Entrust®, Inc.

Scalability

Author: Jim Turnbull

Date: May 15th, 2000

Version: 1.0

Securing Digital Identities
& Information

Table of Contents

1. Introduction

Scalability refers to the ability for a solution to address a problem, as the problem grows ever bigger. Specifically, scalability refers to the ability for Entrust's solutions to bring trust to e-business as the number of users and e-business transactions reach very high levels.

The purpose of this paper is to describe at a high level how Entrust solutions are highly scalable by providing superior levels of **capacity**, **manageability**, and **ease of use**.

2. Capacity

In order to scale to the capacity levels required for e-business, Entrust/PKI supports millions of users per Certification Authority (CA). Also, in order to minimize hardware costs, Entrust/PKI 5.0.1 supports multiple CAs running on the same UNIX platform.

Capacity is also addressed in many other ways including PKI networking, support for best-in-class directories, remote RA support, and by ensuring the system is always running.

2.1 PKI Networking

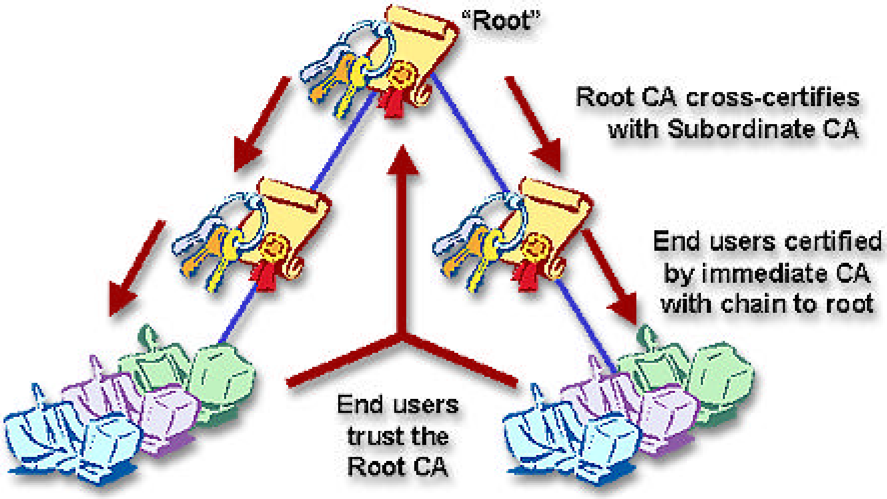
PKI networking refers to a system that establishes and maintains trustworthy electronic relationships between CAs, where multiple CAs can be joined to support an unlimited number of users and e-business transactions.

With PKI networking, users in one CA can communicate securely with users from another, trusted, CA domain. For instance, people who work in a credit card agency may belong to one CA domain, and managers of retail businesses that communicate with the credit card agency may belong to their own CA domains. Through PKI networking, an unlimited number of CAs can be joined together, thereby supporting an unlimited number of users and e-business transactions.

In order to be scalable, these relationships must also be simple to establish and maintain and must be unobtrusive for the people who are actually conducting business. These relationships must also be fine-tuned so that they serve an appropriate business purpose. For instance, a retail vendor who sends encrypted data to a credit card agency may need to be sure that the encrypted data cannot possibly travel outside the one trusted CA domain. Entrust solutions satisfy each of these scalability requirements.

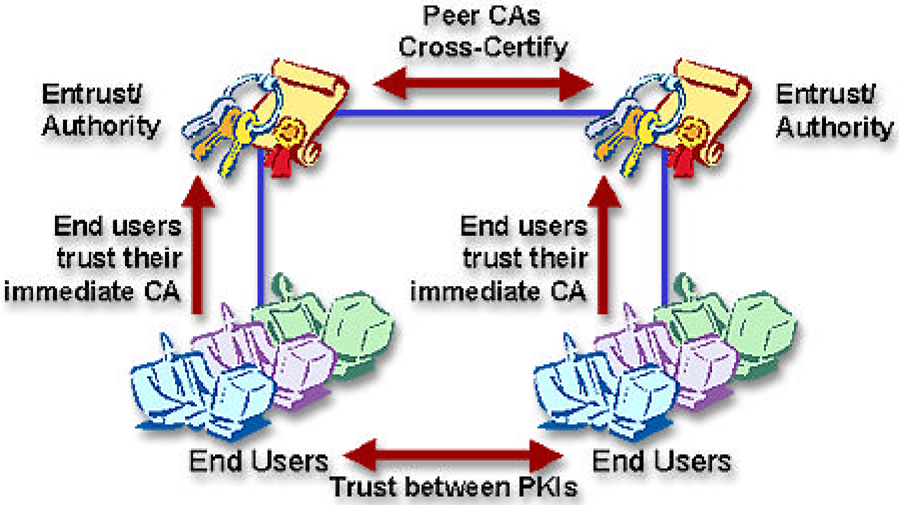
Entrust/PKI offers the following PKI networking features in support of scalability:

- **Hierarchical cross-certification** - Hierarchical cross-certification is ideal within organizations where multiple CAs are needed to scale to the level required. With hierarchical cross-certification, one root CA securely controls all other CAs.


"Root"
Root CA cross-certifies with Subordinate CA
End users certified by immediate CA with chain to root
End users trust the Root CA

Hierarchical cross-certification allows for maximum control by the root CA

- **Peer-to-peer cross-certification** Peer-to-peer cross-certification is ideal between organizations where each organization has secure control over it's own organization and maximum flexibility to scale by forming relationships as business requirements dictate.



Peer-to-peer cross-certification is ideal between organizations that each want complete control over their PKI network.

- **Revocation system networking** – when cross-certification relationships are revoked, Entrust client applications will automatically check the revocation status of each cross-certificate and user certificate in the chain, thereby providing best of breed security. A solution is not scalable unless it is both usable and secure. Entrust solutions meet both requirements by automatically checking certificate revocation status on behalf of users.

- **PKI Policy networking** - provides the flexibility and secure control needed to establish limited trust relationships that match the business relationships between or within organizations. A solution is not scalable unless it can limit trust relationships to meet business needs. For instance, if you've cross-certified with an organization, and they have cross-certified with other organizations, you need to be sure that nothing you have encrypted can be passed along to an organization beyond the original one you cross-certified with. Entrust solutions satisfy this need through PKI policy networking. This ensures that confidentiality agreements stop at an end point that you can control. Typically other vendors don't support policy networking, which can result in trusting everyone in the extended network when that might not be appropriate at all.

2.2 Support for best-in-class directories,

Electronic directories work in unison with Entrust solutions to provide quick authentication and authorization of e-business transactions through rapid access to user certificates, cross-certificates and revocation information from the directory. Scalability requirements demand that quick response times are maintained as the system grows.

Entrust solutions meet these scalability requirements by supporting all the most popular third-party directory products. These products are supported since Entrust solutions support the industry standard LDAP directory access protocol and since Entrust provides testing for 3rd party directory products to ensure compatibility and ease of integration.

2.3 Remote RA support

A system cannot scale to support a large number of users unless the system can also scale the number of administrators required to support these users. Entrust/PKI satisfies this scalability requirement by supporting an unlimited number of administrators per CA. This is accomplished through support for remote administration, where an unlimited number of administrators can concurrently perform administrative operations against one CA from their own desktop. Remote administration is also important to ensure that administrators are close to the users they administer.

2.4 Ensuring that the system is always running

With a mission critical system like Entrust/PKI, it is essential that the system is always running so that e-business transactions can always be conducted. Entrust satisfies this requirement in a number of ways.

Entrust/PKI is designed to detect and report faults and to restart automatically following a re-boot following a power failure. Server operations such as backup are designed to be non-service affecting. The system can be configured to support high availability and disaster recovery requirements.

Automatic key and certificate update ensures that users are still up and running after their original keys and certificates expire. Support for best-of-breed third-party directories ensures that Entrust customers benefit from the availability and disaster recovery capabilities of the directory of their choice. Entrust support for redundant servers for disaster recovery ensures that Entrust/PKI meets your mission critical requirements.

Entrust solutions are also designed to work even if servers components are down. The Entrust client software can cache certificates and CRLs, thereby reducing the need to communicate with the directory over the network if the directory is inaccessible. In addition, Entrust client software is designed to attempt to automatically update keys and certificates before key expiry; if the CA is unavailable then the user is unaffected since the client software will transparently try again the next time the user logs on.

3. Manageability

The biggest hurdle to deploying and managing a PKI is often the cost and effort to the administrator. High manageability is about lowering the cost and effort of administration. The following are the most costly administrative actions and how Entrust eases the cost and effort to the administrator for each administrative action.

3.1 Registering/recovering users

The manageability of the Entrust solution to register and recover users is dependent on a number of configurable products and features as described below:

- Entrust/AutoRA – quickly enroll millions of users without administrator involvement. This product makes deployment hassle-free by providing users with Web-based self-registration and recovery.
- Entrust/RA – the ability to remotely access the CA from Entrust/RA provides the ability to scale to an unlimited number of administrators per CA since each administrator can simultaneously use their own Entrust/RA application on their desktop.
- Bulk processing – allows one administrator to perform operations on many users through the use of bulk processing files.
- Entrust/RA Toolkit – this API allows administrative operations to be integrated into other functions or enrollment procedures, thereby minimizing the administrative burden.

3.2 Deploying software

The need to deploy client software is eliminated with Entrust/TruePass. Entrust/TruePass is a Web security and privacy solution that enables trusted relationships between online businesses and their customers, suppliers and partners. The first product of its kind, Entrust/TruePass has a “zero footprint”, meaning it does not require any client software to be installed or configured on the user’s system.

Other Entrust solutions do require Entrust client software to be deployed to the user’s desktop; for example Entrust/Express for secure email transactions or Entrust/SignOn, which allows users to log in once to the Windows operating system and to all Entrust-Ready applications. In these cases Entrust provides Entrust/DesktopDesigner and

Entrust/UptoDate as administrative tools to speed the deployment and management of Entrust desktop software. With Entrust/DesktopDesigner, using an intuitive interface, administrators are able to customize the Entrust desktop software by defining the business rules for the installation and behavior of the software being deployed. Entrust/UptoDate enables automated software updates through a scheduler that runs on the user's desktop and regularly checks for new updates.

3.3 Administering users

Entrust solutions provide administrative support for the real functions required to scale, including key backup, key recovery, updating information about your users, change DN, change CA, automatic certificate update, and certificate revocation. Automatic key and certificate management is handled seamlessly for all these day-to-day administrative operations. Entrust makes administration simple for administrators and invisible to end users, which is required in order to scale.

3.4 Policy enforcement

An organization needs to establish what, precisely, its security practices will be. For instance, will users need to encrypt data using the strongest available encryption algorithm? Are users permitted to log in from any location, or are they restricted to particular workstations? A scalable solution will support policy requirements like these, and do so without imposing extra operational costs on the PKI. Entrust/PKI satisfies this scalability requirement by providing the ability to centrally specify and automatically enforce the following policies.

- **CA policy management** - securely control user and CA key properties, optional CA hardware and revocation status checking options. With other vendor's solutions, policy is often dictated to you.

- **RA policy management** – securely control RA administrator permissions. For instance, you can limit RA administrators to only specific operations and specific groups of users. This makes the RA administrator's job easier by removing unneeded RA functions from view.

- **User policy management** - control what algorithms are used to encrypt and sign user data, when keys are updated, the length and other aspects of passwords, user mobility options, and the inclusion of additional authorization information in users' certificates.

- **PKI networking policy management** - control the PKI network structure (hierarchical or peer-to-peer), and policy networking to impose specific limits on the trust relationships between CAs in a PKI network.

4. Ease of Use

A system will not scale unless it is easy for users to use. Ease of use means that the solution is transparent and invisible to the user - users shouldn't need to know anything about keys and certificates.

For example, users don’t have to choose the right decryption private key to decrypt data; RA operators don’t have to choose the right decryption key when recovering users’ keys. These operations happen automatically, with no user involvement. Other vendor’s solutions require users to keep track of which key protects which information.

Additionally, users do not have to be aware of critical security functions taking place as they work, such as user key update, CA key update, changes to user identities (DNs), changes of CA location, changes to the list of trusted people in the network, and so on. This minimizes the costs of user training, user downtime, and help desk calls, while at the same time supporting real-life, day-to-day requirements.

Entrust provides a high level of ease of use by providing a single security layer to provide one set of credentials and one password for all user applications.