm1VerificationServiceInstanceStructureRule1'
  Form dlm1VerificationServiceInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to dlm1VerificationServiceInstance.

```

( 1.3.6.1.4.1.412.100.4.1.1.13 NAME
'dlm1VerificationServiceInstanceContentRule'
  DESC 'Aux classes that can attach to
        dlm1VerificationServiceInstance.'
  AUX ( dlm1AuthenticateForUseAuxClass $
        dlm1SecurityServiceUsesAccountAuxClass $
        dlm1ServiceUsesSecurityServiceHelperAuxClass $
        dlm1SecurityServiceForSystemAuxClass $
        dlm1ServiceAccessBySAPAuxClass $
        dlm1ProvidesServiceToElementAuxClass $
        dlm1ServiceServiceDependencyHelperAuxClass $
        dlm1ServiceSAPDependencyAuxClass $
        dlm1LogicalIdentityAuxClass $
        dlm1SynchronizedHelperAuxClass $
        dlm1ElementConfigurationAuxClass $
        dlm1ElementSettingAuxClass $
        dlm1DefaultSettingAuxClass $ dlm1DependencyAuxClass $
        dlm1ElementAsUserAuxClass $
        dlm1AuthenticationTargetAuxClass $
        dlm1AuthorizationSubjectAuxClass $
        dlm1AuthorizationTargetAuxClass $
        dlm1ServiceComponentAuxClass $
        dlm1CollectedMSEsAuxClass $ dlm1ComponentAuxClass $
        dlm1SystemComponentAuxClass $
        dlm1MemberOfCollectionAuxClass $
        dlm1MemberPrincipalHelperAuxClass )
)

```

3.5 CredentialManagementService Classes

These classes map CredentialManagementServices. Entries of these classes model a service that issues credentials and manages the credential lifecycle.

```
( 1.3.6.1.4.1.412.100.4.1.1.14 NAME 'dlm1CredentialManagementService'
  DESC 'CredentialManagementService issues credentials
        and manages the credential lifecycle.'
  SUP dlm1AuthenticationService ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.1.1.15 NAME
'dlm1CredentialManagementServiceAuxClass'
  DESC 'CredentialManagementService issues credentials
        and manages the credential lifecycle.'
  SUP dlm1CredentialManagementService AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.16 NAME
'dlm1CredentialManagementServiceInstance'
  DESC 'CredentialManagementService issues credentials
        and manages the credential lifecycle.'
  SUP dlm1CredentialManagementService
)

( 1.3.6.1.4.1.412.100.4.3.1.4 NAME
'dlm1CredentialManagementServiceInstanceNameForm1'
  OC dlm1CredentialManagementServiceInstance
  MUST ( orderedCimKeys )
)

( <user-sr-4 NAME
'dlm1CredentialManagementServiceInstanceStructureRule1'
  Form dlm1CredentialManagementServiceInstanceNameForm1
)
```

The following content rule specifies the auxiliary classes that may be attached to dlm1CredentialManagementServiceInstance.

```
( 1.3.6.1.4.1.412.100.4.1.1.16 NAME
'dlm1CredentialManagementServiceInstanceContentRule'
  DESC 'Aux classes that can attach to
        dlm1CredentialManagementServiceInstance.'
  AUX ( dlm1TrustHierarchyAuxClass $
        dlm1ManagedCredentialAuxClass $
        dlm1RequireCredentialsFromAuxClass $
        dlm1AuthenticateForUseAuxClass $
        dlm1SecurityServiceUsesAccountAuxClass $
        dlm1ServiceUsesSecurityServiceHelperAuxClass $
        dlm1SecurityServiceForSystemAuxClass $
        dlm1ServiceAccessBySAPAuxClass $
        dlm1ProvidesServiceToElementAuxClass $
        dlm1ServiceServiceDependencyHelperAuxClass $
        dlm1ServiceSAPDependencyAuxClass $
        dlm1LogicalIdentityAuxClass $
        dlm1SynchronizedHelperAuxClass $
```

```

    dlm1ElementConfigurationAuxClass $
    dlm1ElementSettingAuxClass $
    dlm1DefaultSettingAuxClass $ dlm1DependencyAuxClass $
    dlm1ElementAsUserAuxClass $
    dlm1AuthenticationTargetAuxClass $
    dlm1AuthorizationSubjectAuxClass $
    dlm1AuthorizationTargetAuxClass $
    dlm1ServiceComponentAuxClass $
    dlm1CollectedMSEsAuxClass $ dlm1ComponentAuxClass $
    dlm1SystemComponentAuxClass $
    dlm1MemberOfCollectionAuxClass $
    dlm1MemberPrincipalHelperAuxClass )
)

```

3.6 CertificateAuthority Classes

These classes map CertificateAuthority. Entries of this class model credential management services that issues and cryptographically signs certificates. Thus these services provide the trusted third-party intermediary in establishing trust relationship. The service authenticates the holder of the private key that is related to the certificate's public key. The authenticate entity is modeled by entries of the UsersAccess class.

```

( 1.3.6.1.4.1.412.100.4.2.1 NAME 'dlmCADistinguishedName'
  DESC 'Certificates refer to their issuing CA by its
        Distinguished Name (as defined in X.501).'
```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
EQUALITY distinguishedNameMatch
)

```

( 1.3.6.1.4.1.412.100.4.2.2 NAME 'dlmCAPolicyStatement'
  DESC 'The CAPolicyStatement describes what care is
        taken by the CertificateAuthority when signing a new
        certificate. The CAPolicyStatment may be a
        dot-delimited ASN.1 OID string which identifies to the
        formal policy statement.'
```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
EQUALITY caseIgnoreMatch
)

```

( 1.3.6.1.4.1.412.100.4.2.3 NAME 'dlmCRL'
  DESC 'A CRL, or CertificateRevocationList, is a list of
        certificates which the CertificateAuthority has revoked
        and which are not yet expired. Revocation is necessary
        when the private key associated with the public key of
        a certificate is lost or compromised, or when the
        person for whom the certificate is signed no longer is
        entitled to use the certificate.'
```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
EQUALITY caseIgnoreMatch
)

```

( 1.3.6.1.4.1.412.100.4.2.4 NAME 'dlmCRLDistributionPoint'
  DESC 'Certificate Revocation Lists may be available
        from a number of distribution points.
        CRLDistributionPoint array values provide URIs for
```



```

        those distribution points.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.2.5 NAME 'dlmCRLRefreshFrequency'
  DESC 'The frequency, expressed in hours, at which the
        CA will update its Certificate Revocation List. Zero
        implies that the refresh frequency is unknown. The
        value is considered to be Hours.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE
  EQUALITY integerMatch
)

( 1.3.6.1.4.1.412.100.4.2.6 NAME 'dlmMaxChainLength'
  DESC 'The maximum number of certificates in a
        certificate chain permitted for credentials issued by
        this certificate authority or it"s subordinate CAs.
        The MaxChainLength of a superior CA in the trust
        hierarchy should be greater than this value and the
        MaxChainLength of a subordinate CA in the trust
        hierarchy should be less than this value.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE
  EQUALITY integerMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.17 NAME 'dlm1CertificateAuthority'
  DESC 'A Certificate Authority (CA) is a credential
        management service that issues and cryptographically
        signs certificates thus acting as an trusted
        third-party intermediary in establishing trust
        relationships. The CA authenticates the holder of the
        private key related to the certificate"s public key;
        the authenticated entity is represented by the
        UsersAccess class.'
  SUP dlm1CredentialManagementService ABSTRACT
  MAY ( dlmCADistinguishedName $ dlmCAPolicyStatement $
        dlmCRL $ dlmCRLDistributionPoint $
        dlmCRLRefreshFrequency $ dlmMaxChainLength )
)

( 1.3.6.1.4.1.412.100.4.1.1.18 NAME
'dlm1CertificateAuthorityAuxClass'
  DESC 'A Certificate Authority (CA) is a credential
        management service that issues and cryptographically
        signs certificates thus acting as an trusted
        third-party intermediary in establishing trust
        relationships. The CA authenticates the holder of the
        private key related to the certificate"s public key;
        the authenticated entity is represented by the
        UsersAccess class.'
  SUP dlm1CertificateAuthority AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.19 NAME
'dlm1CertificateAuthorityInstance'
  DESC 'A Certificate Authority (CA) is a credential

```

management service that issues and cryptographically signs certificates thus acting as an trusted third-party intermediary in establishing trust relationships. The CA authenticates the holder of the private key related to the certificate's public key; the authenticated entity is represented by the UsersAccess class.'

```
SUP dlm1CertificateAuthority
)

( 1.3.6.1.4.1.412.100.4.3.1.5 NAME
'dlm1CertificateAuthorityInstanceNameForm1'
  OC dlm1CertificateAuthorityInstance
  MUST ( orderedCimKeys )
)

( <user-sr-5 NAME 'dlm1CertificateAuthorityInstanceStructureRule1'
  Form dlm1CertificateAuthorityInstanceNameForm1
)
)
```

The following content rule specifies the auxiliary classes that may be attached to dlm1CertificateAuthorityInstance.

```
( 1.3.6.1.4.1.412.100.4.1.1.19 NAME
'dlm1CertificateAuthorityInstanceContentRule'
  DESC 'Aux classes that can attach to
  dlm1CertificateAuthorityInstance.'
  AUX ( dlm1CAHasPublicCertificateAuxClass $
  dlm1TrustHierarchyAuxClass $
  dlm1ManagedCredentialAuxClass $
  dlm1RequireCredentialsFromAuxClass $
  dlm1AuthenticateForUseAuxClass $
  dlm1SecurityServiceUsesAccountAuxClass $
  dlm1ServiceUsesSecurityServiceHelperAuxClass $
  dlm1SecurityServiceForSystemAuxClass $
  dlm1ServiceAccessBySAPAuxClass $
  dlm1ProvidesServiceToElementAuxClass $
  dlm1ServiceServiceDependencyHelperAuxClass $
  dlm1ServiceSAPDependencyAuxClass $
  dlm1LogicalIdentityAuxClass $
  dlm1SynchronizedHelperAuxClass $
  dlm1ElementConfigurationAuxClass $
  dlm1ElementSettingAuxClass $
  dlm1DefaultSettingAuxClass $ dlm1DependencyAuxClass $
  dlm1ElementAsUserAuxClass $
  dlm1AuthenticationTargetAuxClass $
  dlm1AuthorizationSubjectAuxClass $
  dlm1AuthorizationTargetAuxClass $
  dlm1ServiceComponentAuxClass $
  dlm1CollectedMSEsAuxClass $ dlm1ComponentAuxClass $
  dlm1SystemComponentAuxClass $
  dlm1MemberOfCollectionAuxClass $
  dlm1MemberPrincipalHelperAuxClass )
)
)
```

3.7 KerberosKeyDistributionCenter Classes

Entries of these classes model Kerberos key distribution centers.

```
( 1.3.6.1.4.1.412.100.4.2.7 NAME 'dlmProtocol'
  DESC 'The version of Kerberos supported by this
        service. Values are 0="V4", 1="V5", 2="DCE", 3="MS".'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  EQUALITY integerMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.20 NAME
'dlm1KerberosKeyDistributionCenter'
  DESC 'KerberosKeyDistributionCenter ...'
  SUP dlm1CredentialManagementService ABSTRACT
  MAY ( dlmName $ dlmProtocol )
)

( 1.3.6.1.4.1.412.100.4.1.1.21 NAME
'dlm1KerberosKeyDistributionCenterAuxClass'
  DESC 'KerberosKeyDistributionCenter ...'
  SUP dlm1KerberosKeyDistributionCenter AUXILIARY
  MAY ( dlmName $ dlmProtocol )
)

( 1.3.6.1.4.1.412.100.4.1.1.22 NAME
'dlm1KerberosKeyDistributionCenterInstance'
  DESC 'KerberosKeyDistributionCenter ...'
  SUP dlm1KerberosKeyDistributionCenter
  MAY ( dlmName $ dlmProtocol )
)

( 1.3.6.1.4.1.412.100.4.3.1.6 NAME
'dlm1KerberosKeyDistributionCenterInstanceNameForm1'
  OC dlm1KerberosKeyDistributionCenterInstance
  MUST ( orderedCimKeys )
)

( <user-sr-6 NAME
'dlm1KerberosKeyDistributionCenterInstanceStructureRule1'
  Form dlm1KerberosKeyDistributionCenterInstanceNameForm1
)
```

The following content rule specifies the auxiliary classes that may be attached to `dlm1KerberosKeyDistributionCenterInstance`.

```
( 1.3.6.1.4.1.412.100.4.1.1.22 NAME
'dlm1KerberosKeyDistributionCenterInstanceContentRule'
  DESC 'Aux classes that can attach to
        dlm1KerberosKeyDistributionCenterInstance.'
  AUX ( dlm1TrustHierarchyAuxClass $
        dlm1ManagedCredentialAuxClass $
        dlm1RequireCredentialsFromAuxClass $
        dlm1AuthenticateForUseAuxClass $
        dlm1SecurityServiceUsesAccountAuxClass $
        dlm1ServiceUsesSecurityServiceHelperAuxClass $
```

```

    dlm1SecurityServiceForSystemAuxClass $
    dlm1ServiceAccessBySAPAuxClass $
    dlm1ProvidesServiceToElementAuxClass $
    dlm1ServiceServiceDependencyHelperAuxClass $
    dlm1ServiceSAPDependencyAuxClass $
    dlm1LogicalIdentityAuxClass $
    dlm1SynchronizedHelperAuxClass $
    dlm1ElementConfigurationAuxClass $
    dlm1ElementSettingAuxClass $
    dlm1DefaultSettingAuxClass $ dlm1DependencyAuxClass $
    dlm1ElementAsUserAuxClass $
    dlm1AuthenticationTargetAuxClass $
    dlm1AuthorizationSubjectAuxClass $
    dlm1AuthorizationTargetAuxClass $
    dlm1ServiceComponentAuxClass $
    dlm1CollectedMSEsAuxClass $ dlm1ComponentAuxClass $
    dlm1SystemComponentAuxClass $
    dlm1MemberOfCollectionAuxClass $
    dlm1MemberPrincipalHelperAuxClass )
)

```

3.8 NotaryInstance Classes

Entries of this subclass of CredentialManagementService model services that compare the biometric characteristics of a person with the known characteristics associated with a UserAccess entry. It then determines if the person is the UserAccess entry. As examples, consider a bank teller who compares a picture ID with the person trying to cash a check, or a biometric login service that uses voice recognition to identify a user.

```

( 1.3.6.1.4.1.412.100.4.2.8 NAME 'dlmCharterExpired'
  DESC 'CharterExpired documents when the Notary is no
        longer authorized, by whoever gave it responsibility,
        to perform its service.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 SINGLE-VALUE
  EQUALITY generalizedTimeMatch
)

( 1.3.6.1.4.1.412.100.4.2.9 NAME 'dlmCharterIssued'
  DESC 'CharterIssued documents when the Notary is first
        authorized, by whoever gave it responsibility, to
        perform its service.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 SINGLE-VALUE
  EQUALITY generalizedTimeMatch
)

( 1.3.6.1.4.1.412.100.4.2.10 NAME 'dlmComparitors'
  DESC 'The types of biometric information which this
        Notary can compare. Values are 0="N/A", 1="Other",
        2="Facial", 3="Retina", 4="Mark", 5="Finger",
        6="Voice", 7="DNA-RNA", 8="EEG".'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE
  EQUALITY integerMatch
)

( 1.3.6.1.4.1.412.100.4.2.11 NAME 'dlmSealProtocol'
  DESC 'The SealProtocol is how the decision of the

```

Notary is recorded for future use by parties who will rely on its decision. For instance, a drivers licence frequently includes tamper-resistant coatings and markings to protect the recorded decision that a driver, having various biometric characteristics of height, weight, hair and eye color, using a particular name, has features represented in a photograph of their face.'

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
EQUALITY caseIgnoreMatch

)

(1.3.6.1.4.1.412.100.4.1.1.23 NAME 'd1m1Notary'

DESC 'Notary is an AuthenticationService (credential management service) which compares the biometric characteristics of a person with the known characteristics of an Users Access, and determines whether the person is the UsersAccess. An example is a bank teller who compares a picture ID with the person trying to cash a check, or a biometric login service that uses voice recognition to identify a user.'

SUP d1m1CredentialManagementService ABSTRACT
MAY (d1m1CharterExpired \$ d1m1CharterIssued \$
d1m1Comparitors \$ d1m1SealProtocol)

)

(1.3.6.1.4.1.412.100.4.1.1.24 NAME 'd1m1NotaryAuxClass'

DESC 'Notary is an AuthenticationService (credential management service) which compares the biometric characteristics of a person with the known characteristics of an Users Access, and determines whether the person is the UsersAccess. An example is a bank teller who compares a picture ID with the person trying to cash a check, or a biometric login service that uses voice recognition to identify a user.'

SUP d1m1Notary AUXILIARY
MAY (d1m1CharterExpired \$ d1m1CharterIssued \$
d1m1Comparitors \$ d1m1SealProtocol)

)

(1.3.6.1.4.1.412.100.4.1.1.25 NAME 'd1m1NotaryInstance'

DESC 'Notary is an AuthenticationService (credential management service) which compares the biometric characteristics of a person with the known characteristics of an Users Access, and determines whether the person is the UsersAccess. An example is a bank teller who compares a picture ID with the person trying to cash a check, or a biometric login service that uses voice recognition to identify a user.'

SUP d1m1Notary
MAY (d1m1CharterExpired \$ d1m1CharterIssued \$
d1m1Comparitors \$ d1m1SealProtocol)

)

```

( 1.3.6.1.4.1.412.100.4.3.1.7 NAME 'dmlNotaryInstanceNameForm1'
  OC dmlNotaryInstance
  MUST ( orderedCimKeys )
)

( <user-sr-7 NAME 'dmlNotaryInstanceStructureRule1'
  Form dmlNotaryInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to dmlNotaryInstance.

```

( 1.3.6.1.4.1.412.100.4.1.1.25 NAME 'dmlNotaryInstanceContentRule'
  DESC 'Aux classes that can attach to
        dmlNotaryInstance.'
  AUX ( dmlNotaryVerifiesBiometricAuxClass $
        dmlTrustHierarchyAuxClass $
        dmlManagedCredentialAuxClass $
        dmlRequireCredentialsFromAuxClass $
        dmlAuthenticateForUseAuxClass $
        dmlSecurityServiceUsesAccountAuxClass $
        dmlServiceUsesSecurityServiceHelperAuxClass $
        dmlSecurityServiceForSystemAuxClass $
        dmlServiceAccessBySAPAuxClass $
        dmlProvidesServiceToElementAuxClass $
        dmlServiceServiceDependencyHelperAuxClass $
        dmlServiceSAPDependencyAuxClass $
        dmlLogicalIdentityAuxClass $
        dmlSynchronizedHelperAuxClass $
        dmlElementConfigurationAuxClass $
        dmlElementSettingAuxClass $
        dmlDefaultSettingAuxClass $ dmlDependencyAuxClass $
        dmlElementAsUserAuxClass $
        dmlAuthenticationTargetAuxClass $
        dmlAuthorizationSubjectAuxClass $
        dmlAuthorizationTargetAuxClass $
        dmlServiceComponentAuxClass $
        dmlCollectedMSEsAuxClass $ dmlComponentAuxClass $
        dmlSystemComponentAuxClass $
        dmlMemberOfCollectionAuxClass $
        dmlMemberPrincipalHelperAuxClass )
)

```

3.9 LocalCredentialManagementService Classes

This subclass of CredentialManagementService models those services that provides local system management of credentials that the local system uses.

```

( 1.3.6.1.4.1.412.100.4.1.1.26 NAME
'dmlLocalCredentialManagementService'
  DESC 'LocalCredentialManagementService is a credential
        management service that provides local system
        management of credentials used by the local system.'
  SUP dmlCredentialManagementService ABSTRACT
)

```

```

( 1.3.6.1.4.1.412.100.4.1.1.27 NAME
'dlm1LocalCredentialManagementServiceAuxClass'
  DESC 'LocalCredentialManagementService is a credential
        management service that provides local system
        management of credentials used by the local system.'
  SUP dlm1LocalCredentialManagementService AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.28 NAME
'dlm1LocalCredentialManagementServiceInstance'
  DESC 'LocalCredentialManagementService is a credential
        management service that provides local system
        management of credentials used by the local system.'
  SUP dlm1LocalCredentialManagementService
)

( 1.3.6.1.4.1.412.100.4.3.1.8 NAME
'dlm1LocalCredentialManagementServiceInstanceNameForm1'
  OC dlm1LocalCredentialManagementServiceInstance
  MUST ( orderedCimKeys )
)

( <user-sr-8 NAME
'dlm1LocalCredentialManagementServiceInstanceStructureRule1'
  Form dlm1LocalCredentialManagementServiceInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to `dlm1LocalCredentialManagementServiceInstance`.

```

( 1.3.6.1.4.1.412.100.4.1.1.28 NAME
'dlm1LocalCredentialManagementServiceInstanceContentRule'
  DESC 'Aux classes that can attach to
        dlm1LocalCredentialManagementServiceInstance.'
  AUX ( dlm1TrustHierarchyAuxClass $
        dlm1ManagedCredentialAuxClass $
        dlm1RequireCredentialsFromAuxClass $
        dlm1AuthenticateForUseAuxClass $
        dlm1SecurityServiceUsesAccountAuxClass $
        dlm1ServiceUsesSecurityServiceHelperAuxClass $
        dlm1SecurityServiceForSystemAuxClass $
        dlm1ServiceAccessBySAPAuxClass $
        dlm1ProvidesServiceToElementAuxClass $
        dlm1ServiceServiceDependencyHelperAuxClass $
        dlm1ServiceSAPDependencyAuxClass $
        dlm1LogicalIdentityAuxClass $
        dlm1SynchronizedHelperAuxClass $
        dlm1ElementConfigurationAuxClass $
        dlm1ElementSettingAuxClass $
        dlm1DefaultSettingAuxClass $ dlm1DependencyAuxClass $
        dlm1ElementAsUserAuxClass $
        dlm1AuthenticationTargetAuxClass $
        dlm1AuthorizationSubjectAuxClass $
        dlm1AuthorizationTargetAuxClass $
        dlm1ServiceComponentAuxClass $
        dlm1CollectedMSEsAuxClass $ dlm1ComponentAuxClass $

```

```

    dlm1SystemComponentAuxClass $
    dlm1MemberOfCollectionAuxClass $
    dlm1MemberPrincipalHelperAuxClass )

```

3.10 SharedSecretService Classes

Entries of these classes model a service that determines if messages received from the Principal with whom a secret is shared. Examples are a login service that proves identity based on knowledge of the shared secret, or a transport integrity service (like Kerberos) that includes a MAC (message authentication code) that proves each message in the stream came from someone who has knowledge of the shared secret session key.

```

( 1.3.6.1.4.1.412.100.4.2.12 NAME 'dlmAlgorithm'
  DESC 'The Algorithm used to convey the shared secret,
        such as HMAC-MD5, or PLAINTEXT.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.29 NAME 'dlm1SharedSecretService'
  DESC 'SharedSecretService is a service which ascertains
        whether messages received are from the Principal with
        whom a secret is shared.  Examples include a login
        service that proves identity on the basis of knowledge
        of the shared secret, or a transport integrity service
        (like Kerberos provides) that includes a message
        authenticity code that proves each message in the
        message stream came from someone who knows the shared
        secret session key.'
  SUP dlm1LocalCredentialManagementService ABSTRACT
  MAY ( dlmAlgorithm $ dlmProtocol )
)

( 1.3.6.1.4.1.412.100.4.1.1.30 NAME 'dlm1SharedSecretServiceAuxClass'
  DESC 'SharedSecretService is a service which ascertains
        whether messages received are from the Principal with
        whom a secret is shared.  Examples include a login
        service that proves identity on the basis of knowledge
        of the shared secret, or a transport integrity service
        (like Kerberos provides) that includes a message
        authenticity code that proves each message in the
        message stream came from someone who knows the shared
        secret session key.'
  SUP dlm1SharedSecretService AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.31 NAME 'dlm1SharedSecretServiceInstance'
  DESC 'SharedSecretService is a service which ascertains
        whether messages received are from the Principal with
        whom a secret is shared.  Examples include a login
        service that proves identity on the basis of knowledge
        of the shared secret, or a transport integrity service
        (like Kerberos provides) that includes a message
        authenticity code that proves each message in the
        message stream came from someone who knows the shared

```



```

        secret session key.'
    SUP dlm1SharedSecretService
)

( 1.3.6.1.4.1.412.100.4.3.1.9 NAME
'dlm1SharedSecretServiceInstanceNameForm1'
  OC dlm1SharedSecretServiceInstance
  MUST ( orderedCimKeys )
)

( <user-sr-9 NAME 'dlm1SharedSecretServiceInstanceStructureRule1'
  Form dlm1SharedSecretServiceInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to dlm1SharedSecretServiceInstance.

```

( 1.3.6.1.4.1.412.100.4.1.1.31 NAME
'dlm1SharedSecretServiceInstanceContentRule'
  DESC 'Aux classes that can attach to
  dlm1SharedSecretServiceInstance.'
  AUX ( dlm1TrustHierarchyAuxClass $
    dlm1ManagedCredentialAuxClass $
    dlm1RequireCredentialsFromAuxClass $
    dlm1AuthenticateForUseAuxClass $
    dlm1SecurityServiceUsesAccountAuxClass $
    dlm1ServiceUsesSecurityServiceHelperAuxClass $
    dlm1SecurityServiceForSystemAuxClass $
    dlm1ServiceAccessBySAPAuxClass $
    dlm1ProvidesServiceToElementAuxClass $
    dlm1ServiceServiceDependencyHelperAuxClass $
    dlm1ServiceSAPDependencyAuxClass $
    dlm1LogicalIdentityAuxClass $
    dlm1SynchronizedHelperAuxClass $
    dlm1ElementConfigurationAuxClass $
    dlm1ElementSettingAuxClass $
    dlm1DefaultSettingAuxClass $ dlm1DependencyAuxClass $
    dlm1ElementAsUserAuxClass $
    dlm1AuthenticationTargetAuxClass $
    dlm1AuthorizationSubjectAuxClass $
    dlm1AuthorizationTargetAuxClass $
    dlm1ServiceComponentAuxClass $
    dlm1CollectedMSEsAuxClass $ dlm1ComponentAuxClass $
    dlm1SystemComponentAuxClass $
    dlm1MemberOfCollectionAuxClass $
    dlm1MemberPrincipalHelperAuxClass )
)

```

3.11 PublicKeyManagementService Classes

This subclass of LocalCredentialManagementService models a service that provides local system management of public keys used by the local system.

```

( 1.3.6.1.4.1.412.100.4.1.1.32 NAME 'dlm1PublicKeyManagementService'
  DESC 'PublicKeyManagementService is a credential
  management service that provides local system

```

```

        management of public keys used by the local system.'
    SUP dlm1LocalCredentialManagementService ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.1.1.33 NAME
'dlm1PublicKeyManagementServiceAuxClass'
  DESC 'PublicKeyManagementService is a credential
        management service that provides local system
        management of public keys used by the local system.'
  SUP dlm1PublicKeyManagementService AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.34 NAME
'dlm1PublicKeyManagementServiceInstance'
  DESC 'PublicKeyManagementService is a credential
        management service that provides local system
        management of public keys used by the local system.'
  SUP dlm1PublicKeyManagementService
)

( 1.3.6.1.4.1.412.100.4.3.1.10 NAME
'dlm1PublicKeyManagementServiceInstanceNameForm1'
  OC dlm1PublicKeyManagementServiceInstance
  MUST ( orderedCimKeys )
)

( <user-sr-10 NAME
'dlm1PublicKeyManagementServiceInstanceStructureRule1'
  Form dlm1PublicKeyManagementServiceInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to **dlm1PublicKeyManagementServiceInstance**.

```

( 1.3.6.1.4.1.412.100.4.1.1.34 NAME
'dlm1PublicKeyManagementServiceInstanceContentRule'
  DESC 'Aux classes that can attach to
        dlm1PublicKeyManagementServiceInstance.'
  AUX ( dlm1TrustHierarchyAuxClass $
        dlm1ManagedCredentialAuxClass $
        dlm1RequireCredentialsFromAuxClass $
        dlm1AuthenticateForUseAuxClass $
        dlm1SecurityServiceUsesAccountAuxClass $
        dlm1ServiceUsesSecurityServiceHelperAuxClass $
        dlm1SecurityServiceForSystemAuxClass $
        dlm1ServiceAccessBySAPAuxClass $
        dlm1ProvidesServiceToElementAuxClass $
        dlm1ServiceServiceDependencyHelperAuxClass $
        dlm1ServiceSAPDependencyAuxClass $
        dlm1LogicalIdentityAuxClass $
        dlm1SynchronizedHelperAuxClass $
        dlm1ElementConfigurationAuxClass $
        dlm1ElementSettingAuxClass $
        dlm1DefaultSettingAuxClass $ dlm1DependencyAuxClass $
        dlm1ElementAsUserAuxClass $
        dlm1AuthenticationTargetAuxClass $

```

```

    dlmlAuthorizationSubjectAuxClass $
    dlmlAuthorizationTargetAuxClass $
    dlmlServiceComponentAuxClass $
    dlmlCollectedMSEsAuxClass $ dlmlComponentAuxClass $
    dlmlSystemComponentAuxClass $
    dlmlMemberOfCollectionAuxClass $
    dlmlMemberPrincipalHelperAuxClass )
)

```

3.12 AuthorizationService Classes

This subclass of SecurityService models a service that determine whether a user, that by association with an Account entry used by entries of this subclass, is permitted access to a set of resources.

```

( 1.3.6.1.4.1.412.100.4.1.1.35 NAME 'dlmlAuthorizationService'
  DESC 'AuthorizationService determines whether a user,
        by association with an Account used by the
        AuthorizationService, is permitted access a resource
        or set of resources.'
  SUP dlmlSecurityService ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.1.1.36 NAME
'dlmlAuthorizationServiceAuxClass'
  DESC 'AuthorizationService determines whether a user,
        by association with an Account used by the
        AuthorizationService, is permitted access a resource
        or set of resources.'
  SUP dlmlAuthorizationService AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.37 NAME
'dlmlAuthorizationServiceInstance'
  DESC 'AuthorizationService determines whether a user,
        by association with an Account used by the
        AuthorizationService, is permitted access a resource
        or set of resources.'
  SUP dlmlAuthorizationService
)

( 1.3.6.1.4.1.412.100.4.3.1.11 NAME
'dlmlAuthorizationServiceInstanceNameForm1'
  OC dlmlAuthorizationServiceInstance
  MUST ( orderedCimKeys )
)

( <user-sr-11 NAME 'dlmlAuthorizationServiceInstanceStructureRule1'
  Form dlmlAuthorizationServiceInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to dlmlAuthorizationServiceInstance.

```

( 1.3.6.1.4.1.412.100.4.1.1.37 NAME
'dlmlAuthorizationServiceInstanceContentRule'

```

```

DESC 'Aux classes that can attach to
      dlm1AuthorizationServiceInstance.'
AUX ( dlm1AuthorizedUseAuxClass $
      dlm1SecurityServiceUsesAccountAuxClass $
      dlm1ServiceUsesSecurityServiceHelperAuxClass $
      dlm1SecurityServiceForSystemAuxClass $
      dlm1ServiceAccessBySAPAuxClass $
      dlm1ProvidesServiceToElementAuxClass $
      dlm1ServiceServiceDependencyHelperAuxClass $
      dlm1ServiceSAPDependencyAuxClass $
      dlm1LogicalIdentityAuxClass $
      dlm1SynchronizedHelperAuxClass $
      dlm1ElementConfigurationAuxClass $
      dlm1ElementSettingAuxClass $
      dlm1DefaultSettingAuxClass $ dlm1DependencyAuxClass $
      dlm1ElementAsUserAuxClass $
      dlm1AuthenticationTargetAuxClass $
      dlm1AuthorizationSubjectAuxClass $
      dlm1AuthorizationTargetAuxClass $
      dlm1ServiceComponentAuxClass $
      dlm1CollectedMSEsAuxClass $ dlm1ComponentAuxClass $
      dlm1SystemComponentAuxClass $
      dlm1MemberOfCollectionAuxClass $
      dlm1MemberPrincipalHelperAuxClass )
)

```

3.13 CredentialManagementSAP

This subclass of ServiceAccessPoint models the ability to utilize or invoke a entry of class CredentialManagementService.

```

( 1.3.6.1.4.1.412.100.4.1.1.38 NAME 'dlm1CredentialManagementSAP'
  DESC 'CredentialManagementSAP represents the ability to
        utilize or invoke a CredentialManagementService.'
  SUP dlm1ServiceAccessPoint ABSTRACT
  MAY ( labeledURI )
)

( 1.3.6.1.4.1.412.100.4.1.1.39 NAME
'dlm1CredentialManagementSAPAuxClass'
  DESC 'CredentialManagementSAP represents the ability to
        utilize or invoke a CredentialManagementService.'
  SUP dlm1CredentialManagementSAP AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.40 NAME
'dlm1CredentialManagementSAPInstance'
  DESC 'CredentialManagementSAP represents the ability to
        utilize or invoke a CredentialManagementService.'
  SUP dlm1CredentialManagementSAP
)

( 1.3.6.1.4.1.412.100.4.3.1.12 NAME
'dlm1CredentialManagementSAPInstanceNameForm1'
  OC dlm1CredentialManagementSAPInstance
  MUST ( orderedCimKeys )
)

```

```

( <user-sr-12 NAME
'dlm1CredentialManagementSAPInstanceStructureRule1'
  Form dlm1CredentialManagementSAPInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to `dlm1CredentialManagementSAPInstance`.

```

( 1.3.6.1.4.1.412.100.4.1.1.40 NAME
'dlm1CredentialManagementSAPInstanceContentRule'
  DESC 'Aux classes that can attach to
        dlm1CredentialManagementSAPInstance.'
  AUX ( dlm1ServiceAccessBySAPAuxClass $
        dlm1ServiceSAPDependencyAuxClass $
        dlm1SAPSAPDependencyAuxClass $
        dlm1LogicalIdentityAuxClass $
        dlm1SynchronizedHelperAuxClass $
        dlm1ElementConfigurationAuxClass $
        dlm1ElementSettingAuxClass $
        dlm1DefaultSettingAuxClass $ dlm1DependencyAuxClass $
        dlm1ProvidesServiceToElementAuxClass $
        dlm1ElementAsUserAuxClass $
        dlm1AuthenticationTargetAuxClass $
        dlm1AuthorizationSubjectAuxClass $
        dlm1AuthorizationTargetAuxClass $
        dlm1CollectedMSEsAuxClass $ dlm1ComponentAuxClass $
        dlm1SystemComponentAuxClass $
        dlm1MemberOfCollectionAuxClass $
        dlm1MemberPrincipalHelperAuxClass )
)

```

3.14 AuthenticationRequirement Classes

This subclass of `LogicalElement` models the authentication requirements (captured in the associations from these entries) for access to system resources. As an example, the entries for the authentication service for a particular set of target resources may require that credentials be issued by specific entries of `CredentialManagementService`.

```

( 1.3.6.1.4.1.412.100.4.2.14 NAME 'dlmSecurityClassification'
  DESC 'The SecurityClassification property specifies a
        named level of security associated with the
        AuthenticationRequirement, e.g., "Confidential", "Top
        Secret", etc.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.41 NAME 'dlm1AuthenticationRequirement'
  DESC 'AuthenticationRequirement provides, through its
        associations, the authentication requirements for
        access to system resources. For a particular set of
        target resources, the AuthenticationService may
        require that credentials be issued by a specific
        CredentialManagementService. The
        AuthenticationRequirement class is weak to the system

```

```

        (e.g., Computer System or Administrative Domain) for
        which the requirements apply.'
    SUP dlmlLogicalElement ABSTRACT
    MAY ( dlmCreationClassName $ dlmName $
          dlmSecurityClassification )
)

( 1.3.6.1.4.1.412.100.4.1.1.42 NAME
'dlmlAuthenticationRequirementAuxClass'
  DESC 'AuthenticationRequirement provides, through its
        associations, the authentication requirements for
        access to system resources. For a particular set of
        target resources, the AuthenticationService may
        require that credentials be issued by a specific
        CredentialManagementService. The
        AuthenticationRequirement class is weak to the system
        (e.g., Computer System or Administrative Domain) for
        which the requirements apply.'
  SUP dlmlAuthenticationRequirement AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.43 NAME
'dlmlAuthenticationRequirementInstance'
  DESC 'AuthenticationRequirement provides, through its
        associations, the authentication requirements for
        access to system resources. For a particular set of
        target resources, the AuthenticationService may
        require that credentials be issued by a specific
        CredentialManagementService. The
        AuthenticationRequirement class is weak to the system
        (e.g., Computer System or Administrative Domain) for
        which the requirements apply.'
  SUP dlmlAuthenticationRequirement
)

( 1.3.6.1.4.1.412.100.4.3.1.13 NAME
'dlmlAuthenticationRequirementInstanceNameForm1'
  OC dlmlAuthenticationRequirementInstance
  MUST ( orderedCimKeys )
)

( <user-sr-13 NAME
'dlmlAuthenticationRequirementInstanceStructureRule1'
  Form dlmlAuthenticationRequirementInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to dlmlAuthenticationRequirementInstance.

```

( 1.3.6.1.4.1.412.100.4.1.1.43 NAME
'dlmlAuthenticationRequirementInstanceContentRule'
  DESC 'Aux classes that can attach to
        dlmlAuthenticationRequirementInstance.'
  AUX ( dlmlAuthenticateForUseAuxClass $
        dlmlRequireCredentialsFromAuxClass $
        dlmlAuthenticationTargetAuxClass $
        dlmlLogicalIdentityAuxClass $

```

```

    dlm1SynchronizedHelperAuxClass $
    dlm1ElementConfigurationAuxClass $
    dlm1ElementSettingAuxClass $
    dlm1DefaultSettingAuxClass $ dlm1DependencyAuxClass $
    dlm1ProvidesServiceToElementAuxClass $
    dlm1ElementAsUserAuxClass $
    dlm1AuthorizationSubjectAuxClass $
    dlm1AuthorizationTargetAuxClass $
    dlm1CollectedMSEsAuxClass $ dlm1ComponentAuxClass $
    dlm1SystemComponentAuxClass $
    dlm1MemberOfCollectionAuxClass $
    dlm1MemberPrincipalHelperAuxClass )
)

```

3.15 AccessControlInformation Classes

These subclasses of LogicalElement provide the specification of the access rights granted to a set of subject users to a set of target resources through its attributes and associations.

```

( 1.3.6.1.4.1.412.100.4.2.15 NAME 'dlmAccessQualifier'
  DESC 'The AccessQualifier property is an array of
        string values may be used to further qualify the type
        of access for which the corresponding permission
        applies. For example, it may be used to specify a set
        of parameters that are permitted or denied in
        conjunction with the corresponding AccessType entry
        point name.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.2.16 NAME 'dlmAccessType'
  DESC 'The AccessType property is an array of string
        values that specifies the type of access for which the
        corresponding permission applies. For example, it can
        be used to specify a generic access such as
        "Read-only", "Read/Write", etc. for file or record
        access control or it can be used to specify an entry
        point name for service access control.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.2.17 NAME 'dlmPermission'
  DESC 'The Permission property is an array of string
        values indicating the permission that applies to the
        corresponding AccessType and AccessQualifier array
        values. The values may be extended in subclasses to
        provide more specific access controls. Value Mappings
        are "Unknown", "Allow", "Deny", "Manage".'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.44 NAME 'dlm1AccessControlInformation'
  DESC 'AccessControlInformation provides, through its
        properties and its associations, the specification of

```

```

        the access rights granted to a set of subject users to
        a set of target resources. The AccessControlInformation
        class is weak to the system (e.g., Computer System or
        Administrative Domain) for which the access controls
        apply.'
    SUP dlm1LogicalElement ABSTRACT
    MAY ( dlmAccessQualifier $ dlmAccessType $
          dlmCreationClassName $ dlmName $ dlmPermission $
          dlmSecurityClassification )
)

( 1.3.6.1.4.1.412.100.4.1.1.45 NAME
'dlm1AccessControlInformationAuxClass'
  DESC 'AccessControlInformation provides, through its
        properties and its associations, the specification of
        the access rights granted to a set of subject users to
        a set of target resources. The AccessControlInformation
        class is weak to the system (e.g., Computer System or
        Administrative Domain) for which the access controls
        apply.'
  SUP dlm1AccessControlInformation AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.46 NAME
'dlm1AccessControlInformationInstance'
  DESC 'AccessControlInformation provides, through its
        properties and its associations, the specification of
        the access rights granted to a set of subject users to
        a set of target resources. The AccessControlInformation
        class is weak to the system (e.g., Computer System or
        Administrative Domain) for which the access controls
        apply.'
  SUP dlm1AccessControlInformation
)

( 1.3.6.1.4.1.412.100.4.3.1.14 NAME
'dlm1AccessControlInformationInstanceNameForm1'
  OC dlm1AccessControlInformationInstance
  MUST ( orderedCimKeys )
)

( <user-sr-14 NAME
'dlm1AccessControlInformationInstanceStructureRule1'
  Form dlm1AccessControlInformationInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to `dlm1AccessControlInformationInstance`.

```

( 1.3.6.1.4.1.412.100.4.1.1.46 NAME
'dlm1AccessControlInformationInstanceContentRule'
  DESC 'Aux classes that can attach to
        dlm1AccessControlInformationInstance.'
  AUX ( dlm1AuthorizedUseAuxClass $
        dlm1AuthorizationSubjectAuxClass $
        dlm1AuthorizationTargetAuxClass $
        dlm1LogicalIdentityAuxClass $

```



```

    dlm1SynchronizedHelperAuxClass $
    dlm1ElementConfigurationAuxClass $
    dlm1ElementSettingAuxClass $
    dlm1DefaultSettingAuxClass $ dlm1DependencyAuxClass $
    dlm1ProvidesServiceToElementAuxClass $
    dlm1ElementAsUserAuxClass $
    dlm1AuthenticationTargetAuxClass $
    dlm1CollectedMSEsAuxClass $ dlm1ComponentAuxClass $
    dlm1SystemComponentAuxClass $
    dlm1MemberOfCollectionAuxClass $
    dlm1MemberPrincipalHelperAuxClass )
)

```

3.16 OrganizationalEntity

This abstract subclass of ManagedElement provides a superclass for all classes that fit into an organizational structure.

```

( 1.3.6.1.4.1.412.100.4.1.1.47 NAME 'dlm1OrganizationalEntity'
  DESC 'OrganizationalEntity is an abstract class from
        which classes that fit into an organizational
        structure are derived.'
  SUP dlm1ManagedElement ABSTRACT
)

```

3.17 UserEntity

This abstract subclass of OrganizationalEntity models users.

```

( 1.3.6.1.4.1.412.100.4.1.1.48 NAME 'dlm1UserEntity'
  DESC 'UserEntity is an abstract class that represents
        users.'
  SUP dlm1OrganizationalEntity ABSTRACT
)

```

3.18 UsersAccess Classes

Entries of these subclasses of UserEntity model system users that are permitted access to system resources. The ElementAsUser classes are used to specify the ManagedElement entries (which may be people, services, service access points or collections thereof). This class differs from Account in that Account represents the user's relationship to a system from the perspective of the system's security services, this class represents the relationships independent of a particular system or service.

```

( 1.3.6.1.4.1.412.100.4.2.18 NAME 'dlmBiometric'
  DESC 'Biometric information used to identify a person.
        The property value is left null or set to "N/A" for
        non-human user or a user not using biometric
        information for authentication. Values are 0="N/A",
        1="Other", 2="Facial", 3="Retina", 4="Mark",
        5="Finger", 6="Voice", 7="DNA-RNA", 8="EEG".'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  EQUALITY integerMatch
)

( 1.3.6.1.4.1.412.100.4.2.19 NAME 'dlmElementID'

```

```

DESC 'The ElementID property uniquely specifies the
      ManagedElement object instance that is the user
      represented by the UsersAccess object instance. The
      ElementID is formatted similarly to a model path
      except that the property-value pairs are ordered in
      alphabetical order (US ASCII lexical order).'
```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
EQUALITY caseIgnoreMatch

)

(1.3.6.1.4.1.412.100.4.1.1.49 NAME 'dlm1UsersAccess'

```

DESC 'The UsersAccess object class is used to specify a
      system user that permitted access to system resources.
      The ManagedElement that has access to system resources
      (represented in the model in the ElementAsUser
      association) may be a person, a service, a service
      access point or any collection thereof. Whereas the
      Account class represents the user"s relationship to a
      system from the perspective of the security services
      of the system, the UserAccess class represents the
      relationships to the systems independent of a
      particular system or service.'
```

SUP dlm1UserEntity ABSTRACT
MAY (dlmBiometric \$ dlmCreationClassName \$
 dlmElementID \$ dlmName)

)

(1.3.6.1.4.1.412.100.4.1.1.50 NAME 'dlm1UsersAccessAuxClass'

```

DESC 'The UsersAccess object class is used to specify a
      system user that permitted access to system resources.
      The ManagedElement that has access to system resources
      (represented in the model in the ElementAsUser
      association) may be a person, a service, a service
      access point or any collection thereof. Whereas the
      Account class represents the user"s relationship to a
      system from the perspective of the security services
      of the system, the UserAccess class represents the
      relationships to the systems independent of a
      particular system or service.'
```

SUP dlm1UsersAccess AUXILIARY

)

(1.3.6.1.4.1.412.100.4.1.1.51 NAME 'dlm1UsersAccessInstance'

```

DESC 'The UsersAccess object class is used to specify a
      system user that permitted access to system resources.
      The ManagedElement that has access to system resources
      (represented in the model in the ElementAsUser
      association) may be a person, a service, a service
      access point or any collection thereof. Whereas the
      Account class represents the user"s relationship to a
      system from the perspective of the security services
      of the system, the UserAccess class represents the
      relationships to the systems independent of a
      particular system or service.'
```

SUP dlm1UsersAccess

)

```

( 1.3.6.1.4.1.412.100.4.3.1.15 NAME
'dlm1UsersAccessInstanceNameForm1'
  OC dlm1UsersAccessInstance
  MUST ( orderedCimKeys )
)

( <user-sr-15 NAME 'dlm1UsersAccessInstanceStructureRule1'
  Form dlm1UsersAccessInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to dlm1UsersAccessInstance.

```

( 1.3.6.1.4.1.412.100.4.1.1.51 NAME
'dlm1UsersAccessInstanceContentRule'
  DESC 'Aux classes that can attach to
  dlm1UsersAccessInstance.'
  AUX ( dlm1ElementAsUserAuxClass $
    dlm1UsersAccountAuxClass $ dlm1UsersCredentialAuxClass
    $ dlm1PublicPrivateKeyPairHelperAuxClass $
    dlm1NotaryVerifiesBiometricAuxClass $
    dlm1SystemAdministratorAuxClass $
    dlm1DependencyAuxClass $
    dlm1ProvidesServiceToElementAuxClass $
    dlm1AuthenticationTargetAuxClass $
    dlm1AuthorizationSubjectAuxClass $
    dlm1AuthorizationTargetAuxClass $
    dlm1OrgStructureAuxClass $
    dlm1CollectionInOrganizationAuxClass $
    dlm1MemberOfCollectionAuxClass $
    dlm1MemberPrincipalHelperAuxClass )
)

```

3.19 Credential

This abstract subclass of ManagedElement defines those materials, information or other data that are used to prove the identity of a UserAccess entry to a particular SecurityService. In general, this is shared information or material that is used to identify and authenticate in the process of accessing an Account. This material may be used both for initial identification or on an ongoing basis (for example, to prove that each message or communication came from the UserAccess entry associated with the credential).

```

( 1.3.6.1.4.1.412.100.4.1.1.52 NAME 'dlm1Credential'
  DESC 'Subclasses of Credential define materials,
  information, or other data which are used to prove the
  identity of a UsersAccess to a particular
  SecurityService. Generally, there may be some shared
  information, or credential material which is used to
  identify and authenticate ones self in the process of
  gaining access to, or permission to use, an Account.
  Such credential material may be used to authenticate a
  users access identity initially, as done by a
  AuthenticationService (see later), and additionally on
  an ongoing basis during the course of a connection or
  other security association, as proof that each

```

```

        received message or communication came from the owning
        user access of that credential material.'
    SUP dlmManagedElement ABSTRACT
)

```

3.20 PublicKeyCertificate Classes

These subclasses of Credential model public key certificates that a cryptographically signed by a trusted CertificateAuthority and issued to an authenticated entity (called the Subject in the certificate) which is represented by a UsersAccess entity. The public key in the certificate is cryptographically related to a private key held by the Subject. An example is the ITU/CCITT X.509 standard for public key certificates.

```

( 1.3.6.1.4.1.412.100.4.2.20 NAME 'dlmAltSubject'
  DESC 'Alternate subject identifier for the Certificate.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.2.21 NAME 'dlmPublicKey'
  DESC 'The DER-encoded raw public key.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.40
  EQUALITY octetStringMatch
)

( 1.3.6.1.4.1.412.100.4.2.22 NAME 'dlmSubject'
  DESC 'Certificate subject identifier.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.53 NAME 'dlmPublicKeyCertificate'
  DESC 'A Public Key Certificate is a credential that is
    cryptographically signed by a trusted Certificate
    Authority (CA) and issued to an authenticated entity
    (e.g., human user, service,etc.) called the Subject in
    the certificate and represented by the UsersAccess
    class. The public key in the certificate is
    cryptographically related to a private key that is to
    be held and kept private by the authenticated Subject.
    The certificate and its related private key can then
    be used for establishing trust relationships and
    securing communications with the Subject. Refer to
    the ITU/CCITT X.509 standard as an example of such
    certificates.'
  SUP dlmCredential ABSTRACT
  MAY ( dlmAltSubject $ dlmPublicKey $ dlmSubject )
)

( 1.3.6.1.4.1.412.100.4.1.1.54 NAME
'dlmPublicKeyCertificateAuxClass'
  DESC 'A Public Key Certificate is a credential that is
    cryptographically signed by a trusted Certificate
    Authority (CA) and issued to an authenticated entity
    (e.g., human user, service,etc.) called the Subject in
    the certificate and represented by the UsersAccess

```

```

class. The public key in the certificate is
cryptographically related to a private key that is to
be held and kept private by the authenticated Subject.
The certificate and its related private key can then
be used for establishing trust relationships and
securing communications with the Subject. Refer to
the ITU/CCITT X.509 standard as an example of such
certificates.'
SUP dlm1PublicKeyCertificate AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.55 NAME
'dlm1PublicKeyCertificateInstance'
DESC 'A Public Key Certificate is a credential that is
cryptographically signed by a trusted Certificate
Authority (CA) and issued to an authenticated entity
(e.g., human user, service, etc.) called the Subject in
the certificate and represented by the UsersAccess
class. The public key in the certificate is
cryptographically related to a private key that is to
be held and kept private by the authenticated Subject.
The certificate and its related private key can then
be used for establishing trust relationships and
securing communications with the Subject. Refer to
the ITU/CCITT X.509 standard as an example of such
certificates.'
SUP dlm1PublicKeyCertificate
)

( 1.3.6.1.4.1.412.100.4.3.1.16 NAME
'dlm1PublicKeyCertificateInstanceNameForm1'
OC dlm1PublicKeyCertificateInstance
MUST ( orderedCimKeys )
)

( <user-sr-16 NAME 'dlm1PublicKeyCertificateInstanceStructureRule1'
Form dlm1PublicKeyCertificateInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to `dlm1UsersAccessInstance`.

```

( 1.3.6.1.4.1.412.100.4.1.1.55 NAME
'dlm1PublicKeyCertificateInstanceContentRule'
DESC 'Aux classes that can attach to
dlm1PublicKeyCertificateInstance.'
AUX ( dlm1PublicPrivateKeyPairHelperAuxClass $
dlm1CAHasPublicCertificateAuxClass $
dlm1UsersCredentialAuxClass $
dlm1ManagedCredentialAuxClass $
dlm1DependencyAuxClass $
dlm1ProvidesServiceToElementAuxClass $
dlm1ElementAsUserAuxClass $
dlm1AuthenticationTargetAuxClass $
dlm1AuthorizationSubjectAuxClass $
dlm1AuthorizationTargetAuxClass $

```

```

        dlm1MemberOfCollectionAuxClass $
        dlm1MemberPrincipalHelperAuxClass )
)

```

3.21 UnsignedPublicKey Classes

These classes model an unsigned public key certificate that is accepted because of a direct trust relationship rather than via a CertificateAuthority.

```

( 1.3.6.1.4.1.412.100.4.2.23 NAME 'dlmPeerIdentity'
  DESC 'The Identity of the Peer with whom a direct trust
        relationship exists. The public key may be used for
        security functions with the Peer.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.2.24 NAME 'dlmPeerIdentityType'
  DESC 'PeerIdentityType is used to describe the type of
        the PeerIdentity. The currently defined values are
        used for IKE identities. Values are 0="Other",
        1="IPV4_ADDR", 2="FQDN", 3="USER_FQDN",
        4="IPV4_ADDR_SUBNET", 5="IPV6_ADDR",
        6="IPV6_ADDR_SUBNET", 7="IPV4_ADDR_RANGE",
        8="IPV6_ADDR_RANGE", 9="DER_ASN1_DN",
        10="DER_ASN1_GN", 11="KEY_ID".'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE
  EQUALITY integerMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.56 NAME 'dlm1UnsignedPublicKey'
  DESC 'A UnsignedPublicKey represents an unsigned public
        key credential. The local UsersAccess (or subclass
        thereof) accepts the public key as authentic because
        of a direct trust relationship rather than via a
        third-party Certificate Authority.'
  SUP dlm1Credential ABSTRACT
  MAY ( dlmPeerIdentity $ dlmPeerIdentityType $
        dlmPublicKey )
)

( 1.3.6.1.4.1.412.100.4.1.1.57 NAME 'dlm1UnsignedPublicKeyAuxClass'
  DESC 'A UnsignedPublicKey represents an unsigned public
        key credential. The local UsersAccess (or subclass
        thereof) accepts the public key as authentic because
        of a direct trust relationship rather than via a
        third-party Certificate Authority.'
  SUP dlm1UnsignedPublicKey AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.58 NAME 'dlm1UnsignedPublicKeyInstance'
  DESC 'A UnsignedPublicKey represents an unsigned public
        key credential. The local UsersAccess (or subclass
        thereof) accepts the public key as authentic because
        of a direct trust relationship rather than via a
        third-party Certificate Authority.'
  SUP dlm1UnsignedPublicKey
)

```

```

)

( 1.3.6.1.4.1.412.100.4.3.1.17 NAME
'dlm1UnsignedPublicKeyInstanceNameForm1'
  OC dlm1UnsignedPublicKeyInstance
  MUST ( orderedCimKeys )
)

( <user-sr-17 NAME 'dlm1UnsignedPublicKeyInstanceStructureRule1'
  Form dlm1UnsignedPublicKeyInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to `dlm1UnsignedPublicKeyInstance`.

```

( 1.3.6.1.4.1.412.100.4.1.1.58 NAME
'dlm1UnsignedPublicKeyInstanceContentRule'
  DESC 'Aux classes that can attach to
  dlm1UnsignedPublicKeyInstance.'
  AUX ( dlm1UsersCredentialAuxClass $
    dlm1ManagedCredentialAuxClass $ dlm1DependencyAuxClass
    $ dlm1ProvidesServiceToElementAuxClass $
    dlm1ElementAsUserAuxClass $
    dlm1AuthenticationTargetAuxClass $
    dlm1AuthorizationSubjectAuxClass $
    dlm1AuthorizationTargetAuxClass $
    dlm1MemberOfCollectionAuxClass $
    dlm1MemberPrincipalHelperAuxClass )
)

```

3.22 KerberosTicket Classes

These classes model the credentials issued by a particular Kerberos Key Distribution Center. The credentials are issued to a particular `UserAccess` entry as a result of successful authentication. This class is a superclass for the two types of ticket that a KDC may issue: a `TicketGranting` ticket, which is used to protect and authenticate communications between the `UserAccess` entry and the KDC, and a `Session` ticket which the KDC issues to two `UsersAccess` entries to allow them to communicate with each other.

```

( 1.3.6.1.4.1.412.100.4.2.25 NAME 'dlmAccessesService'
  DESC 'The name of the service for which this ticket is
  used.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.2.26 NAME 'dlmRemoteID'
  DESC 'RemoteID is the name by which the user is known
  at the KDC security service.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.2.27 NAME 'dlmTicketType'

```

```

DESC 'The Type of KerberosTicket is used to indicate
      whether the ticket in question was issued by the
      Kerberos Key Distribution Center (KDC) to support
      ongoing communication between the Users Access and the
      KDC ("TicketGranting\ Values are 0="Session",
      1="TicketGranting".'
```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE
EQUALITY integerMatch

)

(1.3.6.1.4.1.412.100.4.1.1.59 NAME 'dlm1KerberosTicket'

DESC 'A KerberosTicket represents a credential issued
by a particular Kerberos Key Distribution Center (KDC)
to a particular UsersAccess as the result of a
successful authentication process. There are two
types of tickets that a KDC may issue to a Users
Access - a TicketGranting ticket, which is used to
protect and authenticate communications between the
Users Access and the KDC, and a Session ticket, which
the KDC issues to two Users Access to allow them to
communicate with each other. '

SUP dlm1Credential ABSTRACT
MAY (dlmAccessesService \$ dlmRemoteID \$ dlmTicketType)

)

(1.3.6.1.4.1.412.100.4.1.1.60 NAME 'dlm1KerberosTicketAuxClass'

DESC 'A KerberosTicket represents a credential issued
by a particular Kerberos Key Distribution Center (KDC)
to a particular UsersAccess as the result of a
successful authentication process. There are two
types of tickets that a KDC may issue to a Users
Access - a TicketGranting ticket, which is used to
protect and authenticate communications between the
Users Access and the KDC, and a Session ticket, which
the KDC issues to two Users Access to allow them to
communicate with each other. '

SUP dlm1KerberosTicket AUXILIARY

)

(1.3.6.1.4.1.412.100.4.1.1.61 NAME 'dlm1KerberosTicketInstance'

DESC 'A KerberosTicket represents a credential issued
by a particular Kerberos Key Distribution Center (KDC)
to a particular UsersAccess as the result of a
successful authentication process. There are two
types of tickets that a KDC may issue to a Users
Access - a TicketGranting ticket, which is used to
protect and authenticate communications between the
Users Access and the KDC, and a Session ticket, which
the KDC issues to two Users Access to allow them to
communicate with each other. '

SUP dlm1KerberosTicket

)

(1.3.6.1.4.1.412.100.4.3.1.18 NAME
'dlm1KerberosTicketInstanceNameForm1'
OC dlm1KerberosTicketInstance
MUST (orderedCimKeys)


```

)
( <user-sr-18 NAME 'dlm1KerberosTicketInstanceStructureRule1'
  Form dlm1KerberosTicketInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to dlm1KerberosTicketInstance.

```

( 1.3.6.1.4.1.412.100.4.1.1.61 NAME
'dlm1KerberosTicketInstanceContentRule'
  DESC 'Aux classes that can attach to
        dlm1KerberosTicketInstance.'
  AUX ( dlm1UsersCredentialAuxClass $
        dlm1ManagedCredentialAuxClass $ dlm1DependencyAuxClass $
        $ dlm1ProvidesServiceToElementAuxClass $
        dlm1ElementAsUserAuxClass $
        dlm1AuthenticationTargetAuxClass $
        dlm1AuthorizationSubjectAuxClass $
        dlm1AuthorizationTargetAuxClass $
        dlm1MemberOfCollectionAuxClass $
        dlm1MemberPrincipalHelperAuxClass )
)

```

3.23 SharedSecret Classes

These classes model the shared secret between UserAccess entries and SharedSecret security service entries. Secrets may be in the form of a password used for initial authentication or as part of a message authentication code. It is important to note that these entries represent not just the password, but the password used with a particular security service.

```

( 1.3.6.1.4.1.412.100.4.2.28 NAME 'dlmAlgorithm'
  DESC 'algorithm names the transformation algorithm, if
        any, used to protect passwords before use in the
        protocol. For instance, Kerberos doesn't store
        passwords as the shared secret, but rather, a hash of
        the password.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)
( 1.3.6.1.4.1.412.100.4.2.29 NAME 'dlmProtocol'
  DESC 'protocol names the protocol with which the
        SharedSecret is used.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)
( 1.3.6.1.4.1.412.100.4.2.30 NAME 'dlmSecret'
  DESC 'secret is the secret known by the Users Access.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)
( 1.3.6.1.4.1.412.100.4.1.1.62 NAME 'dlm1SharedSecret'

```

```

DESC 'SharedSecret is the secret shared between a Users
Access and a particular SharedSecret security service.
Secrets may be in the form of a password used for
initial authentication, or as with a session key, used
as part of a message authentication code to verify that
a message originated by the pricipal with whom the
secret is shared. It is important to note that
SharedSecret is not just the password, but rather is
the password used with a particular security service.'
SUP dlm1Credential ABSTRACT
MAY ( dlmRemoteID $ dlmalgorithm $ dlmprotocol $
      dlmsecret )
)

( 1.3.6.1.4.1.412.100.4.1.1.63 NAME 'dlm1SharedSecretAuxClass'
DESC 'SharedSecret is the secret shared between a Users
Access and a particular SharedSecret security service.
Secrets may be in the form of a password used for
initial authentication, or as with a session key, used
as part of a message authentication code to verify that
a message originated by the pricipal with whom the
secret is shared. It is important to note that
SharedSecret is not just the password, but rather is
the password used with a particular security service.'
SUP dlm1SharedSecret AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.64 NAME 'dlm1SharedSecretInstance'
DESC 'SharedSecret is the secret shared between a Users
Access and a particular SharedSecret security service.
Secrets may be in the form of a password used for
initial authentication, or as with a session key, used
as part of a message authentication code to verify that
a message originated by the pricipal with whom the
secret is shared. It is important to note that
SharedSecret is not just the password, but rather is
the password used with a particular security service.'
SUP dlm1SharedSecret
)

( 1.3.6.1.4.1.412.100.4.3.1.19 NAME
'dlm1SharedSecretInstanceNameForm1'
OC dlm1SharedSecretInstance
MUST ( orderedCimKeys )
)

( <user-sr-19 NAME 'dlm1SharedSecretInstanceStructureRule1'
Form dlm1SharedSecretInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to `dlm1SharedSecretInstance`.

```

( 1.3.6.1.4.1.412.100.4.1.1.64 NAME
'dlm1SharedSecretInstanceContentRule'
DESC 'Aux classes that can attach to

```

```

        dlm1SharedSecretInstance.'
AUX ( dlm1UsersCredentialAuxClass $
      dlm1ManagedCredentialAuxClass $ dlm1DependencyAuxClass
      $ dlm1ProvidesServiceToElementAuxClass $
      dlm1ElementAsUserAuxClass $
      dlm1AuthenticationTargetAuxClass $
      dlm1AuthorizationSubjectAuxClass $
      dlm1AuthorizationTargetAuxClass $
      dlm1MemberOfCollectionAuxClass $
      dlm1MemberPrincipalHelperAuxClass )
)

```

3.24 NamedSharedIKESecret Classes

These classes indirectly model shared secret credentials. Attribute are used to store the secret and the name as used by a shared secret service to reference the secret.

```

( 1.3.6.1.4.1.412.100.4.2.31 NAME 'dlmLocalIdentity'
  DESC 'The local Identity with whom the direct trust
        relationship exists.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.2.32 NAME 'dlmLocalIdentityType'
  DESC 'LocalIdentityType is used to describe the type of
        the LocalIdentity. Values are 1="IPV4_ADDR", 2="FQDN",
        3="USER_FQDN", 4="IPV4_ADDR_SUBNET", 5="IPV6_ADDR",
        6="IPV6_ADDR_SUBNET", 7="IPV4_ADDR_RANGE",
        8="IPV6_ADDR_RANGE", 9="DER_ASN1_DN",
        10="DER_ASN1_GN", 11="KEY_ID".'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE
  EQUALITY integerMatch
)

( 1.3.6.1.4.1.412.100.4.2.33 NAME 'dlmSharedSecretName'
  DESC 'SharedSecretName is an indirect reference to a
        shared secret. The SecretService does not expose the
        actual secret but rather provides access to the secret
        via a name.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.65 NAME 'dlm1NamedSharedIKESecret'
  DESC 'NamedSharedIKESecret indirectly represents a
        shared secret credential. The local identity,
        IKEIdentity, and the remote peer identity share the
        secret that is named by the SharedSecretName. The
        SharedSecretName is used SharedSecretService to
        reference the secret.'
  SUP dlm1Credential ABSTRACT
  MAY ( dlmLocalIdentity $ dlmLocalIdentityType $
        dlmPeerIdentity $ dlmPeerIdentityType $
        dlmSharedSecretName )
)

```

```

( 1.3.6.1.4.1.412.100.4.1.1.66 NAME
'dlm1NamedSharedIKESecretAuxClass'
  DESC 'NamedSharedIKESecret indirectly represents a
        shared secret credential. The local identity,
        IKEIdentity, and the remote peer identity share the
        secret that is named by the SharedSecretName. The
        SharedSecretName is used SharedSecretService to
        reference the secret.'
  SUP dlm1NamedSharedIKESecret AUXILIARY
)

( 1.3.6.1.4.1.412.100.4.1.1.67 NAME
'dlm1NamedSharedIKESecretInstance'
  DESC 'NamedSharedIKESecret indirectly represents a
        shared secret credential. The local identity,
        IKEIdentity, and the remote peer identity share the
        secret that is named by the SharedSecretName. The
        SharedSecretName is used SharedSecretService to
        reference the secret.'
  SUP dlm1NamedSharedIKESecret
)

( 1.3.6.1.4.1.412.100.4.3.1.20 NAME
'dlm1NamedSharedIKESecretInstanceNameForm1'
  OC dlm1NamedSharedIKESecretInstance
  MUST ( orderedCimKeys )
)

( <user-sr-20 NAME 'dlm1NamedSharedIKESecretInstanceStructureRule1'
  Form dlm1NamedSharedIKESecretInstanceNameForm1
)

```

The following content rule specifies the auxiliary classes that may be attached to `dlm1NamedSharedIKESecretInstance`.

```

( 1.3.6.1.4.1.412.100.4.1.1.67 NAME
'dlm1NamedSharedIKESecretInstanceContentRule'
  DESC 'Aux classes that can attach to
        dlm1NamedSharedIKESecretInstance.'
  AUX ( dlm1UsersCredentialAuxClass $
        dlm1ManagedCredentialAuxClass $ dlm1DependencyAuxClass
        $ dlm1ProvidesServiceToElementAuxClass $
        dlm1ElementAsUserAuxClass $
        dlm1AuthenticationTargetAuxClass $
        dlm1AuthorizationSubjectAuxClass $
        dlm1AuthorizationTargetAuxClass $
        dlm1MemberOfCollectionAuxClass $
        dlm1MemberPrincipalHelperAuxClass )
)

```

3.25 ServiceUsesSecurityService Classes

These classes associate a Service entry with the SecurityService entry it uses.

```

( 1.3.6.1.4.1.412.100.4.1.1.68 NAME 'dlm1ServiceUsesSecurityService'
  DESC 'This relationship associates a Services with the
        Security Service it uses.'
)

```

```

    SUP dlm1ServiceServiceDependency ABSTRACT
  )

  ( 1.3.6.1.4.1.412.100.4.2.34 NAME
'dlmServiceUsesSecurityServiceAntecedentRef'
  DESC ' The value of this attribute points to an entry of class
        dlm1SecurityService.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
  EQUALITY distinguishedNameMatch
  )

  ( 1.3.6.1.4.1.412.100.4.2.35 NAME
'dlmServiceUsesSecurityServiceDependentRef'
  DESC ' The value of this attribute points to an entry of class
        dlm1Service.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
  EQUALITY distinguishedNameMatch
  )

  ( 1.3.6.1.4.1.412.100.4.1.1.69 NAME
'dlm1ServiceUsesSecurityServiceInstance'
  DESC 'This relationship associates a Services with the
        Security Service it uses.'
  SUP dlm1ServiceUsesSecurityService
  MAY ( dlmServiceUsesSecurityServiceAntecedentRef $
        dlmServiceUsesSecurityServiceDependentRef )
  )

  ( 1.3.6.1.4.1.412.100.4.3.1.21 NAME
'dlm1ServiceUsesSecurityServiceInstanceNameForm1'
  OC dlm1ServiceUsesSecurityServiceInstance
  MUST ( orderedCimKeys )
  )

  ( <user-sr-21 NAME
'dlm1ServiceUsesSecurityServiceInstanceStructureRule1'
  Form dlm1ServiceUsesSecurityServiceInstanceNameForm1
  )

  ( 1.3.6.1.4.1.412.100.4.2.36 NAME
'dlmServiceUsesSecurityServiceHelperRef'
  DESC 'Pointer to ServiceUsesSecurityServiceInstance.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
  )

  ( 1.3.6.1.4.1.412.100.4.1.1.70 NAME
'dlm1ServiceUsesSecurityServiceHelperAuxClass'
  DESC 'Helper class for finding
        ServiceUsesSecurityService.'
  SUP top AUXILIARY
  MAY ( dlmServiceUsesSecurityServiceHelperRef )
  )

```

3.26 SecurityServiceForSystem Classes

These classes associate a System entry and the SecurityService entry that provides the services for that System entry.

```
( 1.3.6.1.4.1.412.100.4.1.1.71 NAME 'dlm1SecurityServiceForSystem'
  DESC 'The SecurityServiceForSystem provides the
        association between a System and a SecurityService
        that provides services for that system.'
  SUP dlm1ProvidesServiceToElement ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.37 NAME
'dlmSecurityServiceForSystemAntecedentRef'
  DESC 'The SecurityService that provides services for
        the system. Values of this attribute point to entries of
        class dlm1SecurityService.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
  EQUALITY distinguishedNameMatch
)

(1.3.6.1.4.1.412.100.4.2.38 NAME
'dlmSecurityServiceForSystemDependentRef'
  DESC 'The system that is dependent on the security
        service. Values of this attribute point to entries
        of class dlm1System.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.72 NAME
'dlm1SecurityServiceForSystemAuxClass'
  DESC 'The SecurityServiceForSystem provides the
        association between a System and a SecurityService
        that provides services for that system.'
  SUP dlm1SecurityServiceForSystem AUXILIARY
  MAY ( dlmSecurityServiceForSystemAntecedentRef $
        dlmSecurityServiceForSystemDependentRef )
)
```

3.27 ManagesAccountOnSystem Classes

These classes associate a System entry with the AccountManagementService entry that manages accounts for that system.

```
( 1.3.6.1.4.1.412.100.4.1.1.73 NAME 'dlm1ManagesAccountOnSystem'
  DESC 'The ManagesAccountOnSystem provides the
        association between a System and the
        AccountManagementService that manages accounts for
        that system.'
  SUP dlm1SecurityServiceForSystem ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.39 NAME
'dlmManagesAccountOnSystemAntecedentRef'
  DESC 'An AccountManagementService that manages accounts
```

```

        for the system. Values of this attribute point to
        entries of class dlmlAccountManagementService.'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
    EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.40 NAME
'dlmManagesAccountOnSystemDependentRef'
  DESC 'The system that is dependent on the
        AccountManagementService. Values of this attribute
        Point to entry(s) of class dlmlSystem.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.74 NAME
'dlmlManagesAccountOnSystemAuxClass'
  DESC 'The ManagesAccountOnSystem provides the
        association between a System and the
        AccountManagementService that manages accounts for
        that system.'
  SUP dlmlManagesAccountOnSystem AUXILIARY
  MAY ( dlmlManagesAccountOnSystemAntecedentRef $
        dlmlManagesAccountOnSystemDependentRef )
)

```

3.28 ElementAsUser Classes

These classes associate a ManagedElement entry with the UsersAccess entry to a particular system. Typically the ManagedElement entry is a Collection, Person, Service or ServiceAccessPoint. Other ManagedElement entries would have Services that have the association to a UsersAccess entry.

```

( 1.3.6.1.4.1.412.100.4.1.1.75 NAME 'dlmlElementAsUser'
  DESC 'ElementAsUser is an association used to establish
        the "ownership" of UsersAccess object instances. That
        is, the ManagedElement may have UsersAccess to systems
        and, therefore, be "users" on those systems.
        UsersAccess instances must have an "owning"
        ManagedElement. Typically, the ManagedElements will
        be limited to Collection, Person, Service and
        ServiceAccessPoint. Other non-human ManagedElements
        that might be thought of as having UsersAccess (e.g.,
        a device or system) have services that have the
        UsersAccess.'
  SUP dlmlDependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.41 NAME 'dlmElementAsUserAntecedentRef'
  DESC 'The ManagedElement that has UsersAccess. The value
        of this attribute points to an entry of class
        dlmlManagedElement.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
  EQUALITY distinguishedNameMatch
)

```

```

( 1.3.6.1.4.1.412.100.4.2.42 NAME 'dlmElementAsUserDependentRef'
  DESC 'The "owned" UsersAccess. Values of this
        attribute point to entries of class dlm1UsersAccess.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.76 NAME 'dlm1ElementAsUserAuxClass'
  DESC 'ElementAsUser is an association used to establish
        the "ownership" of UsersAccess object instances. That
        is, the ManagedElement may have UsersAccess to systems
        and, therefore, be "users" on those systems.
        UsersAccess instances must have an "owning"
        ManagedElement. Typically, the ManagedElements will
        be limited to Collection, Person, Service and
        ServiceAccessPoint. Other non-human ManagedElements
        that might be thought of as having UsersAccess (e.g.,
        a device or system) have services that have the
        UsersAccess.'
  SUP dlm1ElementAsUser AUXILIARY
  MAY ( dlmElementAsUserAntecedentRef $
        dlmElementAsUserDependentRef )
)

```

3.29 SystemAdministrator Classes

These classes identify a particular UserEntity entry as a system administrator of a particular System entry.

```

( 1.3.6.1.4.1.412.100.4.1.1.77 NAME 'dlm1SystemAdministrator'
  DESC 'SystemAdministrator is an association used to
        identify the UserEntity as a system administrator of a
        System.'
  SUP dlm1Dependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.43 NAME
'dlmSystemAdministratorAntecedentRef'
  DESC 'The administered system. Values of this
        attribute points to entries of class dlm1System.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.44 NAME
'dlmSystemAdministratorDependentRef'
  DESC 'The UserEntity that provides the administrative
        function for the associated system. Values of this
        attribute points to entries of class dlm1UserEntity.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.78 NAME 'dlm1SystemAdministratorAuxClass'
  DESC 'SystemAdministrator is an association used to
        identify the UserEntity as a system administrator of a
        System.'
)

```



```

SUP dlm1SystemAdministrator AUXILIARY
MAY ( dlmSystemAdministratorAntecedentRef $
      dlmSystemAdministratorDependentRef )
)

```

3.30 SystemAdministratorGroup Classes

These classes identify a Group entry that has system administrator privileges for a System entry.

```

( 1.3.6.1.4.1.412.100.4.1.1.79 NAME 'dlm1SystemAdministratorGroup'
  DESC 'SystemAdministratorGroup is an association used
        to identify a Group that has system administrator
        responsibilities for a System. '
  SUP dlm1Dependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.45 NAME
'dlmSystemAdministratorGroupAntecedentRef'
  DESC 'The administered system. Values of this
        attribute point to entries of class dlm1System.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.46 NAME
'dlmSystemAdministratorGroupDependentRef'
  DESC 'The Group of administrators. Values of this
        attribute point to entries of class groupOfNames.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.80 NAME
'dlm1SystemAdministratorGroupAuxClass'
  DESC 'SystemAdministratorGroup is an association used
        to identify a Group that has system administrator
        responsibilities for a System. '
  SUP dlm1SystemAdministratorGroup AUXILIARY
  MAY ( dlmSystemAdministratorGroupAntecedentRef $
        dlmSystemAdministratorGroupDependentRef )
)

```

3.31 SystemAdministratorRole Classes

These classes identify the system administrator Role entry with a particular System entry.

```

( 1.3.6.1.4.1.412.100.4.1.1.81 NAME 'dlm1SystemAdministratorRole'
  DESC 'SystemAdministratorRole is an association used to
        identify a system administrator Role for a System.'
  SUP dlm1Dependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.47 NAME
'dlmSystemAdministratorRoleAntecedentRef'
  DESC 'The administered system. Values of this
        attribute point to entries of class dlm1System.'
)

```

```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.48 NAME
'dlmSystemAdministratorRoleDependentRef'
DESC 'The system administration role. Values of this
attribute point to entries of class
organizationalRole.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.82 NAME
'dlmlSystemAdministratorRoleAuxClass'
DESC 'SystemAdministratorRole is an association used to
identify a system administrator Role for a System.'
SUP dlmlSystemAdministratorRole AUXILIARY
MAY ( dlmSystemAdministratorRoleAntecedentRef $
dlmSystemAdministratorRoleDependentRef )
)

```

3.32 UserAccount Classes

These classes associated UsersAccess entries with the Account entries that can interact with.

```

( 1.3.6.1.4.1.412.100.4.1.1.83 NAME 'dlmlUsersAccount'
DESC 'This relationship associates UsersAccess with the
Accounts with which they"re able to interact.'
SUP dlmlDependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.49 NAME 'dlmUsersAccountAntecedentRef'
DESC 'The user"s Account. Values of this attribute
Point to entries of class account.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.50 NAME 'dlmUsersAccountDependentRef'
DESC 'The User as identified by their UsersAccess
instance. Values of this attribute point to
entries of class dlmlUsersAccess.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.84 NAME 'dlmlUsersAccountAuxClass'
DESC 'This relationship associates UsersAccess with the
Accounts with which they"re able to interact.'
SUP dlmlUsersAccount AUXILIARY
MAY ( dlmUsersAccountAntecedentRef $
dlmUsersAccountDependentRef )
)

```

3.33 SecurityServiceUsesAccount Classes

The classes associate SecurityService entries with the Account entries they use.

```
( 1.3.6.1.4.1.412.100.4.1.1.85 NAME 'dlm1SecurityServiceUsesAccount'  
  DESC 'This relationship associates SecurityService  
        instances to the Accounts they use in the course of  
        their work.'  
  SUP dlm1Dependency ABSTRACT  
)  
  
( 1.3.6.1.4.1.412.100.4.2.51 NAME  
'dlmSecurityServiceUsesAccountAntecedentRef'  
  DESC ' Values of this attribute point to entries of  
        class account.'  
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12  
  EQUALITY distinguishedNameMatch  
)  
  
( 1.3.6.1.4.1.412.100.4.2.52 NAME  
'dlmSecurityServiceUsesAccountDependentRef'  
  DESC ' Values of this attribute point to entries of  
        class dlm1SecurityService.'  
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12  
  EQUALITY distinguishedNameMatch  
)  
  
( 1.3.6.1.4.1.412.100.4.1.1.86 NAME  
'dlm1SecurityServiceUsesAccountAuxClass'  
  DESC 'This relationship associates SecurityService  
        instances to the Accounts they use in the course of  
        their work.'  
  SUP dlm1SecurityServiceUsesAccount AUXILIARY  
  MAY ( dlmSecurityServiceUsesAccountAntecedentRef $  
        dlmSecurityServiceUsesAccountDependentRef )  
)
```

3.34 ManagesAccount Classes

These classes associate AccountManagement entries to the Account entries they are responsible for.

```
( 1.3.6.1.4.1.412.100.4.1.1.87 NAME 'dlm1ManagesAccount'  
  DESC 'This relationship associates the  
        AccountManagement security service to the Accounts for  
        which it is responsible.'  
  SUP dlm1Dependency ABSTRACT  
)  
  
( 1.3.6.1.4.1.412.100.4.2.53 NAME 'dlmManagesAccountAntecedentRef'  
  DESC ' Values of this attribute point to entries of  
        class dlm1AccountManagementService.'  
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12  
  EQUALITY distinguishedNameMatch  
)
```

```

( 1.3.6.1.4.1.412.100.4.2.54 NAME 'dlmManagesAccountDependentRef'
  DESC ' Values of this attribute point to entries of
        class account.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.88 NAME 'dlm1ManagesAccountAuxClass'
  DESC 'This relationship associates the
        AccountManagement security service to the Accounts for
        which it is responsible.'
  SUP dlm1ManagesAccount AUXILIARY
  MAY ( dlmManagesAccountAntecedentRef $
        dlmManagesAccountDependentRef )
)

```

3.35 TrustHierarchy Classes

These classes model the trust hierarchy between two CredentialManagementService entries.

```

( 1.3.6.1.4.1.412.100.4.1.1.89 NAME 'dlm1TrustHierarchy'
  DESC 'TrustHierarchy is an association between two
        CredentialManagementService instances that establishes
        the trust hierarchy between them.'
  SUP dlm1Dependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.55 NAME 'dlmTrustHierarchyAntecedentRef'
  DESC 'The superior CredentialManagementService from
        which the dependent service gets its authority.
        The value of this attribute points to an entry of class
        dlm1CredentialManagementService.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.56 NAME 'dlmTrustHierarchyDependentRef'
  DESC 'The subordinate CredentialManagementService.
        Value of this attribute point to entries of class
        dlm1CredentialManagementService.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.90 NAME 'dlm1TrustHierarchyAuxClass'
  DESC 'TrustHierarchy is an association between two
        CredentialManagementService instances that establishes
        the trust hierarchy between them.'
  SUP dlm1TrustHierarchy AUXILIARY
  MAY ( dlmTrustHierarchyAntecedentRef $
        dlmTrustHierarchyDependentRef )
)

```

3.36 UsersCredential Classes

These classes establish the credentials that may be used by a UserAccess entry to access a system or set of systems.

```
( 1.3.6.1.4.1.412.100.4.1.1.91 NAME 'dlm1UsersCredential'
  DESC 'UsersCredential is an association used to
        establish the credentials that may be used for a
        UsersAccess to a system or set of systems. '
  SUP dlm1Dependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.57 NAME 'dlmUsersCredentialAntecedentRef'
  DESC 'The issued credential that may be used. Values
        of this attribute point to entries of class
        dlm1Credential.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.58 NAME 'dlmUsersCredentialDependentRef'
  DESC 'The UsersAccess that has use of a credential.
        Values of this attribute point to entries of class
        dlm1UsersAccess.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.92 NAME 'dlm1UsersCredentialAuxClass'
  DESC 'UsersCredential is an association used to
        establish the credentials that may be used for a
        UsersAccess to a system or set of systems. '
  SUP dlm1UsersCredential AUXILIARY
  MAY ( dlmUsersCredentialAntecedentRef $
        dlmUsersCredentialDependentRef )
)
```

3.37 PublicKeyKeyPair Classes

These classes associate a PublicKeyCertificate entry with a public key with the Principal entry that holds the private key used with the public key. For security reasons, the private key is not modeled. It could be accessible via key recovery services, which are considered outside the scope of this mapping.

```
( 1.3.6.1.4.1.412.100.4.2.59 NAME 'dlmRepository'
  DESC 'The repository in which the certificate is backed
        up.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
  EQUALITY caseIgnoreMatch
)

( 1.3.6.1.4.1.412.100.4.2.60 NAME 'dlmUse'
  DESC 'The Certificate may be used for signature only or
        for confidentiality as well as signature Values are
        0="SignOnly", 1="ConfidentialityOrSignature".'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE
)
```

```

EQUALITY integerMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.93 NAME 'dlm1PublicPrivateKeyPair'
DESC 'This relationship associates a
    PublicKeyCertificate with the Principal who has the
    PrivateKey used with the PublicKey. The PrivateKey is
    not modeled, since it is not a data element that ever
    SHOULD be accessible via management applications,
    other than key recovery services, which are outside
    our scope.'
SUP dlm1UsersCredential ABSTRACT
MAY ( dlmRepository $ dlmUse )
)

( 1.3.6.1.4.1.412.100.4.2.61 NAME
'dlmPublicPrivateKeyPairAntecedentRef'
DESC 'The value of this attribute points to an entry of
    class dlm1PublicKeyCertificate.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.62 NAME
'dlmPublicPrivateKeyPairDependentRef'
DESC 'The value of this attribute points to an entry of
    class dlm1UsersAccess.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.94 NAME
'dlm1PublicPrivateKeyPairInstance'
DESC 'This relationship associates a
    PublicKeyCertificate with the Principal who has the
    PrivateKey used with the PublicKey. The PrivateKey is
    not modeled, since it is not a data element that ever
    SHOULD be accessible via management applications,
    other than key recovery services, which are outside
    our scope.'
SUP dlm1PublicPrivateKeyPair
MAY ( dlmPublicPrivateKeyPairAntecedentRef $
    dlmPublicPrivateKeyPairDependentRef )
)

( 1.3.6.1.4.1.412.100.4.3.1.22 NAME
'dlm1PublicPrivateKeyPairInstanceNameForm1'
OC dlm1PublicPrivateKeyPairInstance
MUST ( orderedCimKeys )
)

( <user-sr-22 NAME 'dlm1PublicPrivateKeyPairInstanceStructureRule1'
Form dlm1PublicPrivateKeyPairInstanceNameForm1
)

( 1.3.6.1.4.1.412.100.4.2.63 NAME 'dlmPublicPrivateKeyPairHelperRef'
DESC 'Pointer to PublicPrivateKeyPairInstance.'

```

```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.95 NAME
'dlm1PublicPrivateKeyPairHelperAuxClass'
DESC 'Helper class for finding PublicPrivateKeyPair.'
SUP top AUXILIARY
MAY ( dlm1PublicPrivateKeyPairHelperRef )
)

```

3.38 CAHasPublicCertificate Classes

These classes associates a CertificateAuthority entry with certificates that have been issued by other Cas. As such, it is an optimization of the CA having a UsersAccess entry that is associated to a certificate to capture the LDAP-based CA implementations.

```

( 1.3.6.1.4.1.412.100.4.1.1.96 NAME 'dlm1CAHasPublicCertificate'
DESC 'A CertificateAuthority may have certificates
issued by other CAs. This association is essentially
an optimization of the CA having a UsersAccess
instance with an association to a certificate thus
mapping more closely to LDAP-based certificate
authority implementations.'
SUP dlm1Dependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.64 NAME
'dlmCAHasPublicCertificateAntecedentRef'
DESC 'The Certificate used by the CA. The value of this
attribute points to an entry of class
dlm1PublicKeyCertificate.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.65 NAME
'dlmCAHasPublicCertificateDependentRef'
DESC 'The CA that uses a Certificate. Values of this
attribute point to entries of class
dlm1CertificateAuthority.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.97 NAME
'dlm1CAHasPublicCertificateAuxClass'
DESC 'A CertificateAuthority may have certificates
issued by other CAs. This association is essentially
an optimization of the CA having a UsersAccess
instance with an association to a certificate thus
mapping more closely to LDAP-based certificate
authority implementations.'
SUP dlm1CAHasPublicCertificate AUXILIARY
MAY ( dlmCAHasPublicCertificateAntecedentRef $
dlmCAHasPublicCertificateDependentRef )
)

```

3.39 ManagedCredential Classes

These classes associate a CredentialManagementService entry with the Credential entries it manages.

```
( 1.3.6.1.4.1.412.100.4.1.1.98 NAME 'dlmManagedCredential'
  DESC 'This relationship associates a
        CredentialManagementService with the Credential it
        manages.'
  SUP dlmDependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.66 NAME 'dlmManagedCredentialAntecedentRef'
  DESC 'The credential management service. The value of
        this attribute points to an entry of class
        dlmCredentialManagementService.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.67 NAME 'dlmManagedCredentialDependentRef'
  DESC 'The managed credential. The values of this
        attribute point to entries of class dlmCredential.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.99 NAME 'dlmManagedCredentialAuxClass'
  DESC 'This relationship associates a
        CredentialManagementService with the Credential it
        manages.'
  SUP dlmManagedCredential AUXILIARY
  MAY ( dlmManagedCredentialAntecedentRef $
        dlmManagedCredentialDependentRef )
)
```

3.40 CASignsPublicKeyCertificate Classes

These classes associated a CertificateAuthority entry with the certificates that it signs.

```
( 1.3.6.1.4.1.412.100.4.2.68 NAME 'dlmSignature'
  DESC ''
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  EQUALITY integerMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.100 NAME
'dlmCASignsPublicKeyCertificate'
  DESC 'This relationship associates a
        CertificateAuthority with the certificates it signs.'
  SUP dlmManagedCredential ABSTRACT
  MAY ( dlmSignature )
)

( 1.3.6.1.4.1.412.100.4.2.69 NAME
'dlmCASignsPublicKeyCertificateAntecedentRef'
```



```

DESC 'The CA which signed the certificate. The value of
      this attribute points to an entry of class
      dlm1CertificateAuthority.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.70 NAME
'dlmCASignsPublicKeyCertificateDependentRef'
DESC 'The certificate issued by the CA. Values of
      this attribute point to entries of class
      dlm1PublicKeyCertificate.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.101 NAME
'dlm1CASignsPublicKeyCertificateAuxClass'
DESC 'This relationship associates a
      CertificateAuthority with the certificates it signs.'
SUP dlm1CASignsPublicKeyCertificate AUXILIARY
MAY ( dlmCASignsPublicKeyCertificateAntecedentRef $
      dlmCASignsPublicKeyCertificateDependentRef )
)

```

3.41 LocallyManagedPublicKey Classes

These classes model the relationship between a `PublicKeyManagementService` entry and an `UnsignedPublicKey` entry.

```

( 1.3.6.1.4.1.412.100.4.1.1.102 NAME 'dlm1LocallyManagedPublicKey'
DESC 'LocallyManagedPublicKey association provides the
      relationship between a PublicKeyManagementService and
      an UnsignedPublicKey.'
SUP dlm1ManagedCredential ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.71 NAME
'dlmLocallyManagedPublicKeyAntecedentRef'
DESC 'The PublicKeyManagementService that manages an
      unsigned public key. The value of this attribute points
      to an entry of class dlm1PublicKeyManagementService.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.72 NAME
'dlmLocallyManagedPublicKeyDependentRef'
DESC 'An unsigned public key. Values of this
      attribute point to entries of class
      dlm1UnsignedPublicKey.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.103 NAME
'dlm1LocallyManagedPublicKeyAuxClass'

```

```

DESC 'LocallyManagedPublicKey association provides the
      relationship between a PublicKeyManagementService and
      an UnsignedPublicKey.'
SUP dlm1LocallyManagedPublicKey AUXILIARY
MAY ( dlmLocallyManagedPublicKeyAntecedentRef $
      dlmLocallyManagedPublicKeyDependentRef )
)

```

3.42 SharedSecretIsShared Classes

These classes associate a SharedSecretService entry with the SecretKey entry it verifies.

```

( ( 1.3.6.1.4.1.412.100.4.1.1.104 NAME 'dlm1SharedSecretIsShared'
  DESC 'This relationship associates a
        SharedSecretService with the SecretKey it verifies.'
  SUP dlm1ManagedCredential ABSTRACT
)
)

```

```

( 1.3.6.1.4.1.412.100.4.2.73 NAME
'dlmSharedSecretIsSharedAntecedentRef'
  DESC 'The credential management service. The value of
        this attribute points to an entry of class
        dlm1SharedSecretService.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
  EQUALITY distinguishedNameMatch
)

```

```

( 1.3.6.1.4.1.412.100.4.2.74 NAME
'dlmSharedSecretIsSharedDependentRef'
  DESC 'The managed credential. Values of this
        attribute point to entries of class dlm1SharedSecret.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

```

```

( 1.3.6.1.4.1.412.100.4.1.1.105 NAME
'dlm1SharedSecretIsSharedAuxClass'
  DESC 'This relationship associates a
        SharedSecretService with the SecretKey it verifies.'
  SUP dlm1SharedSecretIsShared AUXILIARY
  MAY ( dlmSharedSecretIsSharedAntecedentRef $
        dlmSharedSecretIsSharedDependentRef )
)

```

3.43 IKESecretIsNamed Classes

These classes model the relationship between a SharedSecretService entry and a NamedSharedIKESecret entry.

```

( 1.3.6.1.4.1.412.100.4.1.1.106 NAME 'dlm1IKESecretIsNamed'
  DESC 'IKESecretIsNamed association provides the
        relationship between a SharedSecretService and a
        NamedSharedIKESecret.'
  SUP dlm1ManagedCredential ABSTRACT
)

```

```

( 1.3.6.1.4.1.412.100.4.2.75 NAME 'dlmIKESecretIsNamedAntecedentRef'
)

```

```

DESC 'The SharedSecretService that manages a
      NamedSharedIKESecret. The value of this attribute
      points to an entry of class dlm1SharedSecretService.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.76 NAME 'dlmIKESecretIsNamedDependentRef'
DESC 'The managed NamedSharedIKESecret. Values of
      this attribute point to entries of class
      dlm1NamedSharedIKESecret.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.107 NAME 'dlmIKESecretIsNamedAuxClass'
DESC 'IKESecretIsNamed association provides the
      relationship between a SharedSecretService and a
      NamedSharedIKESecret.'
SUP dlmIKESecretIsNamed AUXILIARY
MAY ( dlmIKESecretIsNamedAntecedentRef $
      dlmIKESecretIsNamedDependentRef )
)

```

3.44 KDCIssuesKerberosTicket Classes

These classes model the relationship between a KDC entry and the Kerberos tickets it issues.

```

( 1.3.6.1.4.1.412.100.4.1.1.108 NAME 'dlm1KDCIssuesKerberosTicket'
DESC 'The KDC issues and owns Kerberos tickets. This
      association captures the relationship between the KDC
      and its issued tickets.'
SUP dlm1ManagedCredential ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.77 NAME
'dlmKDCIssuesKerberosTicketAntecedentRef'
DESC 'The issuing KDC. The value of this attribute
      points to an entry of class
      dlm1KerberosKeyDistributionCenter.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.78 NAME
'dlmKDCIssuesKerberosTicketDependentRef'
DESC 'The managed credential. The values of this
      attribute point to entries of class
      dlm1KerberosTicket.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.109 NAME
'dlm1KDCIssuesKerberosTicketAuxClass'
DESC 'The KDC issues and owns Kerberos tickets. This

```

```

        association captures the relationship between the KDC
        and its issued tickets.'
    SUP dlm1KDCIssuesKerberosTicket AUXILIARY
    MAY ( dlmKDCIssuesKerberosTicketAntecedentRef $
        dlmKDCIssuesKerberosTicketDependentRef )
)

```

3.45 NotaryVerifiesBiometric Classes

These classes show the relationship between a Notary entry and the UserAccess entry whose biometric information is verified.

```

( 1.3.6.1.4.1.412.100.4.1.1.110 NAME 'dlm1NotaryVerifiesBiometric'
  DESC 'This relationship associates a Notary service
        with the Users Access whose biometric information is
        verified.'
  SUP dlm1Dependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.79 NAME
'dlmNotaryVerifiesBiometricAntecedentRef'
  DESC 'The Notary service that verifies biometric
        information . Values of this attribute point to
        entries of class dlm1Notary.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.80 NAME
'dlmNotaryVerifiesBiometricDependentRef'
  DESC 'The UsersAccess that represents a person using
        biometric information for authentication. Values of
        this attribute point to entries of class
        dlm1UsersAccess.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.111 NAME
'dlm1NotaryVerifiesBiometricAuxClass'
  DESC 'This relationship associates a Notary service
        with the Users Access whose biometric information is
        verified.'
  SUP dlm1NotaryVerifiesBiometric AUXILIARY
  MAY ( dlmNotaryVerifiesBiometricAntecedentRef $
        dlmNotaryVerifiesBiometricDependentRef )
)

```

3.46 HostedAuthenticationRequirement Classes

These classes provide the namespace scoping for AuthenticationRequirement entries.

```

( 1.3.6.1.4.1.412.100.4.1.1.112 NAME
'dlm1HostedAuthenticationRequirement'
  DESC 'HostedAuthenticationRequirement is an association
        used to provide the namespace scoping of
        AuthenticationRequirement. The hosted requirements

```

```

        may or may not apply to resources on the hosting
        system.'
    SUP dlm1Dependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.81 NAME
'dlmHostedAuthenticationRequirementAntecedentRef'
  DESC 'The hosting system. The value of this attribute
        points to an entry of class dlm1System.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.82 NAME
'dlmHostedAuthenticationRequirementDependentRef'
  DESC 'The hosted AuthenticationRequirement. Values of
        this attribute points to entries of class
        dlm1AuthenticationRequirement.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.113 NAME
'dlm1HostedAuthenticationRequirementAuxClass'
  DESC 'HostedAuthenticationRequirement is an association
        used to provide the namespace scoping of
        AuthenticationRequirement. The hosted requirements
        may or may not apply to resources on the hosting
        system.'
  SUP dlm1HostedAuthenticationRequirement AUXILIARY
  MAY ( dlmHostedAuthenticationRequirementAntecedentRef $
        dlmHostedAuthenticationRequirementDependentRef )
)

```

3.47 AuthenticateForUse Classes

These classes model the relationship between an AuthenticationService entry and the AuthenticationRequirement entry it requires to function.

```

( 1.3.6.1.4.1.412.100.4.1.1.114 NAME 'dlm1AuthenticateForUse'
  DESC 'AuthenticateForUse is an association used to
        provide an AuthenticationService with the
        AuthenticationRequirement it needs to do its job.'
  SUP dlm1Dependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.83 NAME
'dlmAuthenticateForUseAntecedentRef'
  DESC 'AuthenticationRequirement for use. Values of
        this attribute point to entries of class
        dlm1AuthenticationRequirement.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.84 NAME 'dlmAuthenticateForUseDependentRef'
  DESC 'AuthenticationService that uses the requirements.

```

```

        Values of this attribute point to entries of class
        dlmlAuthenticationService.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.115 NAME 'dlmlAuthenticateForUseAuxClass'
  DESC 'AuthenticateForUse is an association used to
        provide an AuthenticationService with the
        AuthenticationRequirement it needs to do its job.'
  SUP dlmlAuthenticateForUse AUXILIARY
  MAY ( dlmlAuthenticateForUseAntecedentRef $
        dlmlAuthenticateForUseDependentRef )
)

```

3.48 RequireCredentialsFrom Classes

These classes model the requirement of a user having credentials from a particular CredentialManagementService entry.

```

( 1.3.6.1.4.1.412.100.4.1.1.116 NAME 'dlmlRequireCredentialsFrom'
  DESC 'RequireCredentialsFrom is an association used to
        require that credentials are issued by particular
        Credential Management Services in order to
        authenticate a user.'
  SUP dlmlDependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.85 NAME
'dlmlRequireCredentialsFromAntecedentRef'
  DESC 'CredentialManagementService from which
        credentials are accepted for the associated
        AuthenticationRequirement. Values of this attribute
        Point to entries of class
        dlmlCredentialManagementService.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.86 NAME
'dlmlRequireCredentialsFromDependentRef'
  DESC 'AuthenticationRequirement that limit acceptable
        credentials. Values of this attribute point to
        entries of class dlmlAuthenticationRequirement.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.117 NAME
'dlmlRequireCredentialsFromAuxClass'
  DESC 'RequireCredentialsFrom is an association used to
        require that credentials are issued by particular
        Credential Management Services in order to
        authenticate a user.'
  SUP dlmlRequireCredentialsFrom AUXILIARY
  MAY ( dlmlRequireCredentialsFromAntecedentRef $
        dlmlRequireCredentialsFromDependentRef )
)

```

)

3.49 AuthenticationTarget Classes

These classes associate a particular resource or set of resources (a ManagedElement entry) with a AuthenticationRequirement entry.

```
( 1.3.6.1.4.1.412.100.4.1.1.118 NAME 'dlm1AuthenticationTarget'  
  DESC 'AuthenticationTarget is an association used to  
    apply authentication requirements for access to  
    specific resources. For example, a shared secret may  
    be sufficient for access to unclassified resources,  
    but for confidential resources, a stronger  
    authentication may be required.'  
  SUP dlm1Dependency ABSTRACT  
)
```

```
( 1.3.6.1.4.1.412.100.4.2.87 NAME  
'dlmAuthenticationTargetAntecedentRef'  
  DESC 'AuthenticationRequirement that apply to specific  
    resources. Values of this attribute point to  
    entries of class dlm1AuthenticationRequirement.'  
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12  
  EQUALITY distinguishedNameMatch  
)
```

```
( 1.3.6.1.4.1.412.100.4.2.88 NAME  
'dlmAuthenticationTargetDependentRef'  
  DESC 'Target resources that may be in a Collection or  
    an individual ManagedElement. These resources are  
    protected by the AuthenticationRequirement. Values  
    of this attribute point to entries of class  
    dlm1ManagedElement.'  
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12  
  EQUALITY distinguishedNameMatch  
)
```

```
( 1.3.6.1.4.1.412.100.4.1.1.119 NAME  
'dlm1AuthenticationTargetAuxClass'  
  DESC 'AuthenticationTarget is an association used to  
    apply authentication requirements for access to  
    specific resources. For example, a shared secret may  
    be sufficient for access to unclassified resources,  
    but for confidential resources, a stronger  
    authentication may be required.'  
  SUP dlm1AuthenticationTarget AUXILIARY  
  MAY ( dlmAuthenticationTargetAntecedentRef $  
    dlmAuthenticationTargetDependentRef )  
)
```

3.50 HostedACI Classes

These classes provide namespace coping for AccessControlInformation entries.

```
( 1.3.6.1.4.1.412.100.4.1.1.120 NAME 'dlm1HostedACI'  
  DESC 'HostedACI is an association used to provide the  
    namespace scoping of AccessControlInformation. The
```

```

        hosted ACI may or may not apply to resources on the
        hosting system.'
    SUP dlm1Dependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.89 NAME 'dlmHostedACIAntecedentRef'
  DESC 'The hosting system. Value of this attribute
        points to an entry of class dlm1System.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.90 NAME 'dlmHostedACIDependentRef'
  DESC 'The hosted AccessControlInformation. Values of
        this attribute point to entries of class
        dlm1AccessControlInformation.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.121 NAME 'dlm1HostedACIAuxClass'
  DESC 'HostedACI is an association used to provide the
        namespace scoping of AccessControlInformation. The
        hosted ACI may or may not apply to resources on the
        hosting system.'
  SUP dlm1HostedACI AUXILIARY
  MAY ( dlmHostedACIAntecedentRef $
        dlmHostedACIDependentRef )
)

```

3.51 AuthenticationUse Classes

These classes provide an AuthorizationService entry with a link to the AccessControlInformation entry it requires.

```

( 1.3.6.1.4.1.412.100.4.1.1.122 NAME 'dlm1AuthorizedUse'
  DESC 'AuthorizedUse is an association used to provide
        an AuthorizationService with the
        AccessControlInformation it needs to do its job.'
  SUP dlm1Dependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.91 NAME 'dlmAuthorizedUseAntecedentRef'
  DESC 'AccessControlInformation. Values of this
        attribute point to entries of class
        dlm1AccessControlInformation.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.92 NAME 'dlmAuthorizedUseDependentRef'
  DESC 'AuthorizationService that uses an ACI. Values
        of this attribute point to entries of class
        dlm1AuthorizationService.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

```



```

( 1.3.6.1.4.1.412.100.4.1.1.123 NAME 'dlm1AuthorizedUseAuxClass'
  DESC 'AuthorizedUse is an association used to provide
        an AuthorizationService with the
        AccessControlInformation it needs to do its job.'
  SUP dlm1AuthorizedUse AUXILIARY
  MAY ( dlm1AuthorizedUseAntecedentRef $
        dlm1AuthorizedUseDependentRef )
)

```

3.52 AuthorizationSubject Classes

These classes apply authorization decisions to specific ManagedElement entries.

```

( 1.3.6.1.4.1.412.100.4.1.1.124 NAME 'dlm1AuthorizationSubject'
  DESC 'AuthorizationSubject is an association used to
        apply authorization decisions to specific subjects
        (i.e., users). The subjects may be identified
        directly or they may be aggregated into a collection
        that may, in turn, use the MemberPrincipal association
        to provide further indirection in the specification of
        the subject set.'
  SUP dlm1Dependency ABSTRACT
)

```

```

( 1.3.6.1.4.1.412.100.4.2.93 NAME
'dlm1AuthorizationSubjectAntecedentRef'
  DESC 'AccessControlInformation that applies to a
        subject set. Values of this attribute point to
        entries of class dlm1AccessControlInformation.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

```

```

( 1.3.6.1.4.1.412.100.4.2.94 NAME
'dlm1AuthorizationSubjectDependentRef'
  DESC 'The subject set may be specified as a collection
        or as a set of associations to ManagedElements that
        represent users. Values of this attribute point to
        entries of class dlm1ManagedElement.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

```

```

( 1.3.6.1.4.1.412.100.4.1.1.125 NAME
'dlm1AuthorizationSubjectAuxClass'
  DESC 'AuthorizationSubject is an association used to
        apply authorization decisions to specific subjects
        (i.e., users). The subjects may be identified
        directly or they may be aggregated into a collection
        that may, in turn, use the MemberPrincipal association
        to provide further indirection in the specification of
        the subject set.'
  SUP dlm1AuthorizationSubject AUXILIARY
  MAY ( dlm1AuthorizationSubjectAntecedentRef $
        dlm1AuthorizationSubjectDependentRef )
)

```

3.53 AuthorizationTarget Classes

These classes apply authorization decisions to a set of target resources (a ManagedElement entry).

```
( 1.3.6.1.4.1.412.100.4.1.1.126 NAME 'dlm1AuthorizationTarget'
  DESC 'AuthorizationTarget is an association used to
        apply authorization decisions to specific target
        resources. The target resources may be aggregated
        into a collection or may be represented as a set of
        associations to ManagedElements.'
  SUP dlm1Dependency ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.95 NAME
'dlmAuthorizationTargetAntecedentRef'
  DESC 'AccessControlInformation that applies to the
        target set. Values of this attribute point to
        entries of class dlm1AccessControlInformation.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.96 NAME
'dlmAuthorizationTargetDependentRef'
  DESC 'The target set of resources may be specified as a
        collection or as a set of associations to
        ManagedElements that represent target resources.
        Values of this attribute point to entries of class
        dlm1ManagedElement.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.127 NAME
'dlm1AuthorizationTargetAuxClass'
  DESC 'AuthorizationTarget is an association used to
        apply authorization decisions to specific target
        resources. The target resources may be aggregated
        into a collection or may be represented as a set of
        associations to ManagedElements.'
  SUP dlm1AuthorizationTarget AUXILIARY
  MAY ( dlmAuthorizationTargetAntecedentRef $
        dlmAuthorizationTargetDependentRef )
)
```

3.54 MemberPrincipal Classes

These classes model the aggregation of membership of principals that are in a Collection.

```
( 1.3.6.1.4.1.412.100.4.2.97 NAME 'dlmUserAccessBy'
  DESC 'A MemberPrincipal may be identified in several
        ways that may be either direct or indirect membership
        in the collection. - A "UsersAccess" membership
        directly identifies the user by the UsersAccess
```

```

object instance. - An "Account" membership directly
identifies the user by the Account object class
instance. - A "UsingElement" membership indirectly
identifies the user by the ManagedElement object
instance that has ElementAsUser associations to
UsersAccess object instances. Hence, all
UsersAccess instances are indirectly included in
the collection. Values are 1="UsersAccess",
2="Account", 3="UsingElement", 4
="CredentialManagementService".'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE
EQUALITY integerMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.128 NAME 'dlm1MemberPrincipal'
DESC 'MemberPrincipal is an aggregation used to
establish membership of principals (i.e., users) in a
Collection. That membership can be established either
directly or indirectly as indicated in the
UsersAccessBy property. For example, a user may be
identified directly by their userid (i.e., Account
object instance) or the user may be identified
indirectly by realm from which a ticket was issued
(i.e., CredentialManagementService object instance).
The latter case is useful, for example, for specifying
that only users identified by an internal credential
service are permitted to access very sensitive
information.'
SUP dlm1MemberOfCollection ABSTRACT
MAY ( dlmUserAccessBy )
)

( 1.3.6.1.4.1.412.100.4.2.98 NAME 'dlmMemberPrincipalCollectionRef'
DESC 'The value of this attribute points to an entry of
class dlm1Collection.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.99 NAME 'dlmMemberPrincipalMemberRef'
DESC 'The value of this attribute points to an entry of
class dlm1ManagedElement.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.129 NAME 'dlm1MemberPrincipalInstance'
DESC 'MemberPrincipal is an aggregation used to
establish membership of principals (i.e., users) in a
Collection. That membership can be established either
directly or indirectly as indicated in the
UsersAccessBy property. For example, a user may be
identified directly by their userid (i.e., Account
object instance) or the user may be identified
indirectly by realm from which a ticket was issued
(i.e., CredentialManagementService object instance).
The latter case is useful, for example, for specifying

```

```

        that only users identified by an internal credential
        service are permitted to access very sensitive
        information.'
    SUP dlm1MemberPrincipal
    MAY ( dlmMemberPrincipalCollectionRef $
          dlmMemberPrincipalMemberRef )
)

( 1.3.6.1.4.1.412.100.4.3.1.23 NAME
'dlm1MemberPrincipalInstanceNameForm1'
  OC dlm1MemberPrincipalInstance
  MUST ( orderedCimKeys )
)

( <user-sr-23 NAME 'dlm1MemberPrincipalInstanceStructureRule1'
  Form dlm1MemberPrincipalInstanceNameForm1
)

( 1.3.6.1.4.1.412.100.4.2.100 NAME 'dlmMemberPrincipalHelperRef'
  DESC 'Pointer to MemberPrincipalInstance.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.130 NAME
'dlm1MemberPrincipalHelperAuxClass'
  DESC 'Helper class for finding MemberPrincipal.'
  SUP top AUXILIARY
  MAY ( dlmMemberPrincipalHelperRef )
)

```

3.55 AccountOnSystem Classes

These classes aggregates Account entries and scope the uniqueness of Account names.

```

( 1.3.6.1.4.1.412.100.4.1.1.131 NAME 'dlm1AccountOnSystem'
  DESC 'A system (e.g., ApplicationSystem,
        ComputerSystem, AdminDomain) aggregates Accounts and
        scopes the uniqueness of the Account names (i.e.,
        userids).'
  SUP dlm1SystemComponent ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.101 NAME
'dlmAccountOnSystemGroupComponentRef'
  DESC 'The aggregating system also provides name scoping
        for the Account. The value of this attribute points to
        an entry of class dlm1System.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.102 NAME
'dlmAccountOnSystemPartComponentRef'
  DESC 'The subordinate Account. Values of this
        attribute point to entries of class account.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)

```

```

EQUALITY distinguishedNameMatch
)
( 1.3.6.1.4.1.412.100.4.1.1.132 NAME 'dlm1AccountOnSystemAuxClass'
DESC 'A system (e.g., ApplicationSystem,
      ComputerSystem, AdminDomain) aggregates Accounts and
      scopes the uniqueness of the Account names (i.e.,
      userids).'
```

SUP dlm1AccountOnSystem AUXILIARY

MAY (dlmAccountOnSystemGroupComponentRef \$
 dlmAccountOnSystemPartComponentRef)

3.56 OrgStructure Classes

These classes establish the parent-child relationship between OrganizationalEntity entries and may be used as an alternative to DIT-containment.

```

( 1.3.6.1.4.1.412.100.4.1.1.133 NAME 'dlm1OrgStructure'
DESC 'OrgStructure is an association used to establish
      parent-child relationships between
      OrganizationalEntity instances. This is used to
      capture organizational relationships between object
      instances such as those that are imported from an
      LDAP-accessible directory.'
```

SUP top ABSTRACT

```

)
( 1.3.6.1.4.1.412.100.4.2.103 NAME 'dlmOrgStructureChildRef'
DESC 'The organizational child in this association,
      i.e., the sub-unit or other owned object instance.
      Values of this attribute points to entries of class
      dlm1OrganizationalEntity.'
```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.12

EQUALITY distinguishedNameMatch

```

)
( 1.3.6.1.4.1.412.100.4.2.104 NAME 'dlmOrgStructureParentRef'
DESC 'The organizational parent in this association.
      The value of this attribute points to an entry of class
      dlm1OrganizationalEntity.'
```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE

EQUALITY distinguishedNameMatch

```

)
( 1.3.6.1.4.1.412.100.4.1.1.134 NAME 'dlm1OrgStructureAuxClass'
DESC 'OrgStructure is an association used to establish
      parent-child relationships between
      OrganizationalEntity instances. This is used to
      capture organizational relationships between object
      instances such as those that are imported from an
      LDAP-accessible directory.'
```

SUP dlm1OrgStructure AUXILIARY

MAY (dlmOrgStructureChildRef \$
 dlmOrgStructureParentRef)

3.57 CollectionInOrganization Classes

These classes establish a parent-child relationship between a collection entry and its "owning" OrganizationalEntity entry and may be used as an alternative to DIT-containment.

```
( 1.3.6.1.4.1.412.100.4.1.1.135 NAME 'dlm1CollectionInOrganization'
  DESC 'CollectionInOrganization is an association used
        to establish a parent-child relationship between a
        collection and an "owning" OrganizationalEntity. A
        single collection should not have both a
        CollectionInOrganization and a CollectionInSystem
        association.'
  SUP top ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.105 NAME
'dlmCollectionInOrganizationChildRef'
  DESC 'The collection. Values of this attribute points
        to entries of class dlm1Collection.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.106 NAME
'dlmCollectionInOrganizationParentRef'
  DESC 'The parent organization responsible for the
        collection. The value of this attribute points to
        an entry of class dlmOrganizationalEntity.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.136 NAME
'dlm1CollectionInOrganizationAuxClass'
  DESC 'CollectionInOrganization is an association used
        to establish a parent-child relationship between a
        collection and an "owning" OrganizationalEntity. A
        single collection should not have both a
        CollectionInOrganization and a CollectionInSystem
        association.'
  SUP dlm1CollectionInOrganization AUXILIARY
  MAY ( dlmCollectionInOrganizationChildRef $
        dlmCollectionInOrganizationParentRef )
)
```

3.58 CollectionInSystem Classes

These classes establish a parent-child relationship between a Collection entry and its "owning" System entry and may be used as an alternative to DIT-containment.

```
( 1.3.6.1.4.1.412.100.4.1.1.137 NAME 'dlm1CollectionInSystem'
  DESC 'CollectionInSystem is an association used to
        establish a parent-child relationship between a
        collection and an "owning" System such as an
        AdminDomain or ComputerSystem. A single collection
```

```

        should not have both a CollectionInOrganization and a
        CollectionInSystem association.'
    SUP top ABSTRACT
)

( 1.3.6.1.4.1.412.100.4.2.107 NAME 'dlmCollectionInSystemChildRef'
  DESC 'The collection. Values of this attribute point to
        entries of class dlm1Collection.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.2.108 NAME 'dlmCollectionInSystemParentRef'
  DESC 'The parent system responsible for the collection.
        The value of this attribute points to an entry of
        class dlmSystem.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
  EQUALITY distinguishedNameMatch
)

( 1.3.6.1.4.1.412.100.4.1.1.138 NAME 'dlm1CollectionInSystemAuxClass'
  DESC 'CollectionInSystem is an association used to
        establish a parent-child relationship between a
        collection and an "owning" System such as an
        AdminDomain or ComputerSystem. A single collection
        should not have both a CollectionInOrganization and a
        CollectionInSystem association.'
  SUP dlm1CollectionInSystem AUXILIARY
  MAY ( dlmCollectionInSystemChildRef $
        dlmCollectionInSystemParentRef )
)

```

4 References

Request For Comments (RFC) and Internet Draft documents are available from numerous mirror sites.

[1] CIM, "CIM User & Security Model, v2.5,"

http://www.dmtf.org/spec/CIM_Schema25/CIM_User25.mof.

[2] M. Wahl, T. Howes, S. Kille, "Lightweight Directory Access Protocol (v3)," RFC 2251, December 1997.

[3] Wahl, S. Kille, T. Howes, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names," RFC 2253, December 1997

[4] DMTF, "DMTF LDAP Schema for the CIM v2.4 Core Information Model,"

<http://www.dmtf.org/spec/DEN/DSP0117.doc>, November 2000.

[5] M. Smith, "Definition of the inetOrgPerson LDAP Object Class," RFC 2798, April 2000.

[6] M. Wahl, "A Summary of the X.500(96) User Schema for use with LDAPv3," RFC 2256, December 1997.

[7] P. Barker, S. Kille. "The COSINE and Internet X.500 Schema," RFC 1274, November 1991.

[8] ITU/CCITT, “Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, “X.509, November 1993.

A. Structure Rule definitions

To aid the reader in mapping what structure rules have been defined and referenced, the following table lists sections and documents where they have been defined.

Rule	Structural Class	RDN Attribute	Section
user-sr-1	d1m1AccountManagementServiceInstanceStructureRule1	orderedCimKeys	3.2
user-sr-2	d1m1AuthenticationServiceInstanceStructureRule1	orderedCimKeys	3.3
user-sr-3	d1m1VerificationServiceInstanceStructureRule1	orderedCimKeys	3.4
user-sr-4	d1m1CredentialManagementServiceInstanceStructureRule1	orderedCimKeys	3.5
user-sr-5	d1m1CertificateAuthorityInstanceStructureRule1	orderedCimKeys	3.6
user-sr-6	d1m1KerberosKeyDistributionCenterInstanceStructureRule1	orderedCimKeys	3.7
user-sr-7	d1m1NotaryInstanceStructureRule1	orderedCimKeys	3.8
user-sr-8	d1m1LocalCredentialManagementServiceInstanceStructureRule1	orderedCimKeys	3.9
user-sr-9	d1m1SharedSecretServiceInstanceStructureRule1	orderedCimKeys	3.10
user-sr-10	d1m1PublicKeyManagementServiceInstanceStructureRule1	orderedCimKeys	3.11
user-sr-11	d1m1AuthorizationServiceInstanceStructureRule1	orderedCimKeys	3.12
user-sr-12	d1m1CredentialManagementSAPInstanceStructureRule1	orderedCimKeys	3.13
user-sr-13	d1m1AuthenticationRequirementInstanceStructureRule1	orderedCimKeys	3.14
user-sr-14	d1m1AccessControlInformationInstanceStructureRule1	orderedCimKeys	3.15
user-	d1m1UsersAccessInstanceStructureRule1	orderedCimKeys	3.18

sr-15			
user-sr-16	d1m1PublicKeyCertificateInstanceStructureRule1	orderedCimKeys	3.20
user-sr-17	d1m1UnsignedPublicKeyInstanceStructureRule1	orderedCimKeys	3.21
user-sr-18	d1m1KerberosTicketInstanceStructureRule1	orderedCimKeys	3.22
user-sr-19	d1m1SharedSecretInstanceStructureRule1	orderedCimKeys	3.23
user-sr-20	d1m1NamedSharedIKESecretInstanceStructureRule1	orderedCimKeys	3.24
user-sr-21	d1m1ServiceUsesSecurityServiceInstanceStructureRule1	orderedCimKeys	3.25
user-sr-22	d1m1PublicPrivateKeyPairInstanceStructureRule1	orderedCimKeys	3.37
user-sr-23	d1m1MemberPrincipalInstanceStructureRule1	orderedCimKeys	3.54

B. OID Assignments

The following three tables provides the summary of OID assignments made in this document

B.1 Object Classes

OID	Object Class	Section
1.3.6.1.4.1.412.100.4.1.1.1	d1m1PersonInfoAuxClass	2.1.1
1.3.6.1.4.1.412.100.4.1.1.2	d1m1OrganizationInfoAuxClass	2.1.2
1.3.6.1.4.1.412.100.4.1.1.3	d1m1RoleInfoAuxClass	2.1.3
1.3.6.1.4.1.412.100.4.1.1.139	d1m1CimLDAPInfoAuxClass	2.1.4
1.3.6.1.4.1.412.100.4.1.1.4	d1m1SecurityService	3.1
1.3.6.1.4.1.412.100.4.1.1.5	d1m1AccountManagementService	3.2
1.3.6.1.4.1.412.100.4.1.1.6	d1m1AccountManagementServiceAuxClass	3.2

1.3.6.1.4.1.412.100.4.1.1.7	d1m1AccountManagementServiceInstance	3.2
1.3.6.1.4.1.412.100.4.1.1.8	d1m1AuthenticationService	3.3
1.3.6.1.4.1.412.100.4.1.1.9	d1m1AuthenticationServiceAuxClass	3.3
1.3.6.1.4.1.412.100.4.1.1.10	d1m1AuthenticationServiceInstance	3.3
1.3.6.1.4.1.412.100.4.1.1.11	d1m1VerificationService	3.4
1.3.6.1.4.1.412.100.4.1.1.12	d1m1VerificationServiceAuxClass	3.4
1.3.6.1.4.1.412.100.4.1.1.13	d1m1VerificationServiceInstance	3.4
1.3.6.1.4.1.412.100.4.1.1.14	d1m1CredentialManagementService	3.5
1.3.6.1.4.1.412.100.4.1.1.15	d1m1CredentialManagementServiceAuxClass	3.5
1.3.6.1.4.1.412.100.4.1.1.16	d1m1CredentialManagementServiceInstance	3.5
1.3.6.1.4.1.412.100.4.1.1.17	d1m1CertificateAuthority	3.6
1.3.6.1.4.1.412.100.4.1.1.18	d1m1CertificateAuthorityAuxClass	3.6
1.3.6.1.4.1.412.100.4.1.1.19	d1m1CertificateAuthorityInstance	3.6
1.3.6.1.4.1.412.100.4.1.1.20	d1m1KerberosKeyDistributionCenter	3.7
1.3.6.1.4.1.412.100.4.1.1.21	d1m1KerberosKeyDistributionCenterAuxClass	3.7
1.3.6.1.4.1.412.100.4.1.1.22	d1m1KerberosKeyDistributionCenterInstance	3.7
1.3.6.1.4.1.412.100.4.1.1.23	d1m1Notary	3.8
1.3.6.1.4.1.412.100.4.1.1.24	d1m1NotaryAuxClass	3.8
1.3.6.1.4.1.412.100.4.1.1.25	d1m1NotaryInstance	3.8
1.3.6.1.4.1.412.100.4.1.1.26	d1m1LocalCredentialManagementService	3.9
1.3.6.1.4.1.412.100.4.1.1.27	d1m1LocalCredentialManagementServiceAuxClass	3.9
1.3.6.1.4.1.412.100.4.1.1.28	d1m1LocalCredentialManagementServiceInstance	3.9
1.3.6.1.4.1.412.100.4.1.1.29	d1m1SharedSecretService	3.10
1.3.6.1.4.1.412.100.4.1.1.30	d1m1SharedSecretServiceAuxClass	3.10
1.3.6.1.4.1.412.100.4.1.1.31	d1m1SharedSecretServiceInstance	3.10
1.3.6.1.4.1.412.100.4.1.1.32	d1m1PublicKeyManagementService	3.11
1.3.6.1.4.1.412.100.4.1.1.33	d1m1PublicKeyManagementServiceAuxClass	3.11
1.3.6.1.4.1.412.100.4.1.1.34	d1m1PublicKeyManagementServiceInstance	3.11
1.3.6.1.4.1.412.100.4.1.1.35	d1m1AuthorizationService	3.12
1.3.6.1.4.1.412.100.4.1.1.36	d1m1AuthorizationServiceAuxClass	3.12
1.3.6.1.4.1.412.100.4.1.1.37	d1m1AuthorizationServiceInstance	3.12
1.3.6.1.4.1.412.100.4.1.1.38	d1m1CredentialManagementSAP	3.13
1.3.6.1.4.1.412.100.4.1.1.39	d1m1CredentialManagementSAPAuxClass	3.13
1.3.6.1.4.1.412.100.4.1.1.40	d1m1CredentialManagementSAPInstance	3.13
1.3.6.1.4.1.412.100.4.1.1.41	d1m1AuthenticationRequirement	3.14
1.3.6.1.4.1.412.100.4.1.1.42	d1m1AuthenticationRequirementAuxClass	3.14
1.3.6.1.4.1.412.100.4.1.1.43	d1m1AuthenticationRequirementInstance	3.14
1.3.6.1.4.1.412.100.4.1.1.44	d1m1AccessControlInformation	3.15

1.3.6.1.4.1.412.100.4.1.1.45	d1m1AccessControlInformationAuxClass	3.15
1.3.6.1.4.1.412.100.4.1.1.46	d1m1AccessControlInformationInstance	3.15
1.3.6.1.4.1.412.100.4.1.1.47	d1m1OrganizationalEntity	3.16
1.3.6.1.4.1.412.100.4.1.1.48	d1m1UserEntity	3.17
1.3.6.1.4.1.412.100.4.1.1.49	d1m1UsersAccess	3.18
1.3.6.1.4.1.412.100.4.1.1.50	d1m1UsersAccessAuxClass	3.18
1.3.6.1.4.1.412.100.4.1.1.51	d1m1UsersAccessInstance	3.18
1.3.6.1.4.1.412.100.4.1.1.52	d1m1Credential	3.19
1.3.6.1.4.1.412.100.4.1.1.53	d1m1PublicKeyCertificate	3.20
1.3.6.1.4.1.412.100.4.1.1.54	d1m1PublicKeyCertificateAuxClass	3.20
1.3.6.1.4.1.412.100.4.1.1.55	d1m1PublicKeyCertificateInstance	3.20
1.3.6.1.4.1.412.100.4.1.1.56	d1m1UnsignedPublicKey	3.21
1.3.6.1.4.1.412.100.4.1.1.57	d1m1UnsignedPublicKeyAuxClass	3.21
1.3.6.1.4.1.412.100.4.1.1.58	d1m1UnsignedPublicKeyInstance	3.21
1.3.6.1.4.1.412.100.4.1.1.59	d1m1KerberosTicket	3.22
1.3.6.1.4.1.412.100.4.1.1.60	d1m1KerberosTicketAuxClass	3.22
1.3.6.1.4.1.412.100.4.1.1.61	d1m1KerberosTicketInstance	3.22
1.3.6.1.4.1.412.100.4.1.1.62	d1m1SharedSecret	3.23
1.3.6.1.4.1.412.100.4.1.1.63	d1m1SharedSecretAuxClass	3.23
1.3.6.1.4.1.412.100.4.1.1.64	d1m1SharedSecretInstance	3.23
1.3.6.1.4.1.412.100.4.1.1.65	d1m1NamedSharedIKESecret	3.24
1.3.6.1.4.1.412.100.4.1.1.66	d1m1NamedSharedIKESecretAuxClass	3.24
1.3.6.1.4.1.412.100.4.1.1.67	d1m1NamedSharedIKESecretInstance	3.24
1.3.6.1.4.1.412.100.4.1.1.68	d1m1ServiceUsesSecurityService	3.25
1.3.6.1.4.1.412.100.4.1.1.69	d1m1ServiceUsesSecurityServiceInstance	3.25
1.3.6.1.4.1.412.100.4.1.1.70	d1m1ServiceUsesSecurityServiceHelperAuxClass	3.25
1.3.6.1.4.1.412.100.4.1.1.71	d1m1SecurityServiceForSystem	3.26
1.3.6.1.4.1.412.100.4.1.1.72	d1m1SecurityServiceForSystemAuxClass	3.26
1.3.6.1.4.1.412.100.4.1.1.73	d1m1ManagesAccountOnSystem	3.27
1.3.6.1.4.1.412.100.4.1.1.74	d1m1ManagesAccountOnSystemAuxClass	3.27
1.3.6.1.4.1.412.100.4.1.1.75	d1m1ElementAsUser	3.28
1.3.6.1.4.1.412.100.4.1.1.76	d1m1ElementAsUserAuxClass	3.28
1.3.6.1.4.1.412.100.4.1.1.77	d1m1SystemAdministrator	3.29
1.3.6.1.4.1.412.100.4.1.1.78	d1m1SystemAdministratorAuxClass	3.29
1.3.6.1.4.1.412.100.4.1.1.79	d1m1SystemAdministratorGroup	3.30
1.3.6.1.4.1.412.100.4.1.1.80	d1m1SystemAdministratorGroupAuxClass	3.30
1.3.6.1.4.1.412.100.4.1.1.81	d1m1SystemAdministratorRole	3.31
1.3.6.1.4.1.412.100.4.1.1.82	d1m1SystemAdministratorRoleAuxClass	3.31

1.3.6.1.4.1.412.100.4.1.1.83	d1m1UsersAccount	3.32
1.3.6.1.4.1.412.100.4.1.1.84	d1m1UsersAccountAuxClass	3.32
1.3.6.1.4.1.412.100.4.1.1.85	d1m1SecurityServiceUsesAccount	3.33
1.3.6.1.4.1.412.100.4.1.1.86	d1m1SecurityServiceUsesAccountAuxClass	3.33
1.3.6.1.4.1.412.100.4.1.1.87	d1m1ManagesAccount	3.34
1.3.6.1.4.1.412.100.4.1.1.88	d1m1ManagesAccountAuxClass	3.34
1.3.6.1.4.1.412.100.4.1.1.89	d1m1TrustHierarchy	3.35
1.3.6.1.4.1.412.100.4.1.1.90	d1m1TrustHierarchyAuxClass	3.35
1.3.6.1.4.1.412.100.4.1.1.91	d1m1UsersCredential	3.36
1.3.6.1.4.1.412.100.4.1.1.92	d1m1UsersCredentialAuxClass	3.36
1.3.6.1.4.1.412.100.4.1.1.93	d1m1PublicPrivateKeyPair	3.37
1.3.6.1.4.1.412.100.4.1.1.94	d1m1PublicPrivateKeyPairInstance	3.37
1.3.6.1.4.1.412.100.4.1.1.95	d1m1PublicPrivateKeyPairHelperAuxClass	3.37
1.3.6.1.4.1.412.100.4.1.1.96	d1m1CAHasPublicCertificate	3.38
1.3.6.1.4.1.412.100.4.1.1.97	d1m1CAHasPublicCertificateAuxClass	3.38
1.3.6.1.4.1.412.100.4.1.1.98	d1m1ManagedCredential	3.39
1.3.6.1.4.1.412.100.4.1.1.99	d1m1ManagedCredentialAuxClass	3.39
1.3.6.1.4.1.412.100.4.1.1.100	d1m1CASignsPublicKeyCertificate	3.40
1.3.6.1.4.1.412.100.4.1.1.101	d1m1CASignsPublicKeyCertificateAuxClass	3.40
1.3.6.1.4.1.412.100.4.1.1.102	d1m1LocallyManagedPublicKey	3.41
1.3.6.1.4.1.412.100.4.1.1.103	d1m1LocallyManagedPublicKeyAuxClass	3.41
1.3.6.1.4.1.412.100.4.1.1.104	d1m1SharedSecretIsShared	3.42
1.3.6.1.4.1.412.100.4.1.1.105	d1m1SharedSecretIsSharedAuxClass	3.42
1.3.6.1.4.1.412.100.4.1.1.106	d1m1IKESecretIsNamed	3.43
1.3.6.1.4.1.412.100.4.1.1.107	d1m1IKESecretIsNamedAuxClass	3.43
1.3.6.1.4.1.412.100.4.1.1.108	d1m1KDCIssuesKerberosTicket	3.44
1.3.6.1.4.1.412.100.4.1.1.109	d1m1KDCIssuesKerberosTicketAuxClass	3.44
1.3.6.1.4.1.412.100.4.1.1.110	d1m1NotaryVerifiesBiometric	3.45
1.3.6.1.4.1.412.100.4.1.1.111	d1m1NotaryVerifiesBiometricAuxClass	3.45
1.3.6.1.4.1.412.100.4.1.1.112	d1m1HostedAuthenticationRequirement	3.46
1.3.6.1.4.1.412.100.4.1.1.113	d1m1HostedAuthenticationRequirementAuxClass	3.46
1.3.6.1.4.1.412.100.4.1.1.114	d1m1AuthenticateForUse	3.47
1.3.6.1.4.1.412.100.4.1.1.115	d1m1AuthenticateForUseAuxClass	3.47
1.3.6.1.4.1.412.100.4.1.1.116	d1m1RequireCredentialsFrom	3.48
1.3.6.1.4.1.412.100.4.1.1.117	d1m1RequireCredentialsFromAuxClass	3.48
1.3.6.1.4.1.412.100.4.1.1.118	d1m1AuthenticationTarget	3.49
1.3.6.1.4.1.412.100.4.1.1.119	d1m1AuthenticationTargetAuxClass	3.49
1.3.6.1.4.1.412.100.4.1.1.120	d1m1HostedACI	3.50

1.3.6.1.4.1.412.100.4.1.1.121	d1m1HostedACIAuxClass	3.50
1.3.6.1.4.1.412.100.4.1.1.122	d1m1AuthorizedUse	3.51
1.3.6.1.4.1.412.100.4.1.1.123	d1m1AuthorizedUseAuxClass	3.51
1.3.6.1.4.1.412.100.4.1.1.124	d1m1AuthorizationSubject	3.52
1.3.6.1.4.1.412.100.4.1.1.125	d1m1AuthorizationSubjectAuxClass	3.52
1.3.6.1.4.1.412.100.4.1.1.126	d1m1AuthorizationTarget	3.53
1.3.6.1.4.1.412.100.4.1.1.127	d1m1AuthorizationTargetAuxClass	3.53
1.3.6.1.4.1.412.100.4.1.1.128	d1m1MemberPrincipal	3.54
1.3.6.1.4.1.412.100.4.1.1.129	d1m1MemberPrincipalInstance	3.54
1.3.6.1.4.1.412.100.4.1.1.130	d1m1MemberPrincipalHelperAuxClass	3.54
1.3.6.1.4.1.412.100.4.1.1.131	d1m1AccountOnSystem	3.55
1.3.6.1.4.1.412.100.4.1.1.132	d1m1AccountOnSystemAuxClass	3.55
1.3.6.1.4.1.412.100.4.1.1.133	d1m1OrgStructure	3.56
1.3.6.1.4.1.412.100.4.1.1.134	d1m1OrgStructureAuxClass	3.56
1.3.6.1.4.1.412.100.4.1.1.135	d1m1CollectionInOrganization	3.57
1.3.6.1.4.1.412.100.4.1.1.136	d1m1CollectionInOrganizationAuxClass	3.57
1.3.6.1.4.1.412.100.4.1.1.137	d1m1CollectionInSystem	3.58
1.3.6.1.4.1.412.100.4.1.1.138	d1m1CollectionInSystemAuxClass	3.58

B.2 Attributes

OID	Attribute	Section
1.3.6.1.4.1.412.100.4.2.1	d1mCADistinguishedName	3.6
1.3.6.1.4.1.412.100.4.2.2	d1mCAPolicyStatement	3.6
1.3.6.1.4.1.412.100.4.2.3	d1mCRL	3.6
1.3.6.1.4.1.412.100.4.2.4	d1mCRLDistributionPoint	3.6
1.3.6.1.4.1.412.100.4.2.5	d1mCRLRefreshFrequency	3.6
1.3.6.1.4.1.412.100.4.2.6	d1mMaxChainLength	3.6
1.3.6.1.4.1.412.100.4.2.7	d1mProtocol	3.7
1.3.6.1.4.1.412.100.4.2.8	d1mCharterExpired	3.8
1.3.6.1.4.1.412.100.4.2.9	d1mCharterIssued	3.8
1.3.6.1.4.1.412.100.4.2.10	d1mComparitors	3.8
1.3.6.1.4.1.412.100.4.2.11	d1mSealProtocol	3.8
1.3.6.1.4.1.412.100.4.2.12	d1mAlgorithm	3.10
1.3.6.1.4.1.412.100.4.2.13	d1mURL	3.13
1.3.6.1.4.1.412.100.4.2.14	d1mSecurityClassification	3.14
1.3.6.1.4.1.412.100.4.2.15	d1mAccessQualifier	3.15
1.3.6.1.4.1.412.100.4.2.16	d1mAccessType	3.15

1.3.6.1.4.1.412.100.4.2.17	dImPermission	3.15
1.3.6.1.4.1.412.100.4.2.18	dImBiometric	3.18
1.3.6.1.4.1.412.100.4.2.19	dImElementID	3.18
1.3.6.1.4.1.412.100.4.2.20	dImAltSubject	3.20
1.3.6.1.4.1.412.100.4.2.21	dImPublicKey	3.20
1.3.6.1.4.1.412.100.4.2.22	dImSubject	3.20
1.3.6.1.4.1.412.100.4.2.23	dImPeerIdentity	3.21
1.3.6.1.4.1.412.100.4.2.24	dImPeerIdentityType	3.21
1.3.6.1.4.1.412.100.4.2.25	dImAccessesService	3.22
1.3.6.1.4.1.412.100.4.2.26	dImRemoteID	3.22
1.3.6.1.4.1.412.100.4.2.27	dImTicketType	3.22
1.3.6.1.4.1.412.100.4.2.28	dImAlgorithm	3.23
1.3.6.1.4.1.412.100.4.2.29	dImProtocol	3.23
1.3.6.1.4.1.412.100.4.2.30	dImSecret	3.23
1.3.6.1.4.1.412.100.4.2.31	dImLocalIdentity	3.24
1.3.6.1.4.1.412.100.4.2.32	dImLocalIdentityType	3.24
1.3.6.1.4.1.412.100.4.2.33	dImSharedSecretName	3.24
1.3.6.1.4.1.412.100.4.2.34	dImServiceUsesSecurityServiceAntecedentRef	3.25
1.3.6.1.4.1.412.100.4.2.35	dImServiceUsesSecurityServiceDependentRef	3.25
1.3.6.1.4.1.412.100.4.2.36	dImServiceUsesSecurityServiceHelperRef	3.25
1.3.6.1.4.1.412.100.4.2.37	dImSecurityServiceForSystemAntecedentRef	3.26
1.3.6.1.4.1.412.100.4.2.38	dImSecurityServiceForSystemDependentRef	3.26
1.3.6.1.4.1.412.100.4.2.39	dImManagesAccountOnSystemAntecedentRef	3.27
1.3.6.1.4.1.412.100.4.2.40	dImManagesAccountOnSystemDependentRef	3.27
1.3.6.1.4.1.412.100.4.2.41	dImElementAsUserAntecedentRef	3.28
1.3.6.1.4.1.412.100.4.2.42	dImElementAsUserDependentRef	3.28
1.3.6.1.4.1.412.100.4.2.43	dImSystemAdministratorAntecedentRef	3.29
1.3.6.1.4.1.412.100.4.2.44	dImSystemAdministratorDependentRef	3.29
1.3.6.1.4.1.412.100.4.2.45	dImSystemAdministratorGroupAntecedentRef	3.30
1.3.6.1.4.1.412.100.4.2.46	dImSystemAdministratorGroupDependentRef	3.30
1.3.6.1.4.1.412.100.4.2.47	dImSystemAdministratorRoleAntecedentRef	3.31
1.3.6.1.4.1.412.100.4.2.48	dImSystemAdministratorRoleDependentRef	3.31
1.3.6.1.4.1.412.100.4.2.49	dImUsersAccountAntecedentRef	3.32
1.3.6.1.4.1.412.100.4.2.50	dImUsersAccountDependentRef	3.32
1.3.6.1.4.1.412.100.4.2.51	dImSecurityServiceUsesAccountAntecedentRef	3.33
1.3.6.1.4.1.412.100.4.2.52	dImSecurityServiceUsesAccountDependentRef	3.33
1.3.6.1.4.1.412.100.4.2.53	dImManagesAccountAntecedentRef	3.34
1.3.6.1.4.1.412.100.4.2.54	dImManagesAccountDependentRef	3.34

1.3.6.1.4.1.412.100.4.2.55	dImTrustHierarchyAntecedentRef	3.35
1.3.6.1.4.1.412.100.4.2.56	dImTrustHierarchyDependentRef	3.35
1.3.6.1.4.1.412.100.4.2.57	dImUsersCredentialAntecedentRef	3.36
1.3.6.1.4.1.412.100.4.2.58	dImUsersCredentialDependentRef	3.36
1.3.6.1.4.1.412.100.4.2.59	dImRepository	3.37
1.3.6.1.4.1.412.100.4.2.60	dImUse	3.37
1.3.6.1.4.1.412.100.4.2.61	dImPublicPrivateKeyPairAntecedentRef	3.37
1.3.6.1.4.1.412.100.4.2.62	dImPublicPrivateKeyPairDependentRef	3.37
1.3.6.1.4.1.412.100.4.2.63	dImPublicPrivateKeyPairHelperRef	3.37
1.3.6.1.4.1.412.100.4.2.64	dImCAHasPublicCertificateAntecedentRef	3.38
1.3.6.1.4.1.412.100.4.2.65	dImCAHasPublicCertificateDependentRef	3.38
1.3.6.1.4.1.412.100.4.2.66	dImManagedCredentialAntecedentRef	3.39
1.3.6.1.4.1.412.100.4.2.67	dImManagedCredentialDependentRef	3.39
1.3.6.1.4.1.412.100.4.2.68	dImSignature	3.40
1.3.6.1.4.1.412.100.4.2.69	dImCASignsPublicKeyCertificateAntecedentRef	3.40
1.3.6.1.4.1.412.100.4.2.70	dImCASignsPublicKeyCertificateDependentRef	3.40
1.3.6.1.4.1.412.100.4.2.71	dImLocallyManagedPublicKeyAntecedentRef	3.41
1.3.6.1.4.1.412.100.4.2.72	dImLocallyManagedPublicKeyDependentRef	3.41
1.3.6.1.4.1.412.100.4.2.73	dImSharedSecretIsSharedAntecedentRef	3.42
1.3.6.1.4.1.412.100.4.2.74	dImSharedSecretIsSharedDependentRef	3.42
1.3.6.1.4.1.412.100.4.2.75	dImIKESecretIsNamedAntecedentRef	3.43
1.3.6.1.4.1.412.100.4.2.76	dImIKESecretIsNamedDependentRef	3.43
1.3.6.1.4.1.412.100.4.2.77	dImKDCIssuesKerberosTicketAntecedentRef	3.44
1.3.6.1.4.1.412.100.4.2.78	dImKDCIssuesKerberosTicketDependentRef	3.44
1.3.6.1.4.1.412.100.4.2.79	dImNotaryVerifiesBiometricAntecedentRef	3.45
1.3.6.1.4.1.412.100.4.2.80	dImNotaryVerifiesBiometricDependentRef	3.45
1.3.6.1.4.1.412.100.4.2.81	dImHostedAuthenticationRequirementAntecedentRef	3.46
1.3.6.1.4.1.412.100.4.2.82	dImHostedAuthenticationRequirementDependentRef	3.46
1.3.6.1.4.1.412.100.4.2.83	dImAuthenticateForUseAntecedentRef	3.47
1.3.6.1.4.1.412.100.4.2.84	dImAuthenticateForUseDependentRef	3.47
1.3.6.1.4.1.412.100.4.2.85	dImRequireCredentialsFromAntecedentRef	3.48
1.3.6.1.4.1.412.100.4.2.86	dImRequireCredentialsFromDependentRef	3.48
1.3.6.1.4.1.412.100.4.2.87	dImAuthenticationTargetAntecedentRef	3.49
1.3.6.1.4.1.412.100.4.2.88	dImAuthenticationTargetDependentRef	3.49
1.3.6.1.4.1.412.100.4.2.89	dImHostedACIAntecedentRef	3.50
1.3.6.1.4.1.412.100.4.2.90	dImHostedACIDependentRef	3.50
1.3.6.1.4.1.412.100.4.2.91	dImAuthorizedUseAntecedentRef	3.51
1.3.6.1.4.1.412.100.4.2.92	dImAuthorizedUseDependentRef	3.51

1.3.6.1.4.1.412.100.4.2.93	dImAuthorizationSubjectAntecedentRef	3.52
1.3.6.1.4.1.412.100.4.2.94	dImAuthorizationSubjectDependentRef	3.52
1.3.6.1.4.1.412.100.4.2.95	dImAuthorizationTargetAntecedentRef	3.53
1.3.6.1.4.1.412.100.4.2.96	dImAuthorizationTargetDependentRef	3.53
1.3.6.1.4.1.412.100.4.2.97	dImUserAccessBy	3.54
1.3.6.1.4.1.412.100.4.2.98	dImMemberPrincipalCollectionRef	3.54
1.3.6.1.4.1.412.100.4.2.99	dImMemberPrincipalMemberRef	3.54
1.3.6.1.4.1.412.100.4.2.100	dImMemberPrincipalHelperRef	3.54
1.3.6.1.4.1.412.100.4.2.101	dImAccountOnSystemGroupComponentRef	3.55
1.3.6.1.4.1.412.100.4.2.102	dImAccountOnSystemPartComponentRef	3.55
1.3.6.1.4.1.412.100.4.2.103	dImOrgStructureChildRef	3.56
1.3.6.1.4.1.412.100.4.2.104	dImOrgStructureParentRef	3.56
1.3.6.1.4.1.412.100.4.2.105	dImCollectionInOrganizationChildRef	3.57
1.3.6.1.4.1.412.100.4.2.106	dImCollectionInOrganizationParentRef	3.57
1.3.6.1.4.1.412.100.4.2.107	dImCollectionInSystemChildRef	3.58
1.3.6.1.4.1.412.100.4.2.108	dImCollectionInSystemParentRef	3.58

B.3 Nameforms

OID	Nameform	Section
1.3.6.1.4.1.412.100.4.3.1.1	dIm1AccountManagementServiceInstanceNameForm1	3.2
1.3.6.1.4.1.412.100.4.3.1.2	dIm1AuthenticationServiceInstanceNameForm1	3.3
1.3.6.1.4.1.412.100.4.3.1.3	dIm1VerificationServiceInstanceNameForm1	3.4
1.3.6.1.4.1.412.100.4.3.1.4	dIm1CredentialManagementServiceInstanceNameForm1	3.5
1.3.6.1.4.1.412.100.4.3.1.5	dIm1CertificateAuthorityInstanceNameForm1	3.6
1.3.6.1.4.1.412.100.4.3.1.6	dIm1KerberosKeyDistributionCenterInstanceNameForm1	3.7
1.3.6.1.4.1.412.100.4.3.1.7	dIm1NotaryInstanceNameForm1	3.8
1.3.6.1.4.1.412.100.4.3.1.8	dIm1LocalCredentialManagementServiceInstanceNameForm1	3.9
1.3.6.1.4.1.412.100.4.3.1.9	dIm1SharedSecretServiceInstanceNameForm1	3.10
1.3.6.1.4.1.412.100.4.3.1.10	dIm1PublicKeyManagementServiceInstanceNameForm1	3.11
1.3.6.1.4.1.412.100.4.3.1.11	dIm1AuthorizationServiceInstanceNameForm1	3.12
1.3.6.1.4.1.412.100.4.3.1.12	dIm1CredentialManagementSAPInstanceNameForm1	3.13
1.3.6.1.4.1.412.100.4.3.1.13	dIm1AuthenticationRequirementInstanceNameForm1	3.14
1.3.6.1.4.1.412.100.4.3.1.14	dIm1AccessControlInformationInstanceNameForm1	3.15
1.3.6.1.4.1.412.100.4.3.1.15	dIm1UsersAccessInstanceNameForm1	3.18
1.3.6.1.4.1.412.100.4.3.1.16	dIm1PublicKeyCertificateInstanceNameForm1	3.20
1.3.6.1.4.1.412.100.4.3.1.17	dIm1UnsignedPublicKeyInstanceNameForm1	3.21
1.3.6.1.4.1.412.100.4.3.1.18	dIm1KerberosTicketInstanceNameForm1	3.22

1.3.6.1.4.1.412.100.4.3.1.19	d1m1SharedSecretInstanceNameForm1	3.23
1.3.6.1.4.1.412.100.4.3.1.20	d1m1NamedSharedIKESecretInstanceNameForm1	3.24
1.3.6.1.4.1.412.100.4.3.1.21	d1m1ServiceUsesSecurityServiceInstanceNameForm1	3.25
1.3.6.1.4.1.412.100.4.3.1.22	d1m1PublicPrivateKeyPairInstanceNameForm1	3.37
1.3.6.1.4.1.412.100.4.3.1.23	d1m1MemberPrincipalInstanceNameForm1	3.54