

Entrust Directory Schema Requirements

For Entrust 5.0

Author: Chris Oliva
Date: December 2000
Version: 3.0

© Copyright 2000-2003 Entrust. All rights reserved.

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc or Entrust Limited. All other company and product names are trademarks or registered trademarks of their respective owners.

© Copyright 2000-2003 Entrust. All rights reserved.

Revision History

Date	Comments	Version
November 1999	Original Version	2.0
February 2000	Fix minor errors	2.1
December 2000	Updated for Entrust/PKI™ 5.1	3.0

Table of Contents

1.	INTRODUCTION.....	1
2.	SCHEMA SUMMARY.....	1
3.	OBJECT CLASSES	4
3.1	ENTRUST POLICYOBJECT OBJECT CLASS.....	4
3.2	ENTRUST CA OBJECT CLASS.....	5
3.3	ENTRUST USER OBJECT CLASS	5
3.4	RFC 822MAILUSER OBJECT CLASS	6
3.5	EMAILADDRESSUSER OBJECT CLASS.....	6
3.6	UNIQUELYIDENTIFIEDUSER OBJECT CLASS.....	6
3.7	SIMPLEAUTHOBJECT OBJECT CLASS.....	7
3.8	ENTRUST NAMEDOBJECT OBJECT CLASS.....	7
3.9	UNIQUELYQUALIFIEDOBJECT OBJECT CLASS.....	8
3.10	ENTRUST ROAMINGUSER OBJECT CLASS	8
3.11	MSMAILUSER OBJECT CLASS.....	9
3.12	CCMAILUSER OBJECT CLASS.....	9
3.13	QMMAILUSER OBJECT CLASS.....	9
3.14	TRUST TYPES OBJECT CLASS.....	10
3.15	PKCS10DEVICE OBJECT CLASS	10
3.16	CEPDEVICE OBJECT CLASS.....	10
3.17	ENTRUST DNQUALIFIERUSER OBJECT CLASS.....	11
4.	ATTRIBUTES	11
4.1	ENTRUST POLICYCERTIFICATE ATTRIBUTE.....	11
4.2	ATTRIBUTE CERTIFICATE ATTRIBUTE.....	12
4.3	ENTRUST ROAMFILEENCINFO ATTRIBUTE.....	12
4.4	ENTRUST ROAMINGEOP ATTRIBUTE.....	13
4.5	ENTRUST ROAMINGPAB ATTRIBUTE	13
4.6	ENTRUST ROAMINGPROFILE ATTRIBUTE	13
4.7	ENTRUST ROAMINGPRV ATTRIBUTE.....	14
4.8	ENTRUST ROAMINGRECIPLIST ATTRIBUTE.....	14
4.9	ENTRUST ROAMINGSLA ATTRIBUTE.....	14
4.10	ENTRUST ROAMINGCAPAB ATTRIBUTE.....	15
4.11	MSMAILPOSTOFFICE ATTRIBUTE.....	15
4.12	MSMAILNETWORK ATTRIBUTE	16
4.13	MSMAILID ATTRIBUTE	16
4.14	MSMAILFULLNAME ATTRIBUTE.....	16
4.15	CCMAILPOSTOFFICE ATTRIBUTE.....	17
4.16	CCMAILNAME ATTRIBUTE.....	17
4.17	CCMAILCOMMENTS ATTRIBUTE.....	17
4.18	QMZONE ATTRIBUTE.....	18
4.19	QMMAILCENTER ATTRIBUTE.....	18
4.20	QMUSERNAME ATTRIBUTE	18
4.21	SMIMETRUST ATTRIBUTE.....	19
4.22	SSLTRUST ATTRIBUTE	19
4.23	OBJSIGNTRUST ATTRIBUTE.....	19

5.	NAME FORMS	20
5.1	UNIQUE PERSON NAME FORM	20
5.2	UNIQUE ORGANIZATIONAL PERSON NAME FORM	20
5.3	UNIQUE RESIDENTIAL PERSON NAME FORM	20
5.4	EMAIL USER ORGANIZATIONAL PERSON NAME FORM	21
5.5	VPN DEVICE NAME FORM	21
5.6	ENTRUST CEP DEVICE NAME FORM	21
5.7	ENTRUST PKCS 10 DEVICE	22
6.	STRUCTURE AND CONTENT RULES	22
7.	SCHEMA ISSUES	24
7.1	ATTRIBUTE CERTIFICATE	24

1. Introduction

This document describes the schema required for directory interoperability with Entrust/ PKI™ 5.0¹ and Entrust-Ready™ products. More detailed descriptions of directory requirements and directory integration issues are available in associated white papers from Entrust².

Products that 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 that will allow the equivalent implementation of the recommended Name Forms (users of Entrust/PKI are free to implement any Name Forms regardless of the definitions contained within this document).

2. Schema Summary

This section provides a table reference that lists all the object classes and attributes used by the Entrust software. The table groups the schema elements according to specific product solutions. For example, The “MSMail™ Components” are only required by the integrated MS Mail solution however “Core Schema Components” are required by all Entrust solutions including the Entrust/PKI product.

The tables represent the minimum schema configuration required for Entrust and does not preclude the use of additional schema elements. Standard schema definitions are not included within this document but are referenced. The “LDAP Name” column specifies alternate names required for LDAP servers (the LDAP Name is only specified if it differs from the attribute name in the first column). The “Requirement” column is used to describe whether the schema item is mandatory or optional. There are three possible categories for the “Requirement” field:

Mandatory

The Entrust software requires this item.

Default

The default configuration of the Entrust software requires this item.

Optional

The item is not directly used by the Entrust software. The item is included as a convenience for the implementation of the directory schema.

Items new to Entrust/PKI 5.0 are indicated with the ✓ symbol.

¹ Version 3.0 of this document is updated for Entrust/PKI 5.1.

² Please visit <http://www.entrust.com/resourcecenter/whitepapers.htm> for other Entrust white papers.

Object Classes

Object Class	Defined In	Requirement	New Item
Core Schema Components			
cRLDistributionPoint	X.521 / RFC 2256	Mandatory	
organizationalRole	X.521 / RFC 2256	Mandatory	✓
EntrustPolicyObject	Entrust Schema Document	Default	✓
pkiCA	X.509 (2000) / RFC 2587	Default	✓
entrustCA	Entrust Schema Document	Default	
pkiUser	X.509 (2000) / RFC 2587	Default	✓
pkiUser	X.509 (2000)	Default	✓ (5.1)
entrustUser	Entrust Schema Document	Default	
person	X.521 / RFC 2256	Default	
organizationalPerson	X.521 / RFC 2256	Default	
rfc822MailUser	Entrust Schema Document	Default	
emailAddressUser	Entrust Schema Document	Default	
organizationalUnit	X.521 / RFC 2256	Default	
applicationProcess	X.521 / RFC 2256	Default	✓
uniquelyIdentifiedUser	Entrust Schema Document	Default	
simpleAuthObject	Entrust Schema Document	Optional	
entrustNamedObject	Entrust Schema Document	Optional	✓
entrustDnQualifierUser	Entrust Schema Document	Optional	✓
uniquelyQualifiedObject	Entrust Schema Document	Optional	✓
Entrust/Roaming Solution			
entrustRoamingUser	Entrust Schema Document	Mandatory	✓
MS Mail Components			
msMailUser	Entrust Schema Document	Mandatory	
CC Mail Components			
ccMailUser	Entrust Schema Document	Mandatory	
Quick Mail Components			
qmMailUser	Entrust Schema Document	Mandatory	
Entrust-Ready Netscape Components			
trustTypes	Entrust Schema Document	Mandatory	
Entrust/VPN Connector Components			
pKCS10Device	Entrust Schema Document	Mandatory	
cEPDevice	Entrust Schema Document	Mandatory	

Attributes

Attribute Type	LDAP Name	Defined In	Requirement	New Item
Core Schema Components (common to all products)				
userCertificate (v3)		X.509 (1997) / RFC 2256	Mandatory	
cACertificate		X.509 (1997) / RFC 2256	Mandatory	
certificateRevocationList (v2)		X.509 (1997) / RFC 2256	Mandatory	
authorityRevocationList		X.509 (1997) / RFC 2256	Mandatory	
crossCertificatePair		X.509 (1997) / RFC 2256	Mandatory	
entrustPolicyCertificate		Entrust Schema Document	Mandatory	✓
commonName	cn	X.520 / RFC 2256	Mandatory	
objectClass		X.501 / RFC 2256	Mandatory	
userPassword		X.509 (1997) / RFC 2256	Optional	
attributeCertificateAttribute		X.509	Default ³	✓(5.1)
attributeCertificate		Entrust Schema Document	Mandatory ⁴	
surname	sn	X.520 / RFC 2256	Default	
serialNumber		X.520 / RFC 2256	Default	
rfc822Mailbox	mail	RFC 1274	Default ⁵	
emailAddress	email	PKCS #9	Default	
countryName	c	X.520 / RFC 2256	Default	
organizationName	o	X.520 / RFC 2256	Default	
organizationalUnitName	ou	X.520 / RFC 2256	Default	
description		X.520 / RFC 2256	Default	✓
Entrust/Roaming Solution				
entrustRoamFileEncInfo		Entrust Schema Document	Mandatory	✓
entrustRoamingEOP		Entrust Schema Document	Mandatory	✓
entrustRoamingPAB		Entrust Schema Document	Mandatory	✓
entrustRoamingProfile		Entrust Schema Document	Mandatory	✓
entrustRoamingPRV		Entrust Schema Document	Mandatory	✓
entrustRoamingRecipList		Entrust Schema Document	Mandatory	✓
entrustRoamingSLA		Entrust Schema Document	Mandatory	✓
entrustRoamingCAPAB		Entrust Schema Document	Mandatory	✓
userID	uid	RFC 1274	Default	✓
MS Mail Components				
msMailPostoffice		Entrust Schema Document	Mandatory	
msMailNetwork		Entrust Schema Document	Mandatory	
msMailId		Entrust Schema Document	Mandatory ⁶	

³ The attributeCertificateAttribute attribute is used for the Attribute Authority feature new to Entrust 5.1. The PKI must be configured to use this attribute name. See section 7.1 for more information.

⁴ The attributeCertificate attribute is Mandatory for backwards compatibility with Entrust 4.x or earlier products.

⁵ The rfc822Mailbox attribute is Mandatory for Entrust/Express for Lotus Notes.

⁶ msMailId is also optionally required for Entrust/Express for Microsoft Outlook and Microsoft Exchange.

msMailFullName		Entrust Schema Document	Mandatory	
CC Mail Components				
ccMailPostoffice		Entrust Schema Document	Mandatory	
ccMailName		Entrust Schema Document	Mandatory	
ccMailComments		Entrust Schema Document	Mandatory	
Quick Mail Components				
qmZone		Entrust Schema Document	Mandatory	
qmMailCenter		Entrust Schema Document	Mandatory	
qmUserName		Entrust Schema Document	Mandatory	
Entrust-Ready Netscape Components				
smimetrust		Entrust Schema Document	Mandatory	
ssltrust		Entrust Schema Document	Mandatory	
objsigntrust		Entrust Schema Document	Mandatory	
Entrust/VPN Connector Components				
unstructuredName		PKCS #9	Mandatory	
unstructuredAddress		PKCS #9	Mandatory	

3. Object Classes

The specifications for Entrust-defined object classes are included below, expressed in the same ASN.1 notation as the object classes defined in X.521.

3.1 *entrustPolicyObject* Object Class

The **entrustPolicyObject** object class is used to extend the schema for objects which contain policy information. The affected objects in the directory include the CA, which acts as the policy distribution point, and the policy objects created beneath the CA (one policy object is created for each Role defined in the PKI; these entries are created with the **organizationalRole** structural object class).

```

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

The OID for **id-nsn-oc-entrustPolicyObject** is 1 2 840 113533 7 67 17

3.2 *entrustCA Object Class*

The **entrustCA** auxiliary object class is used to configure directory entries representing Entrust/Authority Certification Authorities. Alternatively, the **pkiCA** auxiliary object class may be used instead of **entrustCA** as long as the **attributeCertificate** attribute is not required for backwards compatibility with Entrust 4.x or earlier products.

The **entrustCA** or **pkiCA** object classes are only required to allow their associated attributes to be added to the indicated entries. If the directory product supports other mechanisms for controlling schema content then the use of these object classes is not mandatory. If their use is needed then one or both of **entrustCA** and **pkiCA** must be added to the CA entry before Entrust/PKI initialization.

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 **id-nsn-oc-entrustCA** is 1 2 840 113533 7 67 1

3.3 *entrustUser Object Class*

The **entrustUser** object class is used to identify directory entries which are managed by Entrust/Authority. This value will be added to the **objectClass** attribute when the object represented by that entry is first issued a certificate by Entrust/Authority. The value will be present for the entire time that the object has credentials managed by 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 **id-nsn-oc-entrustUser** is 1 2 840 113533 7 67 0

3.4 *rfc822MailUser Object Class*

The **rfc822MailUser** object class is used to allow the **rfc822Mailbox** attribute to be added to an entry.

The specification of this object class is:

```
rfc822MailUser OBJECT-CLASS ::= {  
    SUBCLASS OF { top }  
    KIND auxiliary  
    MAY CONTAIN { rfc822Mailbox } – from RFC 1274 - refers to LDAP “mail” attribute  
    ID id-nsn-oc-rfc822MailUser }
```

The OID for **id-nsn-oc-rfc822MailUser** is 1 2 840 113533 7 67 7

3.5 *emailAddressUser Object Class*

The **emailAddressUser** object class is used to the PKCS9 **emailAddress** attribute to be added to an entry.

The specification of this object class is:

```
emailAddressUser OBJECT-CLASS ::= {  
    SUBCLASS OF { top }  
    KIND auxiliary  
    MAY CONTAIN { emailAddress } – from PKCS #9 - refers to LDAP “email” attribute  
    ID id-nsn-oc-emailAddressUser }
```

The OID for **id-nsn-oc-emailAddressUser** is 1 2 840 113533 7 67 9

3.6 *uniquelyIdentifiedUser 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 ::= {
```

AUXILIARY
SUBCLASS OF { top }
MUST CONTAIN { serialNumber }
ID id-nsn-oc-uniquelyIdentifiedUser }

The OID for id-nsn-oc-uniquelyIdentifiedUser is 1 2 840 113533 7 67 4

3.7 simpleAuthObject Object Class

The **simpleAuthObject** object class is used to allow an entry to contain a **userPassword** attribute. This object class is not used by Entrust software and is only provided for user convenience.

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 id-nsn-oc-simpleAuthObject is 1 2 840 113533 7 67 5

3.8 entrustNamedObject Object Class

The **entrustNamedObject** object class is used to allow a series of useful attributes commonly used for naming to be included in an entry. This object class is not used by Entrust software but is provided for convenience.

entrustNamedObject OBJECT-CLASS ::= {
SUBCLASS OF {top}
KIND auxiliary
MAY CONTAIN { name |
commonName |
surname |
givenName |
initials |
generationQualifier |
countryName |
localityName |
stateOrProvinceName |
organizationName |
organizationalUnitName |

```
        title |
        domainComponent | -- from RFC 1274 – refers to LDAP “dc” attribute
        dmdName }
ID      id-nsn-oc-entrustNamedObject }
```

The OID for `id-nsn-oc-entrustNamedObject` is 1 2 840 113533 7 67 15

3.9 uniquelyQualifiedObject Object Class

The `uniquelyQualifiedObject` object class is provided for convenience to allow users to include attributes in entries which can be used to uniquely qualify an object.

```
uniquelyQualifiedObject OBJECT-CLASS ::= {
    SUBCLASS OF {top}
    KIND        auxiliary
    MAY CONTAIN { serialNumber |
                dnQualifier |
                userId | -- from RFC 1274 - refers to LDAP “uid” attribute
                rfc822Mailbox | -- from RFC 1274 - refers to LDAP “mail” attribute
                description}
ID            id-nsn-oc-uniquelyQualifiedObject }
```

The OID for `id-nsn-oc-uniquelyQualifiedObject` is 1 2 840 113533 7 67 16

3.10 entrustRoamingUser Object Class

This object class is used to identify a user as being a roaming user.

```
entrustRoamingUser OBJECT-CLASS ::= {
    SUBCLASS OF {top}
    KIND        auxiliary
    MAY CONTAIN {entrustRoamFileEnclInfo |
                entrustRoamingProfile |
                entrustRoamingPAB |
                entrustRoamingRecipList |
                entrustRoamingSLA |
                entrustRoamingPRV |
                entrustRoamingEOP |
                entrustRoamingCAPAB|
                userId – from RFC 1274 – refers to LDAP “uid” attribute}
ID id-nsn-oc-entrustRoamingUser }
```

The OID for `id-nsn-oc-entrustRoamingUser` is 1 2 840 113533 7 67 13

3.11 msMailUser Object Class

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

The specification of this object class is:

```
msMailUser    OBJECT-CLASS ::= {  
    SUBCLASS OF { top }  
    KIND        auxiliary  
    MAY CONTAIN { msMailFullname |  
                msMailId |  
                msMailNetwork |  
                msMailPostoffice }  
    ID          id-nsn-oc-msMailUser }
```

The OID for **id-nsn-oc-msMailUser** is 1 2 840 113533 7 67 3

3.12 ccMailUser 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:

```
ccMailUser    OBJECT-CLASS ::= {  
    SUBCLASS OF { top }  
    KIND        auxiliary  
    MAY CONTAIN { ccMailComments |  
                ccMailName |  
                ccMailPostoffice }  
    ID          id-nsn-oc-ccMailUser }
```

The OID for **id-nsn-oc-ccMailUser** is 1 2 840 113533 7 67 2

3.13 qmMailUser 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 `id-nsn-oc-qmMailUser` is 1 2 840 113533 7 67 6

3.14 *trustTypes 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 `id-nsn-oc-trustTypes` is 1 2 840 113533 7 67 8

3.15 *pKCS10Device Object Class*

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

The specification of this object class is:

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

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

3.16 *cEPDevice Object Class*

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

The specification of this object class is:

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

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

3.17 *entrustDNQualifierUser Object Class*

The **entrustDNQualifierUser** object class is not used by Entrust software; it is provided for convenience so that the **dnQualifier** attribute can be added to an entry.

The specification of this object class is:

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

The OID for entrustDNQualifierUser is 1 2 840 113533 7 67 14

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 defined elsewhere, a reference is included to the authoritative source for that syntax specification.

4.1 *entrustPolicyCertificate Attribute*

The **entrustPolicyCertificate** attribute is included to replace the **attributeCertificate** attribute for Entrust v5.0 products. It contains policy information and is contained within role specific policy entries.

The syntax of this attribute is an Entrust specific opaque DER encoded CA-signed syntax. For schema configuration purposes, the syntax is defined in a generic manner:

```
entrustPolicyCertificate ATTRIBUTE ::= {  
    WITH SYNTAX          OCTET STRING  
    ID id-nsn-at-entrustPolicyCertificate }
```

The OID for `id-nsn-at-entrustPolicyCertificate` is 1 2 840 113533 7 68 30

4.2 *attributeCertificate Attribute*

Note that the attribute definition in this section defines an early version of the attribute certificate used by early versions of Entrust. This attribute is superseded by the standard definition. For more discussion on this attribute and which definition should be used, please see section 7.1.

The specification of this attribute is:

```
attributeCertificate          ATTRIBUTE ::= {  
    WITH SYNTAX          AttributeCertificate  
    ID                    id-nsn-at-attributeCertificate }
```

```
AttributeCertificate ::= SIGNED {AttributeCertificateInfo}
```

```
AttributeCertificateInfo ::= SEQUENCE {  
    owner CHOICE {  
        baseCertificateID [0] IssuerSerial,  
        entityName [1] Name } -- set to CA Name  
    issuer Name, -- issuer name  
    Number CertificateSerialNumber,  
    validity Validity,  
    attributes SEQUENCE OF Attribute,  
    issuerUniqueID UniqueIdentifier OPTIONAL }
```

The OID for `attributeCertificate` is 1 2 840 113533 7 68 10

4.3 *entrustRoamFileEnclInfo Attribute*

This attribute is used to specify information about the key used to encrypt the roaming user's profile. This attribute must support unbounded maximum sizes. Substring and ordering matching rules are not required.

Current sizing estimates place this attribute size between 800bytes and 2Kbytes.

```
entrustRoamFileEnclInfo ATTRIBUTE ::= {  
    WITH SYNTAX          OCTET STRING  
    EQUALITY MATCHING RULE    octetStringMatch  
    ID id-nsn-at-entrustRoamFileEnclInfo }
```

The OID for `id-nsn-at-entrustRoamFileEnInfo` is 1 2 840 113533 7 68 22

4.4 *entrustRoamingEOP Attribute*

This attribute is used to store a user's Entrust Options File (EOP file) encrypted with a symmetric key. This attribute must support unbounded maximum sizes. Substring and ordering matching rules are not required.

Current sizing estimates place this attribute size between 2 Kbytes and 8 Kbytes.

```
entrustRoamingEOP ATTRIBUTE ::= {  
    WITH SYNTAX                OCTET STRING  
    EQUALITY MATCHING RULE     octetStringMatch  
    ID id-nsn-at-entrustRoamingEOP }
```

The OID for `id-nsn-at-entrustRoamingEOP` is 1 2 840 113533 7 68 28

4.5 *entrustRoamingPAB Attribute*

This attribute is used to store a user's Personal Address Book encrypted with a symmetric key. This attribute must support unbounded maximum sizes. Substring and ordering matching rules are not required.

Current sizing estimates place this attribute size at 5 Kbytes per Personal Address Book entry for a given user.

```
entrustRoamingPAB ATTRIBUTE ::= {  
    WITH SYNTAX                OCTET STRING  
    EQUALITY MATCHING RULE     octetStringMatch  
    ID id-nsn-at-entrustRoamingPAB }
```

The OID for `id-nsn-at-entrustRoamingPAB` is 1 2 840 113533 7 68 24

4.6 *entrustRoamingProfile Attribute*

This attribute is used to store a user's Entrust Profile (EPF) encrypted with a symmetric key. This attribute must support unbounded maximum sizes. Substring and ordering matching rules are not required.

Current sizing estimates place this attribute size at 9 Kbytes. This attribute is expected to grow by approximately 2 Kbytes each time a user's keys roll over.

```
entrustRoamingProfile ATTRIBUTE ::= {  
    WITH SYNTAX                OCTET STRING  
    EQUALITY MATCHING RULE     octetStringMatch  
    ID id-nsn-at-entrustRoamingProfile }
```

The OID for `id-nsn-at-entrustRoamingProfile` is **1 2 840 113533 7 68 23**

4.7 *entrustRoamingPRV Attribute*

This attribute is used to store a user's PRV file encrypted with a symmetric key. This attribute must support unbounded maximum sizes. Substring and ordering matching rules are not required.

Current sizing estimates place this attribute size at approximately 3 Kbytes per Common Key group for which the user is a member.

```
entrustRoamingPRV ATTRIBUTE ::= {  
    WITH SYNTAX                OCTET STRING  
    EQUALITY MATCHING RULE     octetStringMatch  
    ID id-nsn-at-entrustRoamingPRV }
```

The OID for `id-nsn-at-entrustRoamingPRV` is **1 2 840 113533 7 68 27**

4.8 *entrustRoamingRecipList Attribute*

This attribute is used to store a user's recipient lists (user's ERL file) encrypted with a symmetric key. This attribute must support unbounded maximum sizes. Substring and ordering matching rules are not required.

Current sizing estimates place this attribute size at 5 Kbytes per entry in a Recipient List for a given user.

```
EntrustRoamingRecipList ATTRIBUTE ::= {  
    WITH SYNTAX                OCTET STRING  
    EQUALITY MATCHING RULE     octetStringMatch  
    ID id-nsn-at-entrustRoamingRecipList }
```

The OID for `id-nsn-at-entrustRoamingRecipList` is **1 2 840 113533 7 68 25**

4.9 *entrustRoamingSLA Attribute*

This attribute is used to store a user's Single Login Application list (SLA file) encrypted with a symmetric key. This attribute must support unbounded maximum sizes. Substring and ordering matching rules are not required.

Current sizing estimates place this attribute size at 4 Kbytes per Entrust-Ready application for a given user.

```
entrustRoamingSLA ATTRIBUTE ::= {  
    WITH SYNTAX                OCTET STRING  
    EQUALITY MATCHING RULE     octetStringMatch  
    ID id-nsn-at-entrustRoamingSLA }
```

The OID for `id-nsn-at-entrustRoamingSLA` is 1 2 840 113533 7 68 26

4.10 *entrustRoamingCAPAB Attribute*

This attribute is used to store a user's CA PAB encrypted with a symmetric key. This attribute must support unbounded maximum sizes. Substring and ordering matching rules are not required.

Current sizing estimates place this attribute size at 3 Kbytes per CA certificate imported into a given user's CA PAB.

```
entrustRoamingCAPAB ATTRIBUTE ::= {  
    WITH SYNTAX                OCTET STRING  
    EQUALITY MATCHING RULE     octetStringMatch  
    ID id-nsn-at-entrustRoamingCAPAB }
```

The OID for `id-nsn-at-entrustRoamingCAPAB` is 1 2 840 113533 7 79 0

4.11 *msMailPostoffice 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 `id-nsn-at-msMailPostoffice` is 1 2 840 113533 7 68 9

4.12 msMailNetwork 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 **id-nsn-at-msMailNetwork** is 1 2 840 113533 7 68 8

4.13 msMailID 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 **id-nsn-at-msMailId** is 1 2 840 113533 7 68 7

4.14 msMailFullname 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 **id-nsn-at-msMailFullname** is 1 2 840 113533 7 68 6

4.15 ccMailPostoffice 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 **id-nsn-at-ccMailPostoffice** is 1 2 840 113533 7 68 3

4.16 ccMailName 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 **id-nsn-at-ccMailName** is 1 2 840 113533 7 68 2

4.17 ccMailComments 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 **id-nsn-at-ccMailComments** is 1 2 840 113533 7 68 4

4.18 qmZone Attribute

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 **id-nsn-at-qmZone** is 1 2 840 113533 7 68 14

4.19 qmMailCenter Attribute

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

The specification of this attribute is:

```
qmMailCenter    ATTRIBUTE ::= {  
    WITH SYNTAX          DirectoryString { 13 }  
    EQUALITY MATCHING RULE caseIgnoreMatch  
    SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch  
    ID                   id-nsn-at-qmMailCenter }
```

The OID for **id-nsn-at-qmMailCenter** is 1 2 840 113533 7 68 13

4.20 qmUserName Attribute

The **qmUserName** attribute is used to store a QuickMail user's name in their Directory entry.

The specification of this attribute is:

```
qmUserName      ATTRIBUTE ::= {  
    WITH SYNTAX          DirectoryString { 31 }  
    EQUALITY MATCHING RULE caseIgnoreMatch  
    SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch  
    ID                   id-nsn-at-qmUserName }
```

The OID for **id-nsn-at-qmUserName** is 1 2 840 113533 7 68 12

4.21 smimeTrust 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 **id-nsn-at-smimetrust** is **1 2 840 113533 7 68 17**

4.22 sslTrust 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 **id-nsn-at-ssltrust** is **1 2 840 113533 7 68 18**

4.23 objSignTrust 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 **id-nsn-at-objsigntrust** is **1 2 840 113533 7 68 19**

5. Name Forms

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. This name form is recommended by Entrust but is not required.

The specification of this name form is:

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

The OID for `id-nsn-nf-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. This name form is recommended by Entrust but is not required.

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 `id-nsn-nf-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. This name form is recommended by Entrust but is not required.

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 id-nsn-nf-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. This name form is included for backwards compatibility with S/MIME v2.

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 id-nsn-nf-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 id-nsn-nf-deviceVPNNameForm is 1 2 840 113533 7 69 5

5.6 Entrust CEP Device Name Form

This name form is required for interoperability with cisco routers that require device entries to be named with the unstructuredName, serialNumber and the unstructuredAddress attributes.

The definition of the name form is:

```
EntrustCEPDeviceNameForm NAME-FORM ::= {  
    NAMES                device  
    WITH ATTRIBUTES      { UnstructuredName }  
    AND OPTIONALLY       { UnstructuredAddress |  
                          serialNumber }  
    ID                    Entrust-NameForm-EntrustCEPDeviceNameForm }
```

The OID for EntrustCEPDeviceNameForm is **2 16 840 1 114027 20 1**

5.7 Entrust PKCS 10 Device

This name form is required for interoperability with cisco routers that require device entries to be named with **commonName**, **serialNumber** and **description** attributes.

The definition of the name form is:

```
EntrustPKCS10DeviceNameForm NAME-FORM ::= {  
    NAMES                device  
    WITH ATTRIBUTES      { commonName }  
    AND OPTIONALLY       { serialNumber |  
                          description }  
    ID                    Entrust-NameForm-EntrustPKCS10DeviceNameForm }
```

The OID for EntrustPKCS10DeviceNameForm is **2 16 840 1 114027 20 2**

6. Structure and Content Rules

The structure and content rules required for Entrust are explained below. Specific content required before Entrust/PKI initialization is detailed:

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 directory schema must allow the CA entry to contain the following attributes: **caCertificate**, **certificateRevocationList**, **crossCertificatePair**, and **authorityRevocationList**. The **pkiCA** object class can optionally be used to extend the schema of the CA entry for this purpose.

The CA entry must be added before initializing the Entrust/PKI. If required, the **pkiCA** object class must also be added to the entry.

2. For backwards compatibility with Entrust 4.x or earlier products, the CA entry must also contain the **attributeCertificate** attribute. In this configuration, the **entrustCA** object class can optionally be used to extend the schema of the CA entry.

If required, the **entrustCA** object class must be added to the CA entry before initializing the Entrust/PKI.

3. The CA will bind to the directory using the DN of its directory entry as the bind DN. The CA will perform simple authentication therefore the CA must have a password and write/modify access configured in the directory. Many products associate the authentication password with the **userPassword** attribute. In this case, the CA entry must contain the **userPassword** attribute. The **simpleAuthObject** object class can optionally be used to extend the schema of the CA entry for this purpose.

The CA entry must be configured with appropriate bind credentials and access control privileges before installing the Entrust/PKI.

4. Entrust RA (and other administrative products) will use the credentials of the Directory Administrator to bind to the directory using simple authentication. This will allow administrators to create and modify directory entries which represent Entrust user end-entities. This requires the directory to be configured with a DN and password for the Directory Administrator. It is not necessary for the Directory Administrator to be represented by an entry in the directory.

The Directory Administrator must be configured with appropriate bind credentials and access control privileges before installing the Entrust/PKI.

5. The CA entry will act as the policy distribution point for the PKI. This requires the CA entry to contain the **entrustPolicyCertificate** attribute. The **entrustPolicyObject** object class will be used to extend the schema of the CA entry for this purpose.
6. The DIT structure rules must allow entries of structural object class **cRLDistributionPoint**, **organizationalPerson** and **organizationalRole** to be created beneath the CA entry.
7. Policy objects will be created beneath the CA entry with a structural object class of **organizationalRole**. These entries must be able to contain the **entrustPolicyCertificate** attribute and **entrustPolicyObject** object class.
8. 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 default configuration of Entrust/RA will allow **organizationalUnit** entries to be created for this purpose. The default configuration of Entrust/PKI uses the CA entry as the initial Search Base.

9. The DIT structure rules must allow end user entries to be created beneath Search Base entries. If Person entries are created with Entrust/RA then the default structural object class of end user entries will be **organizationalPerson**. If Web Server entries are created with Entrust/RA, the default structural object class is **applicationProcess**. The default configuration for Entrust/RA can be changed to accommodate any entry type that may be required.
10. Entrust RA will use the **commonName** attribute to name entries. For Person entries, the default configuration will allow the **serialNumber** attribute to be added as part of the entry name (i.e. as a distinguished value). The default configuration can be changed to accommodate any naming requirements that may be necessary.
11. The CA will issue certificates to end users. The public key encryption certificate will be added by the CA to end-user entries in the **userCertificate** attribute. The default configuration of the CA will add the **entrustUser** and **pkiUser** object classes to end user entries.
12. The CA will (optionally) issue Attribute Certificates to end users. This will be added to the entry in the **attributeCertificateAttribute** attribute. The default configuration of the CA will add the **pmiUser** object class to the end user entry.
13. The Entrust/VPN Connector product requires that end entity directory entries are created with the **device** structural object class. The DIT structure rules must these entries to be created under the CA entry as well as the Search Base entries. The directory must allow these end entities to contain the **pKCS10Device** and **cEPDevice** auxiliary object classes as well as the **serialNumber**, **unstructuredName** and **unstructuredAddress** attributes.

7. Schema Issues

This section discusses schema implementation issues.

7.1 Attribute Certificate

Early version of Entrust (before 5.0) used an attribute called “attributeCertificate” to store policy information. This attribute is only used in the directory entry for the Certification Authority. The auxiliary object class which allows this attribute to be added to any entry is the **entrustCA** object class.

As of Entrust 5.0, policy information is published to a new attribute defined as “entrustPolicyCertificate”. For backwards compatibility with old clients (before release 5.0) the **attributeCertificate** is still required; if backwards compatibility with the old clients is not required, then the **attributeCertificate** is not needed.

The X.509 standard defines an attribute called “attributeCertificateAttribute”. This attribute is used to publish attribute information about a user and especially for an Attribute Authority to assign privileges. The auxiliary object class which allows this attribute to be added to any entry is the pmiUser object class. At the time of publication of this document, these schema items are defined in X.509 as well as the current working internet draft:

<http://www.ietf.org/internet-drafts/draft-ietf-pkix-ldap-schema-01.txt>

Entrust/PKI 5.1 has the ability to use issue Attribute Certificates but must be configured to use the “attributeCertificateAttribute” attribute.