

Entrust Managed Services PKI™

Getting started with digital certificates and Entrust Managed Services PKI

Document issue: 1.0

Date of issue: May 2009

Copyright © 2009 Entrust. All rights reserved.

Entrust is a trademark or a registered trademark of Entrust, Inc. in certain countries. All Entrust product names and logos are trademarks or registered trademarks of Entrust, Inc. in certain countries. All other company and product names and logos are trademarks or registered trademarks of their respective owners in certain countries.

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

Export and/or import of cryptographic products may be restricted by various regulations in various countries. Export and/or import permits may be required.

Obtaining technical support

For support assistance by telephone call one of the numbers below:

- 1-877-754-7878 in North America
- 1-613-270-3700 outside North America

You can also email Customer Support at:
support@entrust.com

Public Key Infrastructure, digital certificates, and digital signatures

This chapter provides an overview of PKI technology, digital certificates, and digital signatures. The intention is to help you understand what exactly digital certificates do.

The chapter includes the following topics:

- [“PKI technology” on page 3](#)
- [“Digital certificates” on page 4](#)
- [“Digital signatures” on page 6](#)

PKI technology

PKI is an acronym for Public Key Infrastructure, which is the technology behind digital certificates. A digital certificate fulfills a similar purpose to a driver’s license or a passport—it is a piece of identification that proves your identity and provides certain allowances. A digital certificate allows its owner to encrypt, sign, and authenticate. Accordingly, PKI is the technology that allows you to encrypt data, digitally sign documents, and authenticate yourself using certificates.

As the word *infrastructure* in Public Key Infrastructure implies, PKI is the underlying framework for the technology as a whole—it is not a single, physical entity. PKI encapsulates various “pieces” that make up the technology, including the hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke digital certificates (Wikipedia).

An important piece of the PKI technology is the CA, which is the certification authority. The CA is the entity that issues digital certificates.

Cryptography

PKI technology is based on the science of cryptography. Cryptography allows data to be hidden, or encrypted, when transmitted over the Internet, and also translated back to its original form, or decrypted. But not just anyone can decrypt an encrypted message, and this is where PKI's asymmetric cryptography, also known as Public-key cryptography, comes in.

Public-key cryptography involves two complimentary keys that perform either the encryption or decryption process. These keys are created and used in pairs of matched "public" and "private" keys. So every user in a PKI system will have a key pair consisting of a public key and a private key. As the names of the keys suggest, the public key is openly available to anyone looking for it, while the private key is kept secret by its owner.

The analogy often used to describe public-key cryptography is a locked mailbox, where the private key is a physical key. Anyone can put a document into the slot of the mailbox, but only the person with the physical key (or private key) can unlock the mailbox to remove the document.

Digital certificates

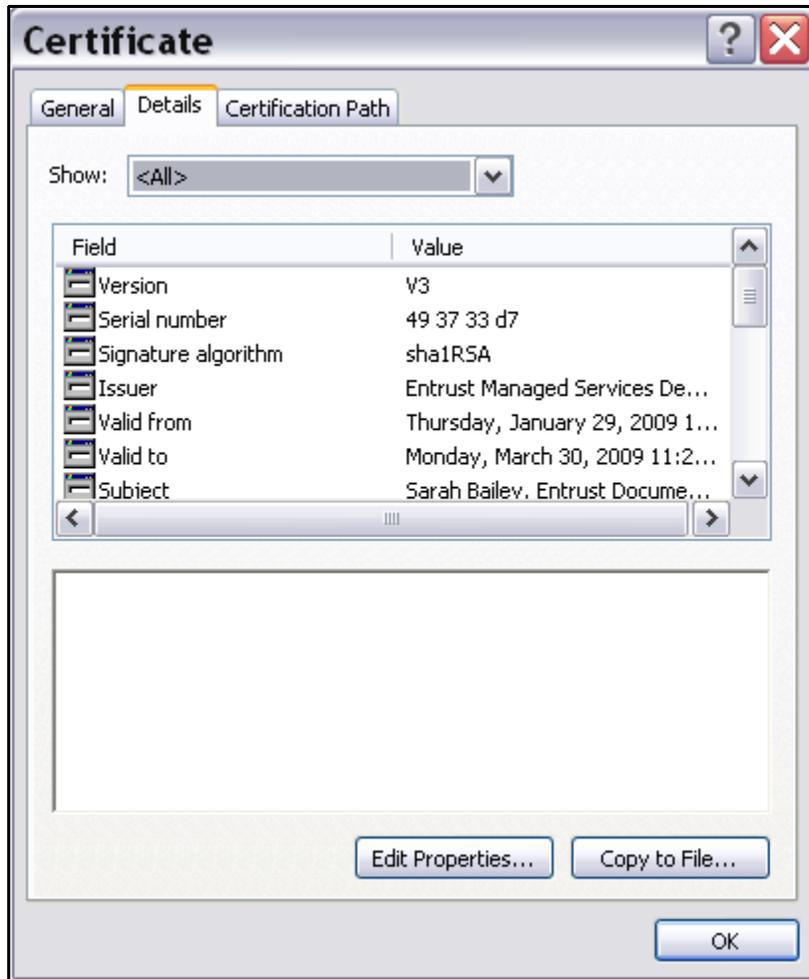
Digital certificates are electronic documents that serve as the holder's identification, much like passports or driver's licenses do outside of the world of electronic communication. It is the CA that issues digital certificates and because it issues them, the CA also attests to the validity of the certificate—to prove to others that the holder of the certificate is who they say they are. To do this, the CA certifies the identity of the certificate holder by applying its own digital signature. The CA's digital signature authenticates itself as the issuer of the certificate, verifies that the certificate has not been altered since it signed it, and binds it to the signing activity.

Each certificate the CA issues is unique. It contains the holder's name, serial number, the expiration dates (or validity dates) of the certificate, the public key of the certificate holder, which is used for authentication and encryption, and the digital signature of the issuing CA.

Digital certificate contents

The contents of a digital certificate are available in plaintext for anyone to see, because it does not contain any sensitive information that needs to remain confidential. You need to be able to view the contents to decide whether you can trust the certificate and certificate holder, much like you need to view the contents of a driver's licence to determine the holder's allowances (such as whether the holder requires prescriptive lenses to drive).

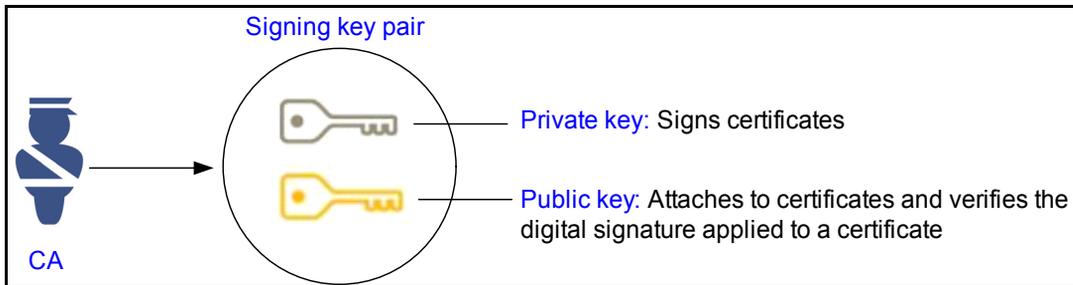
Figure 1: Digital certificate contents



Even though a certificate's contents are not encrypted, it does not open up the certificate for tampering. The CAs digital signature, which is placed on each certificate it issues, allows the CA to determine whether the certificate has been altered.

The CA has its own signing key pair, consisting of a private key and a public key. The CA uses its private key to sign the certificate and attaches its corresponding public key to the certificate so the digital signature can be verified.

Figure 2: CA signing key pair



The signature verification process aims to confirm or deny that the signature was signed with the corresponding private key. If a certificate is altered after the CA signed it, it will be discovered during the signature verification process. How it is discovered has to do with what happens when a digital signature is added to a document (see “[Digital signatures](#)” on page 6 for more information).

Digital signatures

Digital signatures are similar to handwritten signatures, but offer additional benefits and are a lot more secure.

When you digitally sign a document, you are doing three things:

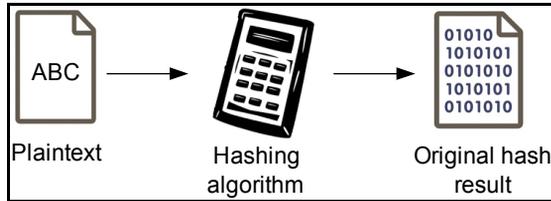
- You are confirming that you signed the document
- You are insuring the integrity of the document’s contents
- You are binding yourself to the signing activity—only you could have signed the document (you cannot later say that you did not sign the document while still keeping your private key private)

Digital signatures are based on public-key cryptography: two complimentary keys that encrypt and decrypt messages (the public key and the private key).

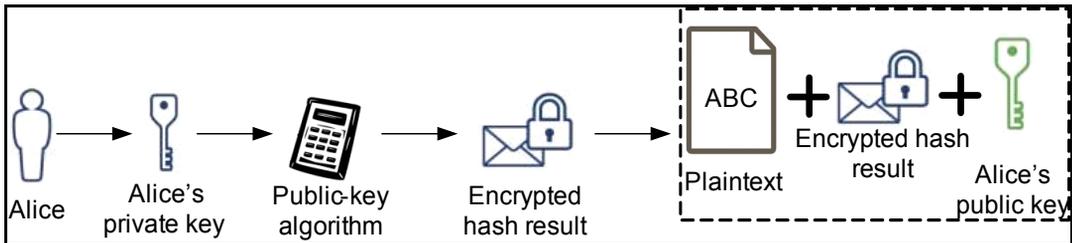
The digital signature process

The digital signature process helps explain how signatures ensure the integrity of data.

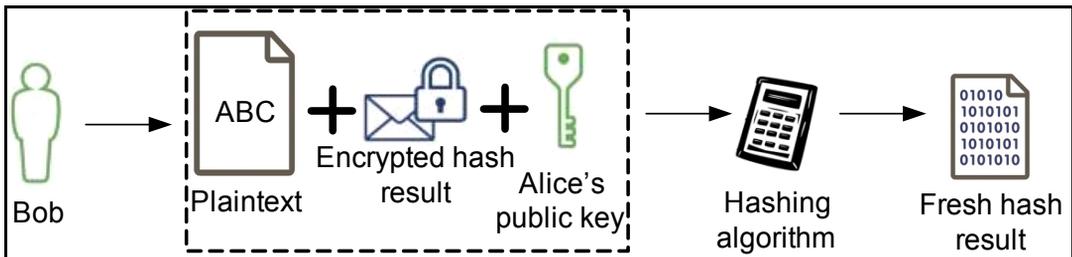
- 1 A hash of the data to be signed is produced.



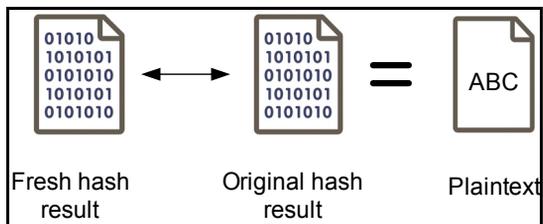
- The hash result is encrypted with the sender's private key and appended to the data. This protects the integrity of the hash result.



- The recipient of the data uses the corresponding public key, which is within the certificate, to decrypt the hash.



- A new hash result is created and compared with the original signed hash result. If the hash codes match, the data has not been altered. The recipient can also verify the sender, because only the possessor of the private key could have signed the message.



Entrust Managed Services PKI overview

Entrust Managed Services PKI gives you the benefits of a fully managed public key infrastructure (PKI) right on your end-users' desktops and laptops. This includes PDF and Office document signing, encryption, secure e-mail, digital signatures, sender verification, and resource authentication.

Setup is easy and quick. Authenticating to VPN devices, as well as encrypting and signing documents and e-mail is a few clicks away in familiar desktop applications. There is no steep learning curve. The benefits of managed certificates are immediate.

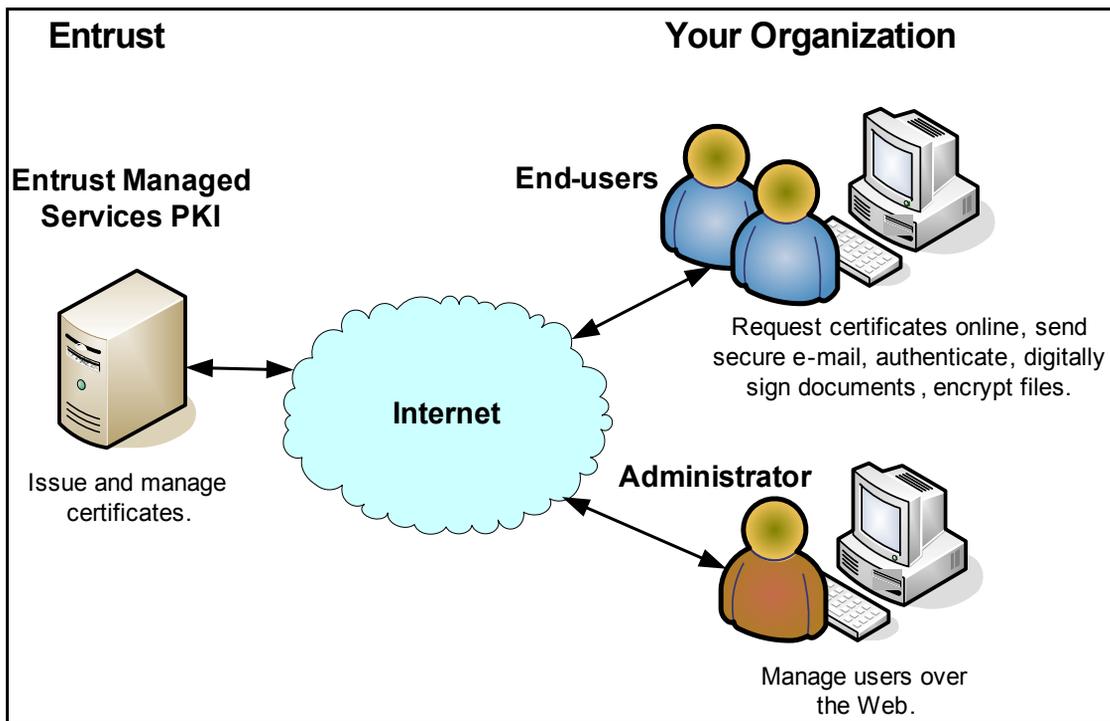
This chapter includes the following topics:

- [“How Entrust Managed Services PKI fits into your business” on page 10](#)
- [“Entrust Managed Services PKI architecture” on page 11](#)
- [“Getting started with Entrust Managed Services PKI” on page 13](#)
- [“What you can do with your Entrust digital certificate” on page 14](#)

How Entrust Managed Services PKI fits into your business

Entrust hosts the Certification Authority (CA), which issues and manages certificates, and other PKI components at secure hosted facilities. An administrator at your company creates user accounts through a simple Web interface and recovers users if a certificate or password is lost. Once end-users enroll their certificates—a process that takes just minutes—they can continue with their usual tasks but with the added ability to authenticate, sign, and encrypt documents and messages.

Figure 1: Managed Services PKI and you



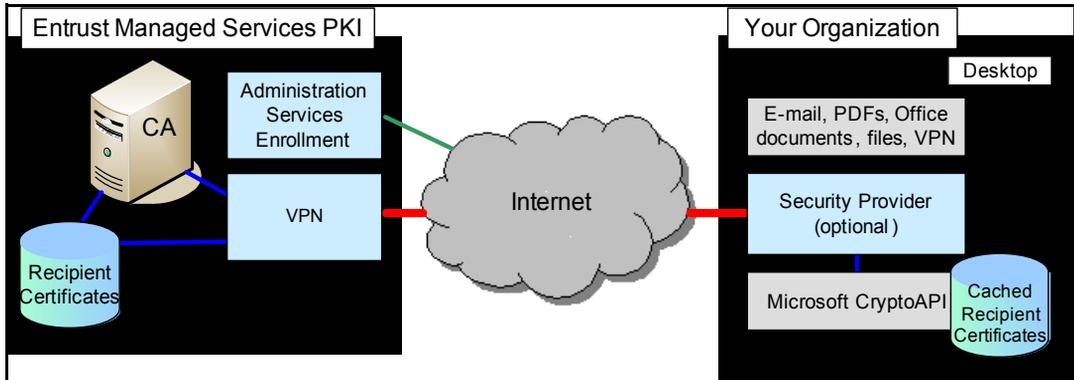
For a more detailed view, see [“Entrust Managed Services PKI architecture” on page 11.](#)

Besides signing and encrypting documents, files, and messages, you can use certificates to authenticate over remote access, to secure electronic forms, and much more.

Entrust Managed Services PKI architecture

Entrust hosts the Certification Authority (CA) and supporting components at secure facilities. You use a browser to access Administration Services and request certificates for users. The users then download their certificates and begin using them to secure data. The result is a secure infrastructure for certificate management, digital signing, and data and resource authentication.

Figure 2: Managed Service architecture with Security Provider



Entrust hosts the following components shown in Figure 2 within state-of-the-art secure facilities:

- **CA** – This is the Certification Authority assigned to a customer. It ensures the trustworthiness of digital identities by digitally signing the certificates, thereby ensuring the integrity of the digital identity. It also manages revocation lists, key history, and other PKI features.
- **VPN** – This service allows client applications, like Entrust Entelligence Security Provider for Windows, to securely communicate with an Entrust CA and back-end servers over the Internet, without requiring customers to make major changes to existing firewall settings.
- **Administration Services Enrollment** – This service allows administrators, using a browser at a customer site, to create user accounts and to recover user's digital IDs if lost.
- **Recipient Certificates** – This is a repository of certificates belonging to users and their e-mail recipients. The repository may also contain revocation data to enable the CA to check certificate validity.

The following components shown in [Figure 2 on page 11](#) reside on your end users' desktops:

- **E-mail, PDFs, Microsoft Office documents, files, and VPN**– You can authenticate, encrypt, and sign documents created in Microsoft Word, Excel,

Outlook, PowerPoint, and similar tools. Any file or document in Windows folders can be encrypted once your Entrust Managed Services PKI service is up and running.

- **Security Provider** (optional)– This refers to Security Provider for Windows and Security Provider for Outlook. These products interact with Microsoft CryptoAPI to provide enhanced PKI services, including initial certificate enrollment and keeping credentials up to date without user intervention. Security Provider for Outlook integrates with Microsoft Outlook to provide enhanced e-mail security. Security Provider acts as a client-side secure communications server by wrapping data packets in HTTPS. The wrapped data packets are sent to Managed Services PKI over port 80.

Note: You do not need Security Provider to use Entrust Managed Services PKI, but it provides additional benefits. See *Why you should use certificates with Entrust Entelligence™ Security Provider*, available under the **Resources** tab of www.entrust.com/managed_services.

- **Microsoft CryptoAPI** – The Microsoft Cryptographic application programming interface allows desktop applications, such as remote access, VPN, and Adobe Acrobat, to take advantage of cryptographic functionality built into Microsoft Windows.
- **Cached Recipient Certificates** – This is a repository of certificates harvested by Security Provider for Outlook from incoming e-mail and from e-mail recipients in outgoing messages. This cache of certificates lets users compose e-mail to frequent recipients while working offline.

Getting started with Entrust Managed Services PKI

Once you sign up for Entrust Managed Services PKI, it is easy to get up and running. Your organization requires an administrator—also known as a local registration authority (LRA)—whose duty it is to manage end-users and their certificates. The LRA must:

- complete the creation of an administrator certificate
- set up end-users so that they can create their certificates

For detailed information on creating an administrator certificate and creating end-user accounts, see the *Entrust Managed Services PKI Administrator Guide* available under the **Resources** tab at www.entrust.com/managed_services.

For a full list of tasks you can perform with your digital certificate and accompanying documentation, see “[What you can do with your Entrust digital certificate](#)” on [page 14](#).

What you can do with your Entrust digital certificate

Digital certificate contents are stored in a standards based format called x509. As a result, the majority of devices and applications accept this format, thereby ensuring compatibility.

Note: All Entrust Managed Services PKI documentation is available under the **Resources** tab at www.entrust.com/managed_services.

Table 1: Task and related documentation

If you want to...	See this guide	Description
obtain an administrator certificate and create end-user accounts	<i>Entrust Managed Services PKI Administrator Guide</i>	This guide documents how to create an administrator certificate and how to create end-user accounts.
obtain an end-user certificate using a Web-based application called Administration Services	<i>Getting an end-user Entrust certificate using Entrust Authority Administration Services</i>	This guide documents how to obtain an end-user certificate using Administration Services. It also briefly describes how to use the certificate and provides documentation resource information.
obtain an end-user certificate using Security Provider	<i>Getting an end-user Entrust certificate using Entrust Intelligence Security Provider</i>	This guide documents how to obtain an end-user certificate using Security Provider. It also briefly describes how to use the certificate and provides documentation resource information.
sign and/or encrypt PDF documents (files and forms)	<i>Using Entrust certificates with Adobe PDF files and forms</i>	This guide documents how to configure Adobe to recognize and trust digital certificates, and how to digitally sign a PDF document.

Table 1: Task and related documentation

If you want to...	See this guide	Description
sign and/or encrypt Microsoft Office documents	<i>Using Entrust certificates with Microsoft Office and Windows</i>	This guide documents: <ul style="list-style-type: none">• Signing and sending messages using Microsoft Word, Excel, and PowerPoint• Sending secure messages using Microsoft Outlook• Configuring Microsoft Outlook to use a single certificate• Removing message encryption in Microsoft Outlook
sign and/or encrypt files on your Windows operating system.	<i>Using Entrust certificates with Microsoft Office and Windows</i>	This guide documents how to secure Windows files and folders and send a secure message from a Windows folder.
authenticate to a VPN for secure, remote access to your network	<i>Using Entrust certificates with VPN</i>	This guide includes information about IPsec and SSL VPN, security issues, and VPN authentication mechanisms. It also provides instructions on how to import your certificate into your VPN client and how to configure your router to trust certificates issued to VPN clients.

