



Public Key Infrastructure Buyer's Guide

Entrust, Inc.
North America Sales: 1-888-690-2424
entrust@entrust.com

EMEA Sales: +44 (0) 118 953 3000
emea.sales@entrust.com

December 2008

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 company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© Copyright 2008 Entrust. All rights reserved.

Table of Contents

Introduction	2
Key Considerations When Selecting a PKI Solution	3
1 Certification Authority	3
1.1 Setup & Administration	3
1.2 Password Management	3
1.3 Key Update and Certificate Update	4
1.4 Key Backup/Recovery	4
1.5 Cross-Certification	4
1.6 Administration	4
1.7 Reporting	5
1.8 Standards and Cryptographic Algorithms	5
1.9 Scalability	5
1.10 Certificates	5
2 Client Software and/or Applets	7
2.1 Security	7
3 End Users	8
3.1 Usability	8
4 PKI as a Hosted Service (in addition to all other sections)	9
4.1 Services Available	9
4.2 Security	9
4.3 Pricing	9
4.4 Setup	9
4.5 Operational Issues	9
5 Vendor	10
5.1 Corporate Information - briefly describe the following	10
5.2 Technical Support	10
5.3 Documentation and Training	10
5.4 Strategic Partnerships	10
5.5 Services	10

Introduction

Governments and commercial organizations are being challenged to implement cost-effective security solutions that meet the operational needs of their end-users while complying with regulatory requirements. This takes place not only within the context of their internal networks but increasingly in a broader “network of networks,” enabling secure collaboration across departments and agencies. Only the highest levels of trust can make this possible; and only solutions and services built on advanced standards-based products can deliver this trust.

Organizations should look for a solution architected specifically to address such challenges. The solution should be designed to provide interoperability in a large network of networks in which security decisions are enabled across the entire environment. For instance, an authentication decision to access a specific network, application or file should be based on a global policy framework that is inherent in the client applications and enabled on a per-application and a per-user basis.

The solution should also make use of advanced certificate lifecycle management capabilities present in its client solutions, as well as toolkits to ensure proper and cost-effective management of keys and certificates are done simply and transparently. This assures end-to-end trust in cross-certified or bridged public key infrastructure (PKI) environments.

Advanced key and certificate management enables the use of digital credentials even in the most demanding of security environments. Such solutions enable users, regardless of whether they are internal or external to their network, to benefit from both basic and enhanced capabilities in a consistent and secure manner.

This document was created to assist organizations in the selection of the best PKI solution to meet their business and security needs. It outlines key questions to be considered during the selection process to ensure the aforementioned requirements are addressed. This is not intended to be an exhaustive list. It is meant as a starting place to assist you in your review process.

Key Considerations When Selecting a PKI Solution

Note: This is not intended to be an exhaustive list. It is meant as a starting place to assist you in your requirements gathering process.

1 Certification Authority (CA)

1.1 Setup & Administration

- 1.1.1 Does the CA support a hardware solution for storage and use of the CA signing private key? What level of FIPS 140-x validation does this hardware device support?
- 1.1.2 Does the solution support users with a single key pair, dual key pairs and multiple key pairs?
- 1.1.3 Does the solution allow for multiple authentication techniques for a single individual (e.g., smartcards, biometrics, passwords only)?
- 1.1.4 Does the solution's client software support the use of smartcards or biometric devices for authentication? List supported devices.
- 1.1.5 Can access to the certification authority administrative functions be customized using an API? Describe the API.
- 1.1.6 What user and device enrollment options are included? Are there self-enrollment and self-recovery options?
- 1.1.7 Does the solution allow the client to define custom certificate types on the fly such as specialized device certificates, code-signing certificates, etc.?
- 1.1.8 Does the solution support CA key rollover? If so, how is this done? To what extent is this process automated? What is the impact on end-users?
- 1.1.9 Does the vendor offer a choice between an in-house PKI and a hosted service provided by the vendor? If so, does the vendor provide the flexibility to switch between the in-house and hosted solutions, should business requirements change?

1.2 Password Management

- 1.2.1 Does the solution provide centrally configurable password rules that can be applied consistently across applications? Describe.
- 1.2.2 Does the solution transmit any passwords in-the-clear over a network or store passwords in-the-clear at any time? Describe the general methodology for avoiding transmission of passwords and residual passwords in memory.

1.3 Key Update and Certificate Update

- 1.3.1 Describe how key pairs are updated. Does the solution provide automatic and transparent updates of both keys and certificates for users before key expiry?
- 1.3.2 Does the solution provide transparent maintenance of encryption and verification key history, allowing users to transparently decrypt or verify archived data encrypted or signed under old keys? Please explain the steps a user would follow to decrypt an encrypted e-mail using a previous encryption key.
- 1.3.3 Is the certificate management applied consistently across all certificate and key pairs regardless of where they are stored (in hardware or in software)?

1.4 Key Backup/Recovery

- 1.4.1 Does the solution provide integrated, transparent key backup and recovery? If so, is there an extra cost to provide this functionality?
- 1.4.2 How does the solution ensure data can be decrypted after one or multiple key rollovers?
- 1.4.3 How are the keys and certificates managed within the key store? Are separate key and certificate pairs managed within a key store or as a single identity?
- 1.4.4 Can all of a user's archived keys (i.e., the user's entire key history) be recovered in a single step or are users and administrators required to perform additional manual operations for each recovered key pair?
- 1.4.5 How does a user recover keys if they become lost or corrupted? Describe the process.
- 1.4.6 Can keys be recovered by a user alone or is administrative assistance required?

1.5 Cross-Certification

- 1.5.1 Does the solution support both peer-to-peer and hierarchical cross-certification?
- 1.5.2 Can digital signatures be fully verified across departments or between organizations in a bridged-PKI environment? If so, how is this accomplished? Is the method used standards-based?
- 1.5.3 Can specific limits on trust relationships between CAs be imposed and automatically enforced for the user? For example, if cross-certifying with another organization, can users establish a trust relationship with pre-determined departments only?
- 1.5.4 Can the CA root of a hierarchical trust model be taken offline to increase security without affecting the non-root hierarchical CA's ability to operate?

1.6 Administration

- 1.6.1 Does the solution deliver comprehensive administrative control of security policy settings and desktop enforcement of those settings?
- 1.6.2 Does the solution support multiple remote registration authorities to securely execute administrative functions on the PKI system simultaneously?

- 1.6.3 Can multiple authorizations be required to apply a higher level of security when performing sensitive administrative functions?
- 1.6.4 Can enrollment and administration requests be queued for single or multiple Administrator approval?

1.7 Reporting

- 1.7.1 Describe any audit trail and reporting capability provided by the solution. Include a discussion of security protection for these audit logs.
- 1.7.2 Can a report be generated that describes all administrative operations performed?
- 1.7.3 Does the solution support automatic notification of events and alarms? Describe how this is achieved. Is SNMP supported?
- 1.7.4 Does the vendor provide data integrity of audit logs?

1.8 Standards and Cryptographic Algorithms

- 1.8.1 Does the vendor use and promote the use of open standards? If so, list the supported standards.
- 1.8.2 List the data encryption algorithms and key lengths supported by your product.
- 1.8.3 Has the vendor's solution received third-party validation? If so, list the relevant ones.

1.9 Scalability

- 1.9.1 How many users per CA does the solution support?
- 1.9.2 Does the solution support communication with multiple LDAP servers (for load balancing, redundancy and scalability)?
- 1.9.3 Describe the directory support provided. List the X.500 or LDAP directories that have successfully been implemented with the solution. List the leading commercial directories that are supported by the product.
- 1.9.4 Describe your deployment experience with the product. Provide three examples of large deployments for companies similar in size and scope.

1.10 Certificates

- 1.10.1 Does the solution support X.509v3 certificates?
- 1.10.2 Can the solution manage both user and non-user credentials, such as device certificates? Are these certificates managed in the same way as user credentials?
- 1.10.3 Does the solution support multiple certificate types from a single infrastructure? (e.g., VPN device certificates, SSL server certificates, end-user S/MIME certificates, etc.)
- 1.10.4 Does the vendor allow flexibility in certificates to support certificate extensions? Can certificate extensions be set on a per-user basis?
- 1.10.5 Does the solution require proprietary (non-standards based) certificate extension(s) for its operations? If so, what are these extensions and can they be removed?

- 1.10.6 Does the solution support a single set of public key credentials for each user to be used across all applications in the organization that require security (e.g., file/folder encryption, desktop authentication, secure e-mail, remote access, Web browsing, e-forms, etc.)?
- 1.10.7 Are multiple key pairs protected with a single strong password with support for single login?
- 1.10.8 Does the vendor provide automated certificate verification and certificate look-up?
- 1.10.9 Does the solution have the ability to automatically issue a certificate revocation list after a certificate is revoked?
- 1.10.10 Does the solution allow users to perform offline revocation checking of certificates?

2 Client Software and/or Applets

2.1 Security

- 2.1.1 Does the solution ensure consistent security policies and one common security mechanism across multiple applications and multiple platforms?
- 2.1.2 Are the solution's configuration and user policies centrally managed? If so, how are they propagated? (This is important to ensure consistency and auditability of the security controls across the customer's organization.)
- 2.1.3 Can changes in policy regarding crypto algorithms be performed centrally, automatically and transparently to end-users?
- 2.1.4 Does the solution support single login to all applications integrated with the PKI, including back-end and desktop applications?
- 2.1.5 Does the solution provide a secure means of protecting the private keys on the client workstation? Describe the methods that are used to protect the private keys.
- 2.1.6 Are the solution's security mechanisms transparent to the end-user?
- 2.1.7 Does the product allow users to perform encryption and revocation checking of certificates while offline?
- 2.1.8 Does the offering provide a complete end-to-end secure desktop solution?
- 2.1.9 What operating systems does the solution support?
- 2.1.10 Does the vendor offer enhanced security management to automate all aspects of the lifecycle of a digital ID?
- 2.1.11 If automatic renewal of certificate and key pairs is supported, how do applications make use of these new keys?
- 2.1.12 Does the solution integrate with a Virtual Private Network (VPN) solution? Is it available on multiple remote access clients? List the VPN clients supported.
- 2.1.13 Which of the following native Microsoft applications are supported?
 - EFS
 - Smart Card Login
 - Outlook
 - Internet Explorer
- 2.1.14 Describe the solution for securing files from unauthorized access and misuse.
- 2.1.15 Describe the solution for securing internal and external e-mail communications.
- 2.1.16 Does the vendor provide a fully integrated, secure electronic form solution? List forms packages that are supported. Describe briefly.
- 2.1.17 Does the vendor provide high-level, easy-to-use API tools to securely enable non-PKI-aware applications? If so, list them.

3 End-Users

3.1 Usability

- 3.1.1 Are the applications supported with a single, managed digital ID or are users required to manage multiple identities for each application?
- 3.1.2 Does the solution support roaming to multiple workstations? If so, for which applications, and is it with or without smart cards?
- 3.1.3 Does the solution support roaming functionality?
- 3.1.4 Can users share common workstations without having to carry an ID?
- 3.1.5 Does the vendor permit users to easily change between locally stored digital IDs, roaming access and smart card-based digital IDs?
- 3.1.6 Does the vendor have an enterprise solution at the client level that does not require software?
- 3.1.7 Describe the process that users follow to receive their certificates for the first time.
- 3.1.8 How long does it take to issue a certificate to an end-user?
- 3.1.9 Will the enrollment process be the same in a distributed environment?
- 3.1.10 Describe the process that users follow to renew their certificates.
- 3.1.11 Describe the process that users follow to recover their certificates.
- 3.1.12 Are certificate licenses reusable (i.e., when an individual leaves the organization and that individual's certificate is revoked, can the licenses be reused for a new user)?
- 3.1.13 What happens during the recovery or update of a smart card credential if the smart card is full?

4 PKI as a Hosted Service

4.1 Services Available

- 4.1.1 What types of hosting arrangements are available to customers? For instance, does the vendor provide the flexibility to switch between the in-house and hosted solutions should business requirements change?
- 4.1.2 Are professional services available to assist customers with implementation?
- 4.1.3 What client software and capabilities are included (secure file protection, secure e-mail, others)?
- 4.1.4 What training and/or documentation is available as part of the service?
- 4.1.5 Is additional training or documentation available?
- 4.1.6 Is a test environment available for customers?
- 4.1.7 Are certificates available for Web servers, VPN devices and users without client-side software?
- 4.1.8 What support is provided for OCSP? Is it integrated into the solution or a separate/additional product?
- 4.1.9 What optional services are available?

4.2 Security

- 4.2.1 Describe the physical security arrangements of the hosting facility.
- 4.2.2 Describe the disaster recovery facilities provided.

4.3 Pricing

- 4.3.1 What are the components of the pricing structure?
- 4.3.2 What is included in each component?

4.4 Setup

- 4.4.1 How much control can/will the customer have over certificate contents?
- 4.4.2 Will the directory be supplied by the customer or the hosting service?
- 4.4.3 Can certificates be authenticated to a public root?

4.5 Operational Issues

- 4.5.1 What are the support terms and conditions?
- 4.5.2 How is recovery data, such as authorization credentials, protected?
- 4.5.3 How are the CA keys protected?
- 4.5.4 Is there a limit on the number of certificates my organization can use?
- 4.5.5 How quickly can new certificate types be available?

5 Vendor

5.1 Corporate Information — briefly describe the following

- 5.1.1 Corporate profile
- 5.1.2 Number of employees
- 5.1.3 Corporate headquarters and other office locations
- 5.1.4 Financials (copy of 10k report or annual report)
- 5.1.5 List any product awards won in the last five years. List any relevant experience and customer deployments. Are these customers referencable?
- 5.1.6 Describe your corporate quality and security assurance process.

5.2 Technical Support

- 5.2.1 Describe your technical support options, policies and procedures.

5.3 Documentation and Training

- 5.3.1 Describe your method of providing documentation and training for your products.

5.4 Strategic Partnerships

- 5.4.1 Describe the strategic relationships or vendor alliances you have for the delivery of digital signatures, authentication and encryption products and services.

5.5 Services

- 5.5.1 Does your company provide professional services capabilities on a global basis?
- 5.5.2 Does your company have a dedicated solution design and deployment team to enable customer input to product enhancements?