Entrust/PKI and You
Contents

What can Entrust/PKI do for me? .............................................. 6
What's a PKI? ..................................................................... 7
  Security through cryptography ......................................... 7
  Certificates .................................................................... 13
  Certification Authority ..................................................... 13
  Public-key infrastructure ............................................... 15
What's Entrust/PKI? ............................................................. 19
  Entrust/Authority ............................................................ 20
  Entrust/Authority Master Control ........................................ 20
  Entrust/RA .................................................................. 20
  The Entrust/Authority database ....................................... 21
  The Directory .................................................................. 21
Expanding Entrust/PKI .......................................................... 22
  Desktop solutions ............................................................ 23
  E-mail solutions ............................................................... 24
  Web solutions ................................................................. 24
  VPN solutions ................................................................ 25
  ERP solutions ................................................................. 25
  Complementary applications and devices .......................... 26
  Toolkits ........................................................................ 26
Managing Entrust/PKI ........................................................... 28
  Master User ................................................................. 29
  Security Officer ............................................................ 29
  Administrator ................................................................. 30
  Directory Administrator .................................................. 30
  Auditor ........................................................................ 31
  End User ....................................................................... 31
Deployment issues and considerations .................................................. 32
  Project initiation and planning ....................................................... 32
  Requirements analysis and design .................................................. 33
  Development and testing ............................................................... 33
  Installation, integration, and testing .............................................. 33
  Deployment .................................................................................... 34
  Operations and maintenance ......................................................... 34
Where to get assistance ...................................................................... 35
  Have comments/suggestions/questions? ........................................ 35
  Telephone, e-mail, and online support ........................................... 35
  Training and certification ............................................................... 37
  Advising on PKIs ........................................................................... 38
  Services .......................................................................................... 38
  Further information on PKI ............................................................ 39
Entrust/PKI and You

This document provides an overview of Entrust/PKI. You should read this document if you want an introduction to public-key infrastructures and a quick overview of Entrust Technologies’ products and services. This document is suitable for new Entrust/PKI administrators, or anyone within your organization who wants to learn more about Entrust/PKI and its operation.

Topics in this document include

- “What can Entrust/PKI do for me?” on page 6
- “What’s a PKI?” on page 7
- “What’s Entrust/PKI?” on page 19
- “Expanding Entrust/PKI” on page 22
- “Managing Entrust/PKI” on page 28
- “Deployment issues and considerations” on page 32
- “Where to get assistance” on page 35

If you require more detailed information on public-key infrastructures and Entrust Technologies’ products and services after reading this document, please refer to our web site, located at

www.entrust.com
What can Entrust/PKI do for me?

Entrust Technologies provides security solutions for e-business. To do this, Entrust software allows you to place trust in all forms of electronic transactions. Trust is gained through user authentication, digital signatures and the protection of confidential information.

While all organizations have a need for security, not all organizations’ security needs are the same. Possible security needs include

- keeping personal documents secret and secure
- keeping e-mail secret and secure
- verifying the origin of a document or e-mail
- establishing the time at which a document or e-mail was created or sent
- deleting files securely
- ensuring that a wide variety of software and hardware components (such as Web browsers and wireless devices) can transmit information securely and confidentially
- ensuring that all of the above requirements can be carried out simply and transparently

In addition to providing these services for their users, an organization’s planners and administrators may have other security requirements such as

- comprehensively managing security policies
- supporting roaming users
- allowing user-based self-registration and administration
- enabling secure communications and transactions over intranets, extranets, and the Internet
- providing controlled resource access to employees, customers, or partners
- providing secure access to virtual private networks (VPNs)
- providing secure access to enterprise resource planning (ERP) software
- providing secure communications over wireless devices
- enforcing security through cryptographic hardware devices
- developing and customizing security solutions through software toolkits

The solution for all of these security needs? Use a **PKI**.
What’s a PKI?

PKI stands for public-key infrastructure. Entrust Technologies enables secure e-business by using a PKI as the basis for all its security solutions. To understand how a PKI provides security, you must first understand three underlying concepts: security through cryptography, certificates, and the Certification Authority.

Security through cryptography

To keep data secure, and to provide a user with a digital signature, each user has a number of different keys. The keys that keep data secure are the encryption key pair, used in conjunction with symmetric keys. The keys that provide a digital signature are known as the signing key pair.

Data security using the encryption key pair and symmetric keys

The encryption key pair, used in conjunction with symmetric keys, keeps data secure. The encryption key pair consists of a public key (used only for “locking”—that is, encrypting—data, known as the encryption public key) and a private key (used only for “unlocking”—that is, decrypting—data, known as the decryption private key). Encrypting and decrypting data through the use of a public-private encryption key pair is known as asymmetric cryptography, or, as it is more popularly known, public-key cryptography.

Encryption public key
Anyone has access to it.
Used for encrypting data.

Decryption private key
Only its owner has access to it.
Used for decrypting data.

The additional keys used for data security are known as symmetric keys. A symmetric key is like a physical key people use in their daily lives, in which the key is used to both lock and unlock items. Symmetric keys, then, are used for both encrypting and decrypting data. This process is known as symmetric cryptography. The primary benefit of symmetric encryption is speed. Because of
this, symmetric algorithms are especially suited to encrypting and decrypting large amounts of data.

1. The sender “locks” the data (that is, encrypts it) with a one-time symmetric key, generated randomly for this step.

2. The sender then encrypts the symmetric key with the recipient’s encryption public key.
Next, the sender forwards both the encrypted data and the encrypted symmetric key to its intended recipient.

3 After receiving the encrypted data and the encrypted symmetric key, the recipient first “unlocks” the symmetric key (that is, decrypts it) with their decryption private key.

![Diagram showing the decryption process: Encrypted symmetric key is decrypted to Decrypted symmetric key.](image)

Remember: since the sender locked the symmetric key using the recipient’s encryption public key, only the recipient’s decryption private key is capable of unlocking it.

4 With the symmetric key usable again, the recipient uses it to decrypt the data.

![Diagram showing the decryption process: Encrypted data is decrypted to Decrypted data.](image)
Digital signatures using the digital signature key pair

The digital signature key pair provides a user with the means of generating a digital signature. A digital signature provides a guarantee to a recipient that signed data came from the person who signed it, and that it was not altered since it was signed. The digital signature key pair is composed of a signing key (known as the signing private key) and a verification key (known as the verification public key).

To affix a digital signature, a sender follows these steps:

1. The sender starts the process by taking a mathematical summary (called a hash code) of the data. This hash code is a uniquely identifying digital fingerprint of the data. If even a single bit of the data changes, the hash code will change.
2 Next, the sender “signs” the hash code with their signing private key.

The sender then forwards the data and the signed hash code to the intended recipient.

How can the signed hash code be considered a signature? The signed hash code is an item that only the sender, using their signing private key, could have produced.

The next series of steps describes verification of the signature and confirmation that the data has not been altered since it was signed.

1 Upon receipt of the data and the signed hash code, the recipient can verify that the hash code was signed by the sender by recovering the hash code using the sender’s verification public key.
The recipient, having possession of what presumably is the original data, uses the data to generate a new hash code.

New hash code and original signed hash code are compared. If the hash codes match, the recipient has verified that the data has not been altered.

How do matching hash codes indicate that the data was not altered since the original hash code was signed? Because the hash function that produced the hash codes is extremely sensitive to changes in data. If the data had been altered in any way, the new hash code it produced would not have been identical to the original hash code. Matching hash codes ensure the data is in the same state that it was in when it produced the original hash code—thus proving that no altering of data has taken place.

Remember: a digital signature guards data against modification, but it does not prevent unauthorized eyes from viewing the data. To protect data against unauthorized access, you must also encrypt the data.
Certificates

Using public and private keys to encrypt and sign data raises an important security-related question: how can you be sure the public key you are using belongs to the right person?

The solution: associate the public key and its user with a certificate.

A certificate is an object that contains (among other items)
- information, in an industry-standard format, detailing the person’s identity
- a public key, associated exclusively with the person

Certification Authority

A certificate associates a public key with an individual user.

But how do you know that the information in the certificate is valid? How do you know that the correct public key has been associated with its rightful user?

The solution: have the information in all certificates guaranteed by a Certification Authority.
A Certification Authority is a trusted entity whose central responsibility is certifying the authenticity of users. In essence, the function of a Certification Authority is analogous to that of the passport issuing office in the Government. A passport is a citizen’s secure document (a “paper identity”), issued by an appropriate authority, certifying that the citizen is who he or she claims to be. Any other country trusting the authority of that country’s Government passport office will trust the citizen’s passport. This is an example of third-party trust.

Similar to a passport, a user’s certificate is issued and signed by a Certification Authority and acts as proof that the correct public key is associated with the user. Therefore, through third-party trust, anyone trusting the Certification Authority can also trust the user’s key.

If Bob or Alice trust the Certification Authority, they can be sure that the certificates signed by it are associated with their rightful owner. With this trust established, encryption can take place, with the sender knowing that only the intended recipient will be able to decrypt the data, and verification can take place, with the recipient knowing that only the signer could have signed the data.

To organize public-key cryptography, certificates, and a Certification Authority in a manner that gives you a manageable, flexible, and reliable form of security, you use a security management system known as a public-key infrastructure.
Public-key infrastructure

A public-key infrastructure (PKI) is a framework that provides security services to an organization using public-key cryptography. These services are generally implemented across a networked environment, work in conjunction with client-side software, and can be customized by the organization implementing them. An added bonus is that all security services are provided transparently—users do not need to know about public keys, private keys, certificates, or Certification Authorities in order to take advantage of the services provided by a PKI.

In addition to providing integrity of digitally signed data and protection of encrypted data, a fully functional PKI must provide a number of core services. These are outlined in Figure 1.
Figure 1: Services implemented by a public-key infrastructure

Enabling trust through a Certification Authority

The following sections discuss the core services of a PKI.

Enabling trust through a Certification Authority

The Certification Authority manages the PKI and enables trust among its users. It enables this trust by certifying that the association between a user and their key pairs is valid.
Certificate retrieval from a certificate repository
The PKI’s users must be able to locate public keys contained within certificates in order to secure information for other users. They can do this by going to a publicly accessible storage area where certificates can be found, known as a certificate repository.

Certificate revocation
The PKI’s users must be sure that a certificate is still trustworthy at the time of use. If a certificate is no longer trustworthy, it must be revoked by the Certification Authority. Certificate revocation mechanisms ensure that information about certificates revoked by the Certification Authority is published in a publicly available list (known as a certificate revocation list, or CRL). If a user attempts to use a revoked certificate, they will be informed that use of the certificate is no longer considered secure.

Key backup, history, and recovery
The PKI’s users must be sure that they will be able to view data that was encrypted for them, even in cases where they may lose their profiles or forget their passwords. To protect users’ access to this data, PKIs perform key backup, history, and recovery tasks for users.

Automatic update of key pairs and certificates
To ensure security, key pairs and certificates must have a finite lifetime. To spare the user the annoyance of having to manually update this information when their key pairs and certificates expire, a PKI can perform this task automatically. Automatic updating keeps things simple for the user, as keys are generated and replaced automatically before they are due to expire. At the same time, security is increased through finite key lifetimes.

Establishing trust with other PKIs
Sometimes users in a PKI community must exchange sensitive communications with users in other PKI communities. For example, two trading partners, each with their own Certification Authority, may want to validate certificates issued by the other partner’s Certification Authority. Two ways of creating extended third-party trust among users of different PKIs include

Peer-to-peer trust—trust is created through two or more Certification Authorities securely exchanging their verification public keys, which are used to verify each Certification Authority’s signature on certificates. By signing each other’s verification public key, each Certification Authority creates a certificate for the other Certification Authority—thus allowing their users to trust the other Certification Authority. This creates a “peer-to-peer” level of trust among the various cross-certified Certification Authorities.
Hierarchical trust—trust is created through establishing a “root of trust” among Certification Authorities. Hierarchical trust of Certification Authorities (also known as a strict hierarchy) is a way of arranging two or more Certification Authorities in a restrictive trust relationship. A Certification Authority that’s in a hierarchy has its Certification Authority certificate signed by its direct superior. A superior may be the root of a hierarchy, or some level of subordinate beneath the root. The pattern of superiors signing their subordinates’ certificates eventually converges at the root, which signs its own Certification Authority certificate. Each subordinate is at the end of a certificate chain that begins with the root’s certificate. In effect, all Certification Authorities and users in a hierarchy can trust each other, because they all share a trust anchor (at the root of the hierarchy).

**Non-repudiation of digitally signed data**
Non-repudiation means that an individual cannot successfully deny involvement in a legitimately signed transaction. To achieve this within a PKI, the key used to create digital signatures (the signing private key) must be generated and securely stored in a manner under the sole control of the user at all times. Since the signing private key is never backed up, or made available to anyone but the user, it is impossible for a user to repudiate data that contains their digital signature.

**Client software**
Client software is used to support all of the elements of a PKI discussed above. Running from the user’s desktop, client software makes trust decisions (for example, whether to use a particular encryption public key contained within a particular certificate to encrypt data) based on signed information that is provided by the PKI. Client software provides security services consistently and transparently across applications on the desktop.
What’s Entrust/PKI?

Entrust/PKI is a PKI containing all the features outlined in the section above and more. There is no one, single application called Entrust/PKI—rather, Entrust/PKI is a collection of applications that work together to make up a PKI. The core components of Entrust/PKI are

- Entrust/Authority
- Entrust/Authority Master Control
- Entrust/RA
- the Entrust/Authority database
- the Directory

Figure 2 provides an overview of the relationships among these core components of Entrust/PKI.

Figure 2: Entrust/PKI core components and their relationships

The following sections discuss the core components of Entrust/PKI.
Entrust/Authority

In Entrust/PKI, the role of Certification Authority is held by Entrust/Authority. Entrust/Authority can be thought of as the “engine” of Entrust/PKI. The main functions of Entrust/Authority are to

- create certificates for all public keys
- create encryption key pairs for users
- manage a secure database of Entrust/PKI information that allows the recovery of users’ encryption key pairs (in case a user forgets their password, for example)
- enforce the security policies defined by your organization

Access to Entrust/Authority is provided through Entrust/Authority Master Control and Entrust/RA.

Entrust/Authority Master Control

Entrust/Authority Master Control is a local interface with direct access into Entrust/Authority. It provides access to Entrust/Authority to only the most highly trusted administrators (for information on users who administer Entrust/PKI, see “Managing Entrust/PKI” on page 28). Running in either command-line or GUI form, Entrust/Authority Master Control is used for tasks that include

- starting and stopping the Entrust/Authority service
- recovering profiles for Security Officers (for information on Security Officers, see “Security Officer” on page 29)
- managing the Entrust/Authority database

Entrust/RA

Entrust/RA (RA stands for “registration authority”) is the administrative component of Entrust/PKI. Entrust/RA uses a graphical interface and communicates securely with Entrust/Authority. Entrust/RA is used for administrative tasks that include

- adding users
- managing users and their certificates
- managing security policies
- cross-certifying with other Certification Authorities
- setting up hierarchies of Certification Authorities
The Entrust/Authority database

The Entrust/Authority database is under the control of Entrust/Authority and acts as a secure storage area for all information related to Entrust/PKI. In this database, Entrust/Authority stores:

- the Certification Authority signing key pair (this key pair may be created and stored on a separate hardware device rather than the database)
- user status information
- the encryption key pair history (including all decryption private keys and encryption public key certificates) for each user
- the verification public key history (including all verification public key certificates) for each user
- the validity periods for signing key pairs, encryption key pairs, and system cross-certificates
- Security Officer and Entrust Administrator information (for more details on users who administer Entrust/PKI, see “Managing Entrust/PKI” on page 28)
- Certification Authority policy information
- revocation information

**Note:** All information stored in the Entrust/Authority database is protected against tampering, with all sensitive information being encrypted.

The Directory

The majority of user requests for information involve retrieving other users’ certificates. To make this information publicly available, Entrust/PKI uses a public repository known as a Directory. Information that is made public through the Directory includes:

- user certificates
- lists of revoked certificates
- client policy information

**Note:** For information requests and network traffic across Entrust/PKI, the Directory is the most frequently accessed component.
Expanding Entrust/PKI

Working with the core components of Entrust/PKI are numerous Entrust-Ready applications, as shown in Figure 3. These applications add increased functionality to Entrust/PKI, provide a greater degree of customization, and add to the number of security services.

There are many ways to expand Entrust/PKI. Some of those ways include:

- desktop solutions
- e-mail solutions
- Web solutions
- virtual private network (VPN) solutions
- enterprise resource planning (ERP) solutions
- complementary applications and devices
- toolkits

**Figure 3:** Expanding Entrust/PKI

The following sections provide an overview of some of the applications which work with Entrust/PKI.
Desktop solutions

Entrust desktop solutions provide strong and flexible protection of sensitive data stored on the user’s computer desktop. Desktop solutions include five main products: Entrust/Entelligence, Entrust/ICE, Entrust/TrueDelete, Entrust/SignOn, and Entrust/Solo.

**Entrust/Entelligence**

Entrust/Entelligence provides a common, single layer of security that allows users to log in once to all other Entrust applications (if their policy is set up to allow it). Entrust/Entelligence transparently and automatically manages certificates, encryption, digital signatures, and other security issues on behalf of the user. In addition to these management functions, Entrust/Entelligence can encrypt, decrypt, sign, and verify files.

**Entrust/ICE**

Entrust/ICE protects sensitive information seamlessly and automatically on workstations, laptops, and network drives by encrypting files in folders.

**Entrust/TrueDelete**

Entrust/TrueDelete is a utility designed to securely scrub deleted files from the user’s system.

**Entrust/SignOn**

Entrust/SignOn allows users the option to log in once using Entrust credentials to the Windows 95, 98, NT, and 2000 operating systems and all Entrust-Ready applications. Entrust/SignOn integrates into Entrust/Entelligence.

**Entrust/Solo**

Entrust/Solo is a stand-alone application that provides enterprise-strength data encryption, digital signature, and data compression capabilities to PCs running Windows 95 or Windows NT.

---

**Note:** Entrust/Solo is free of charge for non-commercial users (including educational institutions and not-for-profit organizations) or is available for a 30-day evaluation for corporate users. You can download it at [www.entrust.com/solo](http://www.entrust.com/solo).
E-mail solutions

E-mail solutions provide encryption, decryption, and digital signature capabilities for a wide variety of popular e-mail programs. E-mail solutions include Entrust/Express and Entrust/Unity.

Entrust/Express

Entrust/Express is a fully featured e-mail plug-in providing e-mail encryption and digital signature services. It integrates into Microsoft Outlook, Microsoft Exchange, Lotus Notes, and Qualcomm Eudora.

Entrust/Unity

Entrust/Unity enables users of Netscape Messenger and Microsoft Outlook to take advantage of Entrust/PKI for secure e-mail.

Web solutions

Entrust Web solutions provide a range of offerings which allow users to verify identities, control access to resources, and communicate securely over the Internet. These products include Entrust/Direct, Entrust/Unity, Entrust/WebConnector, Entrust/TruePass, and Entrust/getAccess.

Entrust/Direct

Entrust/Direct allows organizations to deploy e-commerce services on the Web, while providing secure permanent records of user transactions.

Entrust/Unity

Entrust/Unity enables secure Web browsing and code signing for users of Web browsers from Microsoft and Netscape.

Entrust/WebConnector

Entrust/WebConnector allows Web certificates to be issued to standard, off-the-shelf Web browsers and Web servers, thus enabling secure e-business for both vendors and consumers.

Entrust/TruePass

Entrust/TruePass enables trusted Web-based relationships. This application provides a provable record of transactions, data protection, and privacy capabilities for online businesses, customers, suppliers, and partners. Entrust/TruePass features a “zero-footprint” client that allows greater user transparency and ease of deployment.
**Entrust/getAccess**

Entrust/getAccess is an e-business Web portal management solution. It turns a Web portal into a facility for managing relationships with individuals who interact with your organization, allowing you to tailor each user’s entire online experience. Entrust/getAccess provides direct access to enterprise applications, while protecting the privacy of individual business relationships and the security of your information assets.

**VPN solutions**

Virtual private network (VPN) technology provides network-level security for a wide range of applications. VPN solutions include Entrust/Access and Entrust/VPNConnector.

**Entrust/Access**

Entrust/Access allows users to transparently and securely connect to their enterprise network using managed digital certificates.

**Entrust/VPNConnector**

Entrust/VPNConnector provides digital certificates to VPN devices such as routers, gateways, firewalls, and remote access devices.

**ERP solutions**

Enterprise resource planning (ERP) integrates all facets of a business, including planning, manufacturing, sales, and marketing. Security of ERP applications ensures a reduced risk of loss of revenue, sensitive intelligence, and credibility, while also increasing efficiency, decreasing costs, and expanding business through secured transactions. ERP solutions include Entrust Security for SAP R/3 and Entrust Security for PeopleSoft.

**Entrust Security for SAP R/3**

Entrust Security for SAP R/3 ensures encryption of data traveling over public networks and provides digital signatures to authenticate both data and messages exchanged and stored within SAP R/3.

**Entrust Security for PeopleSoft**

Entrust Security for PeopleSoft provides security for PeopleSoft’s Win32 and Java clients by replacing password transmission with authentication using managed digital certificates.
Complementary applications and devices

Entrust/PKI’s flexibility can be complemented in areas such as administration, notarization, user mobility, and hardware-based security. The applications and devices providing these solutions include Entrust/ProfileServer, Entrust/AutoRA, Entrust/Timestamp, and Entrust-Ready cryptographic hardware devices.

Entrust/ProfileServer
Entrust/ProfileServer enables a secure, central store of user profiles so that users can log in from anywhere on their organization’s network.

Entrust/AutoRA
Entrust/AutoRA provides a secure way to add and administer Entrust/PKI users without the involvement of an administrator. Using a Web page tailored for your organization, users can enroll at any time, and from any location. Users are authenticated using information already stored in an organization’s databases.

Entrust/Timestamp
Entrust/Timestamp provides secure, trustworthy timestamping services to Entrust/PKI users.

Entrust-Ready cryptographic hardware devices
Entrust Technologies offers support for an array of devices that offer tamper-resistant protection to Certification Authority keys and user profiles.

Toolkits
The Entrust/Toolkit Application Programming Interface (API) is a family of APIs that provide software developers with low-level access to Entrust Technologies’ encryption, digital signature, and automated key management tools. Entrust Technologies’ toolkits enable developers to make their applications Entrust-Ready. The toolkits provided are

- EntrustFile Toolkit
- EntrustSession Toolkit
- EntrustIPSec Negotiator Toolkit
- Entrust/Toolkit for Java
- Entrust/Toolkit for Visual Basic
- Entrust/Toolkit for SSL/TLS
- Entrust/RA Toolkit
**Note:** The Entrust/Toolkit family of APIs (with the exception of the Entrust/RA Toolkit) is provided to developers free of charge. Copies of the toolkits are available for download at [developer.entrust.com](http://developer.entrust.com).
Managing Entrust/PKI

Entrust/PKI provides a division of responsibilities to ensure security, as shown in Figure 4. Supporting this division are a variety of distinct user roles, capable of carrying out the full range of tasks within Entrust/PKI. The default administrator roles in Entrust/PKI are Master User, Security Officer, Administrator, Directory Administrator, and Auditor. The default non-administrator role is End User.

Figure 4: User roles in Entrust/PKI

It is possible to create new administrator and end-user roles and to customize their capabilities. For example, you can create an administrator role that can only carry out certain functions, such as creating users or revoking users. As another
example, you can create several end-user roles, each specifying different key lifetimes for various types of users.
The following sections describe each of the Entrust/PKI default user roles.

**Master User**

This role is for three highly trusted people who, along with a Security Officer, install and configure Entrust/PKI. Master Users are the only users who can use Entrust/Authority Master Control. Master Users perform system-level operations involving Entrust/Authority, including starting and stopping the Entrust/Authority service.

Documentation used by Master Users consists of

- *Entrust/PKI 5.1 Supplement on Windows NT*  
  or *Entrust/PKI 5.1 Supplement on UNIX*
- *Installing Entrust/PKI 5.1 on Windows NT*  
  or *Installing Entrust/PKI 5.1 on UNIX*
- *Administering Entrust/PKI 5.0 on Windows NT*  
  or *Administering Entrust/PKI 5.0 on UNIX*

**Note:** Unlike other default roles, you can’t modify the Master User role or use it as a basis for creating custom roles.

**Security Officer**

This role is for a few highly trusted people in your organization who will use Entrust/RA to administer sensitive Entrust/PKI operations. The first Security Officer is created when you initialize Entrust/PKI. Security Officers set the security policy for your organization’s PKI, and supervise administrators.

Security Officers use Entrust/RA to perform tasks such as

- setting up Entrust/PKI so that its operations conform to your organization's policies and procedures regarding security
- administering other administrators
- establishing trust relationships with other Certification Authorities

Documentation used by Security Officers consists of

- *Entrust/PKI 5.1 Supplement on Windows NT*  
  or *Entrust/PKI 5.1 Supplement on UNIX*
- *Administering Entrust/PKI 5.0 on Windows NT*  
  or *Administering Entrust/PKI 5.0 on UNIX*
You can modify this role by changing its name, the number of authorizations required for sensitive operations, and its user policy certificate. This role can be used as a basis for creating a custom role.

**Administrator**

This role is for any number of trusted people in your organization. For convenience, and depending on the size and nature of your user community, you may wish to have several Administrators. Administrators primarily administer End Users.

Administrators use Entrust/RA to perform tasks such as
- adding, removing, and deactivating End Users
- revoking End User certificates
- recovering End Users

Documentation used by Administrators consists of

- *Entrust/PKI 5.1 Supplement on Windows NT*
  - or *Entrust/PKI 5.1 Supplement on UNIX*
- *Administering Entrust/PKI 5.0 on Windows NT*
  - or *Administering Entrust/PKI 5.0 on UNIX*

You can modify this role by changing its name, the number of authorizations required for sensitive operations, and its user policy certificate. This role can also be used as a basis for creating a custom role.

**Directory Administrator**

This role is for any number of trusted people in your organization. Directory Administrators perform tasks that modify information listed in Entrust/PKI’s Directory.

Directory Administrators use the Directory Browser tool in Entrust/RA to perform tasks such as
- adding and deleting entries in the Directory, either in batch mode or one at a time
- adding, changing, and deleting attributes in Directory entries

Documentation used by Directory Administrators consists of

- *Entrust/PKI 5.1 Supplement on Windows NT*
  - or *Entrust/PKI 5.1 Supplement on UNIX*
- *Administering Entrust/PKI 5.0 on Windows NT*
  - or *Administering Entrust/PKI 5.0 on UNIX*
You can modify this role by changing its name, the number of authorizations required for sensitive operations, and its user policy certificate. This role can also be used as a basis for creating a custom role.

**Auditor**

This role is for any number of trusted people in your organization. Auditors have a view-only role in Entrust/RA: they can view (but not modify) audit logs, reports, security policies, and user properties.

Documentation used by Auditors consists of

- *Entrust/PKI 5.1 Supplement on Windows NT*
- or *Entrust/PKI 5.1 Supplement on UNIX*
- *Administering Entrust/PKI 5.0 on Windows NT*
- or *Administering Entrust/PKI 5.0 on UNIX*

You can modify this role by changing its name, the number of authorizations required for operations, and its user policy certificate. This role can also be used as a basis for creating a custom role.

**End User**

This role is for non-administrative Entrust users. End Users cannot log in to Entrust/RA. End Users can be either people (members of your organization) or things (a Web site, a wireless device)—the qualification being that they must be granted a certificate for use within your PKI.

Documentation used by End Users consists of user guides and online help provided with the Entrust-Ready applications they are using.

You can modify this role by changing its name and user policy certificate. This role can also be used as a basis for creating a custom role.

On the client side, the person’s name and keys are encrypted, and stored as a profile. The Entrust profile authenticates the users’ identities to the Certification Authority and allows them to access their private data. Note that roaming end users do not need to carry their profiles. You can create roaming users if your organization has Entrust/Profile Server.
Deployment issues and considerations

Setting up a PKI that suits your security goals involves making numerous decisions before installing any software. To assist your organization in this decision making, Entrust Technologies offers a line of services known as the Entrust RapidPKI Deployment Methodology. These services provide PKI planning and implementation to organizations who want to jump-start their Entrust security solution.

Figure 5 provides an overview of the Entrust RapidPKI Deployment Methodology.

Figure 5: Entrust RapidPKI Deployment Methodology

The main RapidPKI services are outlined below.

Project initiation and planning

Project initiation and planning focuses on preparing for your organization’s deployment of Entrust/PKI. Project planning involves

- determining and documenting business and PKI requirements
• engaging sponsors and champions within your organization
• engaging functional specialists within your organization
• scoping an initial project
• developing and documenting a project management plan

Requirements analysis and design
Requirements analysis and design involves assessing what resources, physical or otherwise, are necessary for implementing Entrust/PKI. The focus is on
• analyzing, designing, and documenting Certificate Policy and Certification Practice Statements
• documenting PKI system requirements and design
• documenting PKI facility needs
• identifying staff and training needs
• procuring hardware and software

Development and testing
Development and testing focuses on developing any necessary custom software, as well as testing all software and system components. This takes place before your PKI is installed. Development and testing involves
• developing and testing custom/customized PKI components (if required)
• documenting your organization’s PKI operations manual
• enhancing your facilities (if required)
• training PKI operations staff, registration authorities, and helpdesk staff

Installation, integration, and testing
In this phase your organization installs all components of the PKI. All operations are closely monitored. Installation, integration, and testing involves
• installing network, firewall, hardware, operating system, and third-party software components
• installing supporting Directory and Web software
• installing Entrust software and supporting hardware
• integrating back-end systems
• testing all functionality
Deployment
Deployment involves running your PKI in a pilot program, followed by full rollout. Deployment consists of
• engaging the pilot user community
• running the pilot for four to six weeks
• monitoring PKI usage and feedback
• monitoring operations staff, registration authorities, helpdesk staff, and performance
• enhancing the PKI environment as required
• initiating full rollout

Operations and maintenance
With active deployment complete and PKI usage under way, your organization now must ensure continued operation and maintenance. Operations and maintenance involves
• conducting ongoing maintenance and support services
• leveraging the PKI and extending your company’s return on investment by deploying additional PKI applications

Other services
The Entrust RapidPKI Deployment Methodology offers other services in addition to those listed above. These include
• RapidPKI deployment tips
• provision of best practices
• identification of the project critical path
• identification of the most common critical success factors
• identification of the most common PKI deployment pitfalls
• provision of templates, such as a project GANTT chart

For more details on RapidPKI, Entrust Technologies provides the Entrust “RapidPKI” Deployment Methodology Manual. To obtain this manual, contact Entrust Technologies (see “Advising on PKIs” on page 38 for details).
Where to get assistance

We are always interested in your experiences using Entrust/PKI and its related products and services.

Have comments/suggestions/questions?

We are continually trying to improve the quality and coverage of information related to Entrust/PKI. If you have any comments or questions about any aspect of Entrust/PKI, send us an e-mail at entrust@entrust.com

You can also visit our web site at www.entrust.com

General inquiries can be directed to the following telephone numbers:

Tel: 1-972-943-7300
Fax: 1-972-943-7305

We look forward to hearing from you.

Telephone, e-mail, and online support

Entrust Technologies offers telephone, e-mail, and online support through the Entrust/Reliance customer care program. Three levels of support are available to meet your needs: Silver Key, Gold Key, and Platinum Key. Information on the three levels of customer support are listed in Table 1.

Table 1: Customer support

<table>
<thead>
<tr>
<th>Service</th>
<th>Platinum Key</th>
<th>Gold Key</th>
<th>Silver Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours of support:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Basic(^1)</td>
<td>7x24</td>
<td>5x24, Monday to Friday</td>
<td>8 AM to 8 PM (EST) Monday to Friday</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 AM to 7 PM (GMT) Monday to Friday</td>
<td></td>
</tr>
<tr>
<td>• Emergency(^2)</td>
<td>7x24</td>
<td>7x24</td>
<td>7x24</td>
</tr>
<tr>
<td>Mutually defined trouble priority</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
**Table 1: Customer support (continued)**

<table>
<thead>
<tr>
<th>Service</th>
<th>Platinum Key</th>
<th>Gold Key</th>
<th>Silver Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software maintenance releases</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Access to online support</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Early notification of significant technical bulletins</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Technical account manager</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quarterly service reviews</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Requirements definition</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Five days of Entrust training</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Basic support includes the customer support newsletter, access to online support, and support by telephone or e-mail.
2. Emergency support includes assistance in circumstances where a customer experiences a production system problem (a “production system” is defined as a PKI with active users outside of a test lab environment).

**Telephone support**

For telephone support, simply call the appropriate number listed in your Customer Resource Kit. The Customer Resource Kit is a package made available to customers after the Entrust/Reliance customer care program has been purchased. You must provide your Unique ID (listed on your Customer Support Xtranet account) whenever you call.

**E-mail support**

E-mail support is offered to provide assistance for non-critical issues. Questions can be sent to support@entrust.com

**Online support**

Online support is provided through the Customer Support Xtranet. This portal contains online versions of product documentation, an information knowledge base, and problem resolutions. It also provides the ability to submit and track
service requests via the Web in a secure manner. You must have an account to access this portal. You can sign up for an account at

www.entrust.com/xtranet/support/

**Training and certification**

Entrust Technologies provides comprehensive training for customers who want to deploy a PKI. Training is also available to implement e-business portal solutions via the Entrust/getAccess product. Our training consists of a combination of theory and hands-on laboratory exercises which enables users to quickly maximize their return on investment. Selected self-study courses are also available.

**Entrust Courses**

- *Security Technologies for E-Business* - An introduction to the basic concepts of security and PKI, including encryption and digital signature.
- *Entrust/PKI (Release 5.0) Management* - A hands-on, comprehensive and detailed look at the components and management of an Entrust/PKI solution.
- *PeerLogic LiveContent Directory Training* - A hands-on exploration of this high-performance, scalable Directory product.
- *Developing Entrust Applications for e-Business* - A comprehensive overview of EntrustFile and EntrustSession APIs and the development of both store-and-forward and online transaction-oriented applications.
- *Introduction to Entrust Desktop Applications CBT v5.0* - A self-directed learning tool for end users of Entrust software, to allow them to quickly begin securing files and participating in e-business transactions.
- *Entrust/getAccess Training:*
  - getAccess Fundamentals
  - getAccess System Administration and Installation
  - getAccess Customization and Integration
  - getAccess Deployment Self-Study

For more information about Entrust course offerings, or how to register for an Entrust course, please consult

www.entrust.com/training

New courses are constantly being added, so please check the Web site regularly.
Advising on PKIs

In order to operate a PKI that performs to its greatest potential, Entrust Technologies recommends that you consult the Entrust Technologies Professional Services department. Professionals experienced in the areas of PKI implementation and deployment are available to provide a number of useful services, including

- PKI security consulting
- PKI deployment using the Entrust RapidPKI Deployment Methodology
- systems integration
- an insourcing program

To contact Professional Services about these or other offerings (such as obtaining the *Entrust “RapidPKI” Deployment Methodology Manual*), please call Entrust Technologies at 1-888-690-2424

Services

Entrust Technologies offers a number of services to meet the ever-growing range of security needs. Two of these services are Entrust.net and Entrust@YourService.

**Entrust.net**

Entrust.net provides services for issuing and managing digital certificates for publicly trusted Web and Wireless Application Protocol (WAP) servers. These certificates enable secure communications over wired and wireless networks using the Secure Sockets Layer (SSL) and Wireless Transport Layer Security (WTLS) protocols. Certificates issued by Entrust.net are trusted by the vast majority of browsers and wireless micro-browsers in use today. For more information, please visit the Entrust.net Web site at

**www.entrust.net**

**Entrust@YourService**

Entrust@YourService allows you to secure Business-to-Business, Business-to-Consumer, and Enterprise transactions with PKI technology—while at the same time outsourcing system hosting, management, and operations. This allows you to provide the high level of security provided by a PKI without deploying an infrastructure within your organization. For more information on outsourcing the tasks related to setting up and operating a PKI, without giving up your control over it, please visit the Entrust@YourService Web page at

**www.entrust.com/yourservice**
Further information on PKI

There are a broad range of sources of information available on PKI technology. A good place to start is by referring to our whitepapers, which can be found at Entrust Technologies' online Resource Center at

www.entrust.com/resourcecenter

For a more comprehensive explanation of PKI, Entrust Technologies recommends the following book:

Understanding Public-Key Infrastructure—Concepts, Standards, and Deployment Considerations

Co-authored by Entrust Technologies' Carlisle Adams and Steve Lloyd, this book provides a thorough examination of the details surrounding PKI. This book will benefit those responsible for planning, deploying, or operating a PKI, as well as serving as an educational tool and reference guide for both novices and professionals alike.
encryption key pair
  about 7
data security 7
  See also encryption public key, decryption private key
encryption public key
  keeping data secure using a 7
  See also encryption
End User
  about 31
documentation used 31
Entrust "RapidPKI" Deployment Methodology 32–34
Entrust "RapidPKI" Deployment Methodology Manual
  about 34
  obtaining 38
Entrust products
  See expanding Entrust/PKI
Entrust Security for PeopleSoft 25
  See also ERP solutions
Entrust Security for SAP R/3 25
  See also ERP solutions
Entrust Technologies
  about 6
customer support 35–37
  sending comments to 35
Entrust.net
  about 38
Entrust/Access 25
  See also VPN solutions
Entrust/Authority
  about 20
  access to 20
  services performed 20
Entrust/Authority database
  about 21
data stored in 21
Entrust/Authority Master Control
  about 20
  tasks used for 20
  used by 20, 29
Entrust/AutoRA 26
  See also complementary applications and devices
Entrust/Direct 24
  See also Web solutions
Entrust/Entelligence 23
  See also desktop solutions
Entrust/Express 24
  See also e-mail solutions
Entrust/getAccess 25
Entrust/ICE 23
  See also desktop solutions
Entrust/PKI
  about 19
core components 19
  expanding 22
  managing 28
Entrust/ProfileServer 26
  See also complementary applications and devices
Entrust/RA
  about 20
tasks used for 20
  used by 29, 30, 31
Entrust/RA Toolkit 26
  See also toolkits
Entrust/SignOn 23
  See also desktop solutions
Entrust/Solo 23
  See also desktop solutions
Entrust/Timestamp 26
  See also complementary applications and devices
Entrust/Toolkit for Java 26
  See also toolkits
Entrust/Toolkit for SSL/TLS 26
  See also toolkits
Entrust/Toolkit for Visual Basic 26
  See also toolkits
Entrust/TrueDelete 23
  See also desktop solutions
Entrust/TruePass 24
  See also Web solutions
Entrust/Unity 24
  See also e-mail solutions, Web solutions
Entrust/VPNConnector 25
  See also VPN solutions
Entrust/WebConnector 24
  See also Web solutions
Entrust@YourService 38
EntrustFile Toolkit 26
  See also toolkits
EntrustIPSec Negotiator Toolkit 26
  See also toolkits
Entrust-Ready applications 22
Entrust-Ready cryptographic hardware devices 26
  See also complementary applications and devices
EntrustSession Toolkit 26
  See also toolkits
ERP solutions 25
  establishing trust with other PKIs 17
  expanding Entrust/PKI 22

G
getAccess
  See Entrust/getAccess
going for assistance
  See support
guaranteeing information in certificates
  See Certification Authority
H
hardware devices
See Entrust-Ready cryptographic hardware devices
hash code 10
hierarchical trust 18

I
Informix database
See Entrust/Authority database
installation, integration, and testing 33
See also deployment issues and considerations

K
key
back-up 17
history 17
recovery 17
See also encryption public key, decryption private key,
signing private key, verification public key

L
locking data
See encryption

M
managing Entrust/PKI 28
See also Entrust/PKI
Master User
about 29
documentation used 29
tasks 29

N
networks
as used by a PKI 15
traffic on 21
non-repudiation of digitally signed data 18
See also digital signature

O
operations and maintenance 34
See also deployment issues and considerations
outsourcing 38

P
peer-to-peer trust 17
PKI
See public-key infrastructure
plug-ins
See complementary applications and devices
private key
See decryption private key, signing private key
products
See expanding Entrust/PKI
profile 31
project initiation and planning 32
See also deployment issues and considerations
public key
association with a certificate 13
See encryption public key, verification public key
public-key infrastructure
about 15
advising on 38
basis for security solutions 7
core services
automatic update of key pairs and certificates 17
certificate retrieval from a certificate repository 17
certificate revocation 17
client software 18
enabling trust through a Certification Authority 16
establishing trust with other PKIs 17
key back-up, history, and recovery 17
non-repudiation of digitally signed data 18
deployment issues and considerations 32
further information on 39
underlying concepts 7

R
RapidPKI
See Entrust *RapidPKI* Deployment Methodology
recovering keys 17
requirements analysis and design 33
See also deployment issues and considerations
retrieving certificates from a certificate repository 17
revoking certificates 17
root of trust 18

S
Secure Sockets Layer (SSL) 38
security
about 6
requirements for
individuals 6
organizations 6
planners and administrators 6
through cryptography 7
Security Officer
about 29
documentation used 29
tasks 29
sending comments to Entrust Technologies 35
services
Entrust.net 38
Entrust@YourService 38
signing digital signatures
See digital signature
signing key
See signing private key
signing private key 10
strict hierarchy 18
support 35–37
e-mail 36
online 36
telephone 36
symmetric-key cryptography 7

T
third-party trust 14
toolkits 26
training and certification 37
transparency 15
trust 14, 17
hierarchical trust 18
peer-to-peer trust 17
third-party trust 14

U
unlocking data
See decryption
user roles
See managing Entrust/PKI

V
verification key
See verification public key
verification public key 10
verifying digital signatures
See digital signature
Virtual Private Networks
See VPN solutions
VPN solutions 25

W
Web portals 25
Web solutions 24
what can Entrust do for you 6
who should read this document 5
Wireless Application Protocol (WAP) 38
wireless devices 38
Wireless Transport Layer Security (WTLS) 38