



Entrust® White Paper

Entrust Directory Schema Requirements

Author: Chris Oliva
Date: August 1998
Version: 1.0



Table of Contents

1. INTRODUCTION.....	2
2. SCHEMA SUMMARY	2
3. OBJECT CLASSES.....	5
3.1 ENTRUST USER OBJECT CLASS.....	5
3.2 ENTRUST CA OBJECT CLASS	5
3.3 CC MAIL USER OBJECT CLASS	6
3.4 MS MAIL USER OBJECT CLASS	6
3.5 UNIQUELY IDENTIFIED USER OBJECT CLASS.....	6
3.6 SIMPLE AUTHENTICATION OBJECT CLASS.....	7
3.7 QM MAIL USER OBJECT CLASS.....	7
3.8 RFC 822 MAIL USER OBJECT CLASS.....	8
3.9 TRUST TYPES OBJECT CLASS.....	8
3.10 EMAIL ADDRESS USER OBJECT CLASS	8
3.11 CISCO ENROLLMENT PROTOCOL ENABLED DEVICE.....	9
3.12 PKCS#10 ENABLED DEVICE OBJECT CLASS.....	9
4. ATTRIBUTES.....	9
4.1 EMAIL ADDRESS ATTRIBUTE	10
4.2 CC MAIL NAME ATTRIBUTE	10
4.3 CC MAIL POSTOFFICE ATTRIBUTE	10
4.4 CC MAIL COMMENTS ATTRIBUTE	11
4.5 MS MAIL FULLNAME ATTRIBUTE.....	11
4.6 MS MAIL ID ATTRIBUTE	11
4.7 MS MAIL NETWORK ATTRIBUTE	12
4.8 MS MAIL POSTOFFICE ATTRIBUTE	12
4.9 ATTRIBUTE CERTIFICATE ATTRIBUTE.....	12
4.10 QM USER NAME ATTRIBUTE	13
4.11 QM MAIL CENTER ATTRIBUTE.....	13
4.12 QM ZONE ATTRIBUTE.....	13
4.13 S/MIME TRUST ATTRIBUTE.....	14
4.14 SSL TRUST ATTRIBUTE	14
4.15 OBJECT SIGNING TRUST ATTRIBUTE	14
4.16 UNSTRUCTURED NAME ATTRIBUTE.....	15
4.17 UNSTRUCTURED ADDRESS ATTRIBUTE	15
5. NAME FORMS	15
5.1 UNIQUE PERSON NAME FORM.....	16
5.2 UNIQUE ORGANIZATIONAL PERSON NAME FORM.....	16
5.3 UNIQUE RESIDENTIAL PERSON NAME FORM.....	16
5.4 EMAIL USER ORGANIZATIONAL PERSON NAME FORM	17
5.5 VPN DEVICE NAME FORM.....	17
6. STRUCTURE RULES	17

1. Introduction

This document describes the schema required for directory interoperability with Entrust PKI and Entrust-Ready products. Schema elements are described in ASN.1 notation with accompanying text so that LDAP or X.500 products may be adequately configured. A more detailed description of directory requirements and directory integration issues is available in the document entitled “Entrust Directory Integration Guide”.

Products which use this schema specification must support the indicated object classes and attributes. Name Forms are defined which indicate how entries might be named. Products should support functionality which will allow the equivalent implementation of the Name Forms. Structure Rules are not mandated by Entrust, however, it is necessary that entries which include the structural objectclasses “cRLDistributionPoint” and “organizationalPerson” can be created under the CA entry. The CA entry can be any structural object class but will include the auxiliary object class “entrustCA”.

2. Schema Summary

This section provides a table reference which lists all the object classes and attributes which are required. The table groups the schema elements into categories which defines the specific product solution which requires them. For example, the “Core Schema Components” are required by all Entrust PKI solutions including the Entrust/PKI product. The “MSMail Components” are only required by the integrated MS Mail solution.

This list represents the minimum schema configuration required for Entrust and does not preclude the use of additional schema elements. Refer to the “Entrust Directory Integration Guide” for more detailed information. Standard X.500 definitions are not included within this document but are referenced. Attribute type descriptions include alternate short form names which can be configured for LDAP servers.

Required Object Classes

Object Class	Defined In
Core Schema Components	
entrustUser	Entrust Schema Document
entrustCA	Entrust Schema Document
organizationalPerson	X.521
cRLDistributionPoint	X.521

uniquelyIdentifiedUser	Entrust Schema Document
simpleAuthObject	Entrust Schema Document
rfc822MailUser	Entrust Schema Document
emailAddressUser	Entrust Schema Document
MS Mail Components	
msMailUser	Entrust Schema Document
CC Mail Components	
ccMailUser	Entrust Schema Document
Quick Mail Components	
qmMailUser	Entrust Schema Document
Entrust Ready Netscape Components	
trustTypes	Entrust Schema Document
VPN Connector Components	
pKCS10Device	Entrust Schema Document
cEPDevice	Entrust Schema Document

Required Attributes

Attribute Type	LDAP Short Name	Defined In
Core Schema Components		
userCertificate (v3)		X.509 (1997)
cACertificate		X.509 (1997)
certificateRevocationList (v2)		X.509 (1997)
authorityRevocationList		X.509 (1997)
crossCertificatePair		X.509 (1997)
userPassword		X.509 (1997)
attributeCertificate		Entrust Schema Document
commonName	cn	X.520

Entrust Directory Schema Requirements

surname	sn	X.520
serialNumber		X.520
rfc822Mailbox	mail	RFC 1274
emailAddress	email	PKCS #9 Entrust Schema Document
countryName	c	X.520
organizationName	o	X.520
organizationalUnitName	ou	X.520
MS Mail Components		
msMailPostoffice		Entrust Schema Document
msMailNetwork		Entrust Schema Document
msMailId		Entrust Schema Document
msMailFullName		Entrust Schema Document
CC Mail Components		
ccMailPostoffice		Entrust Schema Document
ccMailName		Entrust Schema Document
ccMailComments		Entrust Schema Document
Quick Mail Components		
qmZone		Entrust Schema Document
qmMailCenter		Entrust Schema Document
qmUserName		Entrust Schema Document
Entrust Ready Netscape Components		
smimetrust		Entrust Schema Document
ssltrust		Entrust Schema Document
objsigntrust		Entrust Schema Document
VPN Connector Components		
unstructuredName		PKCS #9 Entrust Schema Document
unstructuredAddress		PKCS #9 Entrust Schema Document

3. Object Classes

These object class specifications support the generation of appropriate directory entries and define the attribute types which are to be contained in the resulting entries. The specification of each object class is included below, expressed in the same ASN.1 format as the object classes defined in X.521.

3.1 *Entrust User Object Class*

The **entrustUser** object class is used to establish directory entries representing objects which have been issued certificates by an Entrust/Authority. The **entrustUser** OID will be held in resulting directory entries as a value of the **objectClass** attribute. This value will be added to the **objectClass** attribute when the object represented by that entry is first issued a certificate by an Entrust/Authority. The value will be present for the entire time that the object has credentials managed by an Entrust/Authority.

The specification of this object class is:

```
entrustUser          OBJECT-CLASS ::= {
    SUBCLASS OF      { top }
    KIND              auxiliary
    MAY CONTAIN      { userCertificate }
    ID                id-nsn-oc-entrustUser }
```

The OID for **entrustUser** is 1 2 840 113533 7 67 0

3.2 *Entrust CA Object Class*

The **entrustCA** object class is used to establish directory entries representing Entrust/Authority Certification Authorities. The **entrustCA** OID will be held in resulting directory entries as a value of the **objectClass** attribute.

The specification of this object class is:

```
entrustCA           OBJECT-CLASS ::= {
    SUBCLASS OF      { top }
    KIND              auxiliary
    MAY CONTAIN      { cACertificate |
                     certificationRevocationList |
                     authorityRevocationList |
                     crossCertificatePair |
                     userPassword |
                     attributeCertificate }
    ID                id-nsn-oc-entrustCA }
```

The OID for `entrustCA` is 1 2 840 113533 7 67 1

3.3 CC Mail User Object Class

The `ccMailUser` object class is for use in directory content rules and for use in denoting that an entry represents a cc:mail user.

The specification of this object class is:

<code>ccMailUser</code>	OBJECT-CLASS ::= {
SUBCLASS OF	{ top }
KIND	auxiliary
MAY CONTAIN	{ ccMailComments
	ccMailName
	ccMailPostoffice }
ID	id-nsn-oc-ccMailUser }

The OID for `ccMailUser` is 1 2 840 113533 7 67 2

3.4 MS Mail User Object Class

The `msMailUser` object class is for use in directory content rules and for use in denoting that an entry represents an MSMail user.

The specification of this object class is:

<code>msMailUser</code>	OBJECT-CLASS ::= {
SUBCLASS OF	{ top }
KIND	auxiliary
MAY CONTAIN	{ msMailFullname
	msMailId
	msMailNetwork
	msMailPostoffice }
ID	id-nsn-oc-msMailUser }

The OID for `msMailUser` is 1 2 840 113533 7 67 3

3.5 Uniquely Identified User Object Class

The `uniquelyIdentifiedUser` object class is used to specify that an entry must contain a `serialNumber` attribute. This attribute will be used to uniquely identify the object represented by

that entry. One of the values of the **serialNumber** attribute should be distinguished, and that value must be unique within the Directory Management Domain (DMD) responsible for the entry.

The specification of this object class is:

```
uniquelyIdentifiedUser OBJECT-CLASS ::= {  
    SUBCLASS OF      { top }  
    KIND              auxiliary  
    MUST CONTAIN     { serialNumber }  
    ID                id-nsn-oc-uniquelyIdentifiedUser }
```

The OID for **uniquelyIdentifiedUser** is 1 2 840 113533 7 67 4

3.6 Simple Authentication Object Class

The **simpleAuthObject** object class is used to indicate that the object represented by an entry may bind to the Directory using simple authentication. This object class will be of particular usefulness for users representing objects which do not normally have **userPassword** attributes, (e.g. locality).

The specification of this object class is:

```
simpleAuthObject OBJECT-CLASS ::= {  
    SUBCLASS OF      { top }  
    KIND              auxiliary  
    MUST CONTAIN     { userPassword }  
    ID                id-nsn-oc-simpleAuthObject }
```

The OID for **simpleAuthObject** is 1 2 840 113533 7 67 5

3.7 QM Mail User Object Class

The **qmMailUser** object class is used in content rules and in denoting that an entry represents a QuickMail user.

The specification of this object class is:

```
qmMailUser OBJECT-CLASS ::= {  
    SUBCLASS OF      { top }  
    KIND              auxiliary  
    MAY CONTAIN     { qmUserName |  
                    qmMailCenter |  
                    qmZone }  
    ID                id-nsn-oc-qmMailUser }
```

The OID for `qmMailUser` is 1 2 840 113533 7 67 6

3.8 RFC 822 Mail User Object Class

The `rfc822MailUser` object class is used in content rules and in denoting that an entry represents a rfc822 Mail user.

The specification of this object class is:

```
rfc822MailUser      OBJECT-CLASS ::= {
  SUBCLASS OF      { top }
  KIND              auxiliary
  MAY CONTAIN      { rfc822Mailbox }
  ID                id-nsn-oc-rfc822MailUser }
```

The definition of `rfc822Mailbox` is contained in RFC 1274.

The OID for `rfc822MailUser` is 1 2 840 113533 7 67 7

3.9 Trust Types Object Class

The `trustTypes` object class is used in content rules and in denoting that an entry represents an Entrust Ready Netscape user with specific trust types.

The specification of this object class is:

```
trustTypes          OBJECT-CLASS ::= {
  SUBCLASS OF      { top }
  KIND              auxiliary
  MAY CONTAIN      { smimetrust |
                   ssltrust |
                   objsigntrust }
  ID                id-nsn-oc-trustTypes }
```

The OID for `trustTypes` is 1 2 840 113533 7 67 8

3.10 Email Address User Object Class

The `emailAddressUser` auxiliary object class is used in content rules and in denoting that an entry may contain a PKCS9 `emailAddress`.

The specification of this object class is:

```
emailAddressUser      OBJECT-CLASS ::= {
  SUBCLASS OF         { top }
  KIND                 auxiliary
  MAY CONTAIN         { emailAddress }
  ID                   id-nsn-oc-emailAddressUser }
```

The OID for `emailAddressUser` is 1 2 840 113533 7 67 9

3.11 CISCO Enrollment Protocol Enabled Device

The `cEPDevice` object class is used, by the VPN Connector to search for Cisco Enrollment Protocol devices in the directory.

The specification of this object class is:

```
cEPDevice            OBJECT-CLASS ::= {
  KIND                 auxiliary
  SUBCLASS OF         { top }
  MAY CONTAIN         { unstructuredName |
                      unstructuredAddress }
  ID                   id-nsn-oc-cEPDevice }
```

The OID for `cEPDevice` is 1 2 840 113533 7 67 11

3.12 PKCS#10 Enabled Device Object Class

The `pKCS10Device` object class is used by the VPN connector to search for PKCS#10 enabled devices in the directory.

The specification of this object class is:

```
pKCS10Device        OBJECT-CLASS ::= {
  KIND                 auxiliary
  SUBCLASS OF         { top }
  MAY CONTAIN         { serialNumber }
  ID                   id-nsn-oc-pKCS10Device }
```

The OID for `pKCS10Device` is 1 2 840 113533 7 67 12

4. Attributes

The specification of each attribute is included below, expressed in the same ASN.1 format as the attributes defined in X.520. Where new attribute syntaxes are also required, their specification is included with the attribute specification. For attributes using syntaxes defined elsewhere, a reference is included to the authoritative source for that syntax specification.

4.1 Email Address Attribute

The **emailAddress** attribute is used to store an entry's electronic mail address. The OID for this attribute is defined in PKCS#9. The matching rules should be applicable to the IA5String syntax and allow for equality and substring matches where the case is ignored.

```
emailAddress      ATTRIBUTE ::= {
  WITH SYNTAX      IA5String (SIZE(1..128))
  ID                pkcs9-emailAddress }
```

The OID for **pkcs9-emailAddress** is 1 2 840 113549 1 9 1

4.2 CC Mail Name Attribute

The **ccMailName** attribute is used to store the ccMail name of a user in their Directory entry.

The specification of this attribute is:

```
ccMailName        ATTRIBUTE ::= {
  WITH SYNTAX      DirectoryString { 256 }
  EQUALITY MATCHING RULE caseIgnoreMatch
  SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch
  ID                id-nsn-at-ccMailName }
```

The OID for **ccMailName** is 1 2 840 113533 7 68 2

4.3 CC Mail Postoffice Attribute

The **ccMailPostoffice** attribute is used to store the ccMail postoffice for a user in their Directory entry.

The specification of this attribute is:

```
ccMailPostoffice  ATTRIBUTE ::= {
  WITH SYNTAX      DirectoryString { 256 }
  EQUALITY MATCHING RULE caseIgnoreMatch
  SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch
  ID                id-nsn-at-ccMailPostoffice }
```

The OID for `ccMailPostoffice` is 1 2 840 113533 7 68 3

4.4 CC Mail Comments Attribute

The `ccMailComments` attribute is used to store additional information about a ccMail user in their Directory entry.

The specification of this attribute is:

```
ccMailComments          ATTRIBUTE ::= {
  WITH SYNTAX           DirectoryString { 256 }
  EQUALITY MATCHING RULE caseIgnoreMatch
  SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch
  ID                    id-nsn-at-ccMailComments }
```

The OID for `ccMailComments` is 1 2 840 113533 7 68 4

4.5 MS Mail Fullname Attribute

The `msMailFullname` attribute is used to store an MS Mail user's fullname in their Directory entry.

The specification of this attribute is:

```
msMailFullname         ATTRIBUTE ::= {
  WITH SYNTAX           DirectoryString { 256 }
  EQUALITY MATCHING RULE caseIgnoreMatch
  SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch
  ID                    id-nsn-at-msMailFullname }
```

The OID for `msMailFullname` is 1 2 840 113533 7 68 6

4.6 MS Mail ID Attribute

The `msMailId` attribute is used to store an MS Mail user's identifier in their Directory entry.

The specification of this attribute is:

```
msMailId               ATTRIBUTE ::= {
  WITH SYNTAX           DirectoryString { 256 }
  EQUALITY MATCHING RULE caseIgnoreMatch
  SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch }
```

ID id-nsn-at-msMailId }

The OID for msMailId is 1 2 840 113533 7 68 7

4.7 MS Mail Network Attribute

The msMailNetwork attribute is used to store an MS Mail user's network information in their Directory entry.

The specification of this attribute is:

```
msMailNetwork          ATTRIBUTE ::= {  
  WITH SYNTAX          DirectoryString { 256 }  
  EQUALITY MATCHING RULE caseIgnoreMatch  
  SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch  
  ID                   id-nsn-at-msMailNetwork }
```

The OID for msMailNetwork is 1 2 840 113533 7 68 8

4.8 MS Mail Postoffice Attribute

The msMailPostoffice attribute is used to store an MS Mail user's postoffice information in their Directory entry.

The specification of this attribute is:

```
msMailPostoffice      ATTRIBUTE ::= {  
  WITH SYNTAX          DirectoryString { 256 }  
  EQUALITY MATCHING RULE caseIgnoreMatch  
  SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch  
  ID                   id-nsn-at-msMailPostoffice }
```

The OID for msMailPostoffice is 1 2 840 113533 7 68 9

4.9 Attribute Certificate Attribute

The attributeCertificate attribute is used to attribute certificates in an Entrust CA's Directory entry.

The specification of this attribute is:

```
attributeCertificate   ATTRIBUTE ::= {  
  WITH SYNTAX          AttributeCertificate
```


The **qmZone** attribute is used to store a QuickMail user's mail zone information in their Directory entry.

The specification of this attribute is:

```
qmZone          ATTRIBUTE ::= {  
    WITH SYNTAX      DirectoryString { 32 }  
    EQUALITY MATCHING RULE    caseIgnoreMatch  
    SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch  
    ID                id-nsn-at-qmZone }
```

The OID for **qmZone** is 1 2 840 113533 7 68 14

4.13 S/MIME Trust Attribute

The **smimetrust** attribute is used to represent the state of trust assigned for S/MIME (internal, internal+PAB or external). The attribute is stored in the user's entry. Matching rules should be configured which allow matching for presence and equality.

The specification of this attribute is:

```
smimetrust     ATTRIBUTE ::= {  
    WITH SYNTAX      IA5String  
    ID                id-nsn-at-smimetrust }
```

The OID for **smimetrust** is 1 2 840 113533 7 68 17

4.14 SSL Trust Attribute

The **ssltrust** attribute is used to represent the state of trust assigned for SSL (internal, internal+PAB or external). The attribute is stored in the user's entry. Matching rules should be configured which allow matching for presence and equality.

The specification of this attribute is:

```
ssltrust       ATTRIBUTE ::= {  
    WITH SYNTAX      IA5String  
    ID                id-nsn-at-ssltrust }
```

The OID for **ssltrust** is 1 2 840 113533 7 68 18

4.15 Object Signing Trust Attribute

The **objsigntrust** attribute is used to represent the state of trust assigned for object signing (internal, internal+PAB or external). The attribute is stored in the user's entry. Matching rules should be configured which allow matching for presence and equality.

The specification of this attribute is:

```
objsigntrust          ATTRIBUTE ::= {  
  WITH SYNTAX        IA5String  
  ID                  id-nsn-at-objsigntrust }
```

The OID for **objsigntrust** is 1 2 840 113533 7 68 19

4.16 Unstructured Name Attribute

The **unstructuredName** attribute is used by the VPN Connector product to name a subject of a certificate. The matching rules should be applicable to the IA5String syntax and allow for equality and substring matches where the case is ignored.

```
unstructuredName     ATTRIBUTE ::= {  
  WITH SYNTAX        IA5String (SIZE(1..256))  
  ID                  pkcs9-unstructuredName }
```

The OID for **unstructuredName** is 1 2 840 113549 1 9 2

4.17 Unstructured Address Attribute

The **unstructuredAddress** attribute is used by the VPN Connector product to specify the address of a subject of a certificate.

```
unstructuredAddress  ATTRIBUTE ::= {  
  WITH SYNTAX        DirectoryString { 256 }  
  EQUALITY MATCHING RULE  caseIgnoreMatch  
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch  
  ID                  pkcs9-unstructuredAddress }
```

The OID for **unstructuredAddress** is 1 2 840 113549 1 9 8

5. Name Forms

This arc is used to register name forms, as required by Entrust. The specification of each name form is included below, expressed in the same ASN.1 format as the name forms defined in X.521.

5.1 Unique Person Name Form

The `uniquePersonNameForm` name form is used to name entries of the `person` object class.

The specification of this name form is:

```
uniquePersonNameForm NAME-FORM
  NAMES                person
  WITH ATTRIBUTES     commonName,serialNumber
  ID                   id-nsn-nf-uniquePersonNameForm }
```

The OID for `uniquePersonNameForm` is 1 2 840 113533 7 69 1

5.2 Unique Organizational Person Name Form

The `uniqueOrganizationalPersonNameForm` name form is used to name entries of the `organizationalPerson` object class.

The specification of this name form is:

```
uniqueOrganizationalPersonNameForm NAME-FORM
  NAMES                OrganizationalPerson
  WITH ATTRIBUTES     commonName,serialNumber
  AND OPTIONALLY     organizationalUnitName
  ID                   id-nsn-nf-uniqueOrganizationalPersonNameForm }
```

The OID for `uniqueOrganizationalPersonNameForm` is 1 2 840 113533 7 69 2

5.3 Unique Residential Person Name Form

The `uniqueResidentialPersonNameForm` name form is used to name entries of the `residentialPerson` object class.

The specification of this name form is:

```
uniqueResidentialPersonNameForm NAME-FORM
  NAMES                ResidentialPerson
  WITH ATTRIBUTES     commonName,serialNumber
  AND OPTIONALLY     streetAddress
  ID                   id-nsn-nf-uniqueResidentialPersonNameForm }
```

The OID for `uniqueResidentialPersonNameForm` is 1 2 840 113533 7 69 3

5.4 Email User Organizational Person Name Form

The `emailUserOrgPersonNameForm` name form is used to name entries of the `organizationalPerson` object class.

The specification of this name form is:

```
emailUserOrgPersonNameForm  NAME-FORM
NAMES                       OrganizationalPerson
WITH ATTRIBUTES             commonName
AND OPTIONALLY              organizationalUnitName,serialNumber,emailAddress
ID                           id-nsn-nf- emailUserOrgPersonNameForm }
```

The OID for `emailUserOrgPersonNameForm` is 1 2 840 113533 7 69 4

5.5 VPN Device Name Form

The `deviceVPN` name form is used to name entries of the `device` object class.

The specification of this name form is:

```
deviceVPNNameForm          NAME-FORM
NAMES                       device
WITH ATTRIBUTES             commonName
AND OPTIONALLY              serialNumber,
                             unstructuredAddress,
                             unstructuredName,
ID                           id-nsn-nf-deviceVPNNameForm }
```

The OID for `deviceVPNNameForm` is 1 2 840 113533 7 69 5

6. Structure Rules

The structure rules required for Entrust are expressed as the relationship between structural object classes. The necessary structure rules are expressed below:

1. The structural object class of the CA entry is not mandated however most organizations will use either the **organization** or **organizationalUnit** structural object class. The DIT structure must allow entries of structural object class **cRLDistributionPoint** and

organizationalPerson to be created beneath the CA entry.

2. Entrust defines the concept of a **Search Base** in order to identify name spaces within the DIT. The Search Base is defined as a non-leaf node within the DIT. The structural object class of the Search Base is not mandated however the DIT structure rules must allow end user entries to be created beneath Search Base entries. If end user entries are created with Entrust/Admin then the end user entries will be of structural object class **organizationalPerson**.
3. The VPN Connector product requires that end user entries are created as structural object class **device**. This implies that the DIT structure rules must allow entries of object class **device** to be created under the CA entry as well as the Search Base entries.