Entrust Technologies White Paper

Entrust Directory Requirements

Author: Sharon Boeyen
Date: May 1997
Version: 1.0

1. Introduction

Entrust® is a family of network security products. Designed to be the single security infrastructure for organizations, Entrust provides numerous security services to system administrators, network users, and applications. In particular, Entrust provides automatic and transparent key management so that neither developers nor end-users need to understand the details of cryptography to take advantage of Entrust security services.

One component of an Entrust Public Key Infrastructure (PKI) is a repository, or Directory, to make the public key certificates and Certificate Revocation Lists (CRL) available to the users of that infrastructure. In the context of this paper, a directory system providing the PKI repository will be referred to as “the Directory". The Directory is comprised of entries named with Distinguished Names (DN) as defined in ITU-T Recommendation X.501 (1997) | ISO/IEC 9594-2:1997.

This paper outlines the minimum and very basic requirements for a Directory for Entrust release 3.0. There are many directory products currently available from a variety of vendors, which satisfy these requirements.

Depending on the scale of the PKI deployment, the supported applications and the operating environment, other considerations need to be addressed when selecting a directory system for a particular deployment. These may include aspects of distributed directory services, replication, support for standard server-server protocols, such as those defined in the X.500 Series of Recommendations, and others. As these are not part of the basic requirements for a directory system working with Entrust, and may vary greatly from one deployment to another, these are outside the scope of this paper.

This paper can be used by vendors of directory products to examine the suitability of their offerings for an Entrust PKI. This paper may also be used by organizations considering deployment of an Entrust PKI to assess their existing directory systems as well as directory products they may be considering acquiring, with respect to their suitability as the PKI repository. It is assumed that the reader is already familiar with the Entrust product architecture and the Entrust components which interact with the Directory.

Future releases of Entrust may place additional requirements on a directory.

1.1 Conventions

A number of Abstract Syntax Notation One (ASN.1) data types, defined elsewhere, are included in this paper. All ASN.1 elements can be distinguished from other text by their style, **as illustrated here**.

Frequent reference to parts of the X.500 Series of Recommendations and ISO/IEC International Standard appear in this paper. Rather than include the formal reference for each, the ITU-T Recommendation number is used. Unless otherwise specified, this represents the 1997 specification of that specification. For example an occurrence of "X.509" should be interpreted as ITU-T X.509 (1997) | ISO/IEC 9594-8:1997. The complete multi-part standard is referred to as the X.500 Series of Specifications.

2. Functional Model

In an Entrust PKI, Entrust/Manager™, Entrust/Admin™, and Entrust client applications require access to the Directory.

Entrust/Manager represents the Certification Authority (CA) in an Entrust system. Entrust/Manager accesses the Directory to:

- modify its own directory entry (add/delete cross-certificates and revocation lists);
- modify Entrust users' directory entries (i.e. add/delete certificates and add "entrustUser" to object class);
- create directory entries for Certificate Revocation List (CRL) distribution points;
- retrieve data from its own directory entry, verify existence of user entries, etc.

Entrust/Admin enables Security Officers, Entrust Administrators, and Directory Administrators to perform various administrative tasks in the system. Entrust/Admin accesses the Directory to:

- locate entries for purposes of Entrust administration;
- manage Directory entries for purposes of Directory and Entrust administration (e.g. add/delete user and CA entries, modify entry information which is not PKI-related, etc.).

Entrust client applications represent the end-users in an Entrust system. Entrust client applications, such as Entrust/Client™ and applications built using Entrust/Toolkit™ access the Directory to:

- retrieve information required at Entrust login (the user's certificate, and associated CRL);
- perform base object searches to:
    - retrieve encryption public key certificates for other user entries;
    - retrieve CRLs associated with other users’ certificates;
    - retrieve cross-certificates for other CAs in certificate chains;
    - retrieve Authority Revocation Lists (ARLs) associated with other CAs in certificate chains;
    - retrieve CA search base information from the attribute certificate. This search base indicates the points (directory entries) in the Directory from which searches for certificates are to be started.

Entrust client applications may also access the Directory to perform subtree searches to locate user entries for subsequent certificate retrieval. While a "base object search" checks only the directory entry for which the Distinguished Name (DN) is provided, a "subtree" search checks the named entry and entries which are named subordinate to that entry and which satisfy the bounds indicated for the subtree.

In particular, certificates and CRLs are retrieved by Entrust/Engine™, the key management and cryptography engine common to all Entrust client applications, while subtree searches, if performed at all, are performed by the Entrust client application. For example:

- Entrust/Engine retrieves the current user's certificate, and associated CRL, at each login, and retrieves the certificates, cross-certificate pairs, if any, and associated revocation lists of other users when encrypting for those users or verifying other user's digital signatures.
- Entrust/Client allows users to search the directory for potential users in order to encrypt and/or sign data for those users. Once potential users are located, their DNs are passed to Entrust/Engine for subsequent certificate and revocation list retrieval and the completion of the desired security operation. Applications built using Entrust/Toolkit may or may not perform directory searches; this depends on their requirements. Entrust/ICE™ in "My Eyes Only" mode is an example of an application that performs no subtree searches: all directory access is in the form of base object searches performed by Entrust/Engine.

3. Protocol

The protocol used by the Entrust components to access the services provided by a Directory system is the Lightweight Directory Access Protocol (LDAP), version 2, as specified in Internet RFC 1777. This specification can be found at http://ds.internic.net/rfc/rfc1777.txt.

The LDAP model is one where LDAP clients perform protocol operations against LDAP servers. The LDAP servers are then responsible for performing the necessary operations on the Directory and upon completion, returning a response to the LDAP client. In this model, the Entrust/Manager, Entrust/Admin, and Entrust client applications are acting as LDAP clients.

This paper addresses the requirements of LDAP servers to interact with, and satisfy the requirements of the Entrust components through their roles as LDAP clients. This paper does not specify requirements for the interface between the LDAP server and the specific product providing the underlying directory services, since this is not a concern for Entrust. Such directory systems may be fully compliant X.500 Directory System Agents (DSAs) or directories based on other technology. The required schema elements, directory naming issues and security requirements that need to be supported by the underlying directory system are included in this paper.

This section profiles the LDAP protocol and indicates which aspects are currently used by Entrust PKI components. However, it should be noted that future releases of Entrust could require support for additional parameters as well as additional operations not currently used.

Entrust does not place trust in the Directory. All data used for security is signed and the trust model is built using information without needing a trusted network.

3.1 Transport Protocol

Support for LDAP v2 over TCP transport, as defined in Section 3.1 of RFC 1777, is required.

3.2 Required LDAP Operations

3.2.1 Bind and Unbind

Entrust/Manager, Entrust/Admin and Entrust client applications make use of the LDAP Bind and Unbind operations.

The **BindRequest**, **BindResponse** and **UnbindRequest** are required to be supported. On the **BindRequest**, the LDAP version is set to **(v2)**. Only the "simple" authentication level is currently used by the Entrust components. Entrust client applications bind anonymously to the Directory (with a zero-length string for the password parameter of the simple authentication parameter). Entrust/Manager and Entrust/Admin both bind by supplying a Distinguished Name (DN) and password.

As Entrust/Client may access the Directory at the same time as Entrust/Manager and/or Entrust/Admin, the Directory must be able to support both anonymous and password-based bindings simultaneously.

3.2.2 Search

Entrust/Manager, Entrust/Admin and Entrust client applications all make use of the LDAP Search operation. To support the types of searches performed by these components, all aspects of the search request and search result must be supported, with the following exception:

- in the **derefAliases** parameter, only the **neverDerefAliases** option is currently used by Entrust. The **derefInSearching**, **derefFindingBaseObj**, and **derefAlways** are not currently used.

3.2.3 Modify

Entrust/Manager and Entrust/Admin make use of the LDAP Modify operation. To support the types of operations currently performed by these components, all aspects of the modify request and modify result must be supported, with the following exception:

- in the operation parameter, only the “add” and “delete” modes are currently used by Entrust. The “replace” mode is not currently used.

3.2.4 Add

Entrust/Manager and Entrust/Admin make use of the LDAP Add operation. To support the types of operations currently performed by these components, all aspects of the add request and add result must be supported.

3.2.5 Delete

Entrust/Manager and Entrust/Admin make use of the LDAP Delete operation. To support the types of operations currently performed by these components, all aspects of the delete request and delete result must be supported.

3.3 Operations Not Used

The following LDAP operations are not currently used by the Entrust PKI components:

- Modify RDN
- Compare
- Abandon

Although these operations are not currently used by Entrust, future releases of Entrust may have additional requirements.

3.4 Specific Attribute Value Encodings

When conveyed in LDAP requests and results, attributes defined in the X.500 Series of Specifications are to be encoded using string representations defined in Internet RFC 1778, (String Representation of Standard Attribute Syntaxes). These string encodings are based on the attribute definitions from the 1988 edition of the X.500 Series of Specifications. Thus, the string representations of the attributes as listed below are for version 1 certificates and version 1 CRLs:

- **userCertificate** (RFC 1778 section 2.25)
- **cACertificate** (RFC 1778 section 2.26)
- **authorityRevocationList** (RFC 1778 section 2.27)
- **certificateRevocationList**, (RFC 1778 section 2.28)
- **crossCertificatePair** (RFC 1778 section 2.29)

Entrust uses version 3 certificates and version 2 revocation lists, as defined in X.509 (1997) and as such, the RFC 1778 string encoding of these attributes is inappropriate.

For this reason, Entrust encodes these attributes using a syntax similar to the syntax **Undefined** from section 2.1 of RFC 1778. Values of these attributes are encoded as if they were values of type **OCTET STRING**, with the string value of the encoding being the Distinguished Encoding Rule (DER)-

encoding of the value itself. For example, when writing a **userCertificate** to the directory, Entrust/Manager generates a DER-encoding of the certificate and uses that encoding as the value of the **userCertificate** attribute in the LDAP Modify request.

This encoding style is consistent with the encoding scheme proposed for LDAPv3, which is now being defined within the IETF and must be supported by the Directory.

4. Schema

Entrust requires that the Directory support a number of object classes and attributes. Most are defined in the X.500 Series of Specifications, specifically X.520/X.521 or X.509. X.501 also provides tools for additional schema elements to be defined, as required. Consistent with X.501, Entrust Technologies has defined some additional schema elements which are also required. These specifications are included in this paper.

The schema requirements are described in terms of the directory entries accessed and managed by the Entrust components. The X.500 Series of Specifications include two mechanisms for specifying the contents of directory entries: object class specification, and DIT content rule specification. In most cases, either of these may be used by the directory administrator to add the PKI attributes to entries. Exceptions, where a specific object class is required by Entrust, are indicated below.

In all cases, where certificates are referenced, the format is version 3 (v3) certificate and version 2 (v2) CRL, including certificate and CRL extensions, as defined in X.509. Entrust requires full support for these versions including support for a subset of the standard extensions and one private extension defined by Entrust Technologies in accordance with the standard tools defined for that purpose in X.509.

4.1 Certification Authority Entries

Entrust currently imposes no requirements on the CA entry object class content. The entry may have **organization**, **organizationalUnit**, **organizationalPerson**, **organizationalRole** or some other object class as the structural class of the entry. The placement of the entry in the DIT and its naming attribute(s) are not mandated by Entrust. However, it is required that the DN be unique and not be re-used at a later stage for some other CA.

The attributes defined in X.521 which are currently required to be supported for CA entries in an Entrust environment are:

- **objectClass**

- **userPassword**
- **cACertificate**
- **certificateRevocationList**
- **authorityRevocationList**
- **crossCertificatePair**

In addition, the **attributeCertificate** attribute, as defined below, needs to be supported for inclusion in CA entries.

```
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 value of **id-nsn-at-attributeCertificate**, the OID for **attributeCertificate** is:

```
1 2 840 113533 7 68 10
```

The **attributeCertificate** attribute is placed in the CA directory entry. Entrust populates the attributes element of **attributeCertificate** with the **entrustCAInfo** attribute defined below. The **entrustCAInfo** provides the search base for searching in the PKI repository for certificates and revocation lists in the CA domain.

```
entrustCAInfo ::= ATTRIBUTE {
            WITH SYNTAX             EntrustCAInfo
            ID                               id-nsn-at-entrustCAInfo }

EntrustCAInfo ::= SEQUENCE {
   version                 [0]      INTEGER DEFAULT 0
   searchBases     SEQUENCE OF SEQUENCE {
            searchBase                       Name,
            searchBaseName                   IA5STRING OPTIONAL }  OPTIONAL,
   cAFlags BIT STRING OPTIONAL }

searchBases         SEQUENCE OF SEQUENCE {
            searchBase                       Name,
            searchBaseName                   IA5STRING OPTIONAL }
```

The value of **id-nsn-at-entrustCAInfo**, the OID for **entrustCAInfo** is:

1 2 840 113533 7 68 0

As the standardization of attribute certificates and the associated infrastructure (in X.509 and in ASNI X9.57) evolves and converges to a single specification, future releases of Entrust will likely require support for that resulting standardized form of **attributeCertificate** rather than that defined here.

Certificates issued by Entrust include a number of extension fields as defined in X.509. All certificates will also contain an additional extension which indicates which Entrust release was used in issuing this certificate. This specification of this extension, defined using the standard specification technique from X.509, is provided below. As certificates will appear in both CA entries and Entrust user entries, this extension is relevant to the schema specification for both types of entries.

```
entrustVersInfo  EXTENSION  ::=
SYNTAX EntrustVersInfoSyntax
     IDENTIFIED BY  {id-nsn-ext 0}

EntrustVersInfoSyntax  ::=  OCTET STRING
```

The value of **id-nsn-ce-entrustVersInfo,** the OID for **entrustVersInfo** is:

1 2 840 113533 7 65 0

4.2 Distribution Point Entries

CRL distribution point entries must be of the **cRLDistributionPoint** structural object class, as defined in X.521. The attributes defined for that object class which are currently required to be supported in an Entrust environment are:

- **objectClass**
- **commonName**
- **certificateRevocationList**
- **authorityRevocationList**

The **deltaRevocationList** attribute type is not currently used by Entrust PKI components. However, future releases of Entrust may have additional requirements.

A value of the **commonName** attribute is used to create the Relative Distinguished Name (RDN) for entries of this object class. CRL distribution point entries are to be supported in the directory schema as entries which are immediately subordinate to the entry of the issuing CA.

4.3 Entrust User Entries

The attributes defined in X.521 which are currently required to be supported for Entrust user entries are:

- **objectClass**
- **userCertificate**

The **entrustVersInfo** certificate extension defined in 4.1 above will be included in certificates held in Entrust user entries.

No requirements are imposed by Entrust on the structural object class of Entrust user entries. Typically, these will be of the **organizationalPerson** object class.

Entrust does currently require that the object class attribute be capable of modification to add new values, as the Entrust/Manager will add the **entrustUser** value to this attribute at the time an Entrust user is initialized. The specification and registered OID for this object class is as follows:

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

The value of **id-nsn-oc-entrustUser**, the OID for **entrustUser is:**

1 2 840 113533 7 67 0

The placement of Entrust user entries in the DIT and their naming attribute(s) are not mandated by Entrust. However, it is required that the DN be unique and not be re-used at a later stage for some other entry. It is therefore recommended that the following two attributes, defined in X.521, be supported for Entrust user directory entries and that the RDN of Entrust user entries be constructed using a type and value of each.

- **commonName**
- **serialNumber**

4.4 Other Useful Schema Definitions

Entrust Technologies has also defined a number of elements of schema, including object class and attribute type definitions, which may be useful in configuring a directory for use with Entrust and specific e-mail applications. These definitions are not required by Entrust itself or used by the Entrust PKI components specifically, and therefore these are not included in this paper. These specifications will also be made available from the Entrust Technologies Web site (http://www.entrust.com) to provide further assistance in the deployment of a PKI repository supporting various e-mail applications.

5. Security

5.1 Authentication

As described in 3.2.1 above, the Directory must simultaneously allow unauthenticated bind operations (i.e. bind operations in which the optional credentials are not present) and simple authenticated bind operations (i.e. bind operations in which the DN and user password are supplied as credentials).

5.2 Access Control

Entrust/Manager must have sufficient access permissions to allow it to:

- For CA entries:
  - add, modify and delete all attributes identified in 4.1 for its own directory entry; and to
  - add, modify and delete all values of these attributes.

- For CRL distribution point entries:
  - create, modify and delete entries of structural object class **cRLDistributionPoint** immediately subordinate to its own entry; and to
  - add, modify and delete all attributes, and all values of these attributes identified in 4.2 for these entries.

- For Entrust user entries:
  - add and delete the value **entrustUser** to/from the **objectClass** attribute of all entries representing prospective Entrust users; and to
  - add, modify and delete the attribute **userCertificate** and all values of that attribute to/from these entries.

Entrust/Manager must be the only entity with these permissions.

There are no specific access permissions required for Entrust/Admin.

Entrust/Client must be able to read all of the attributes and all of the entries mentioned herein.

6. Summary

Entrust is designed to be the single security infrastructure for organizations. The product family provides numerous security services to system administrators, network users, and applications.

Entrust places minimal requirements on a directory system to fulfill the PKI repository role in an Entrust PKI. These include support for:

- LDAP version 2 protocol (subset only);
- Standard schema elements defined in the X.500 Series of Recommendations;
- Additional schema elements defined by Entrust Technologies, using the tools defined for that purpose in the X.500 Series of Recommendations;
- Simultaneous binds with two authentication levels (none and simple);
- Specific access permissions on the PKI data only.

There are currently many directory products which satisfy these requirements, from a number of vendors.

This information is subject to change as Entrust Technologies reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances may warrant.

Export restrictions apply to all cryptographic products and licenses may be required.

Printed in Canada.