Entrust® Securing Digital Identities & Information

SECURITY ON

Entrust Managed Services PKI

Strong User Authentication on the Web

This document describes the importance of using certificates to authenticate users external to your network over the Web as a means of protecting your application or network from unauthorized access. It also identifies the value of using Entrust Managed Services PKI to employ certificate-based authentication.

How do I achieve strong authentication over the Web?
Various approaches can be used to properly authenticate over the Web. The most effective and secure mechanism, however, is the use of digital certificates, which are based on public key infrastructure (PKI) technology.

Certificates are issued by a certification authority (CA) and use the x.509 standards-based format. Because it is a standard format, it is accepted by the majority of applications on both Microsoft® Windows® and other third-party operating systems.

Unlike other mechanisms for Web-based authentication, certificates ensure the person or machine is who they claim to be.

Why issue certificates to users accessing my network over the Web?
Organizations may have little influence over users outside their network; computers outside the network, because unmonitored, are security risks. The computer, for example, might be unsafe for transmission of sensitive data (e.g., a public kiosk from which others can extract intellectual property or sensitive data).

By issuing certificates to users accessing your application or network over the Web, you enable certificate-based authentication; only those users to which you issue a certificate are authorized for access. This allows you to keep sensitive data and transmissions secure, as a PKI system, if implemented correctly, is impervious to man-in-the-middle (MITM) attacks.

> *When PKI and the use of trusted CAs is employed, strong authentication can be achieved between two parties involved in electronic transactions (e.g., over the Internet). Strong authentication is the cornerstone for performing secured on-line transactions, and can help many organizations avoid traditional security risks such as MITM attacks, eavesdropping, traffic analysis, replay attacks and denial of service attacks.*[1]

Certificate-based authentication over the Web also provides data encryption capabilities between the client, on one side of the network, and the server on the other.

[1] Using PKI to prevent man-in-the-middle attacks, Secure Identity Services Accreditation Corporation (SISAC).

Who should issue certificates outside the enterprise?
Any organization that collaborates online with employees, partners and customers outside their network, and does not want unauthorized individuals to access their applications or network, should issue certificates.

Users with certificates can authenticate to Web page applications, such as a banking site or an eCommerce site (for online purchases), and into the enterprise through IPSec or SSL VPN connections.

What ways can I use certificates?
Certificates issued to external users or machines can be used:

- For mutual (or two-way) SSL authentication, which is built into every Web browser and Web server.

  With mutual authentication, the client or user authenticates to the server, and the server, in turn, authenticates itself to the client or user. In this way, both parties are assured of each others' identity. Mutual SSL also provides authentication and non-repudiation of the client authentication (depending on how the key was created), which regular SSL does not.

  Using certificates with SSL is easy and economical to deploy, as no software is required.
- With various network protocols (SSL, SFTP, SSH, etc.)
- With HTTPS connections (often used for online transactions)
- With cloud computing environments, which includes the software-as-a-service (SaaS) deployment model

To satisfy those organizations whose users use multiple machines, certificates can be portable. You can export the certificate and place it on another machine, or you can store it on a smart card or token. Smart cards and tokens are the most secure place to store a certificate's private key.

They also lower the complexity and cost of managing your certificate and keys, since it removes the requirement of creating multiple copies of your certificate and keys to achieve portability. For organizations that do not want portability, you can configure the private key to be non-exportable.

How does it work?
End-users of Microsoft Windows and other operating systems request a certificate (private/public key pair) over the Internet through a Web-based application.

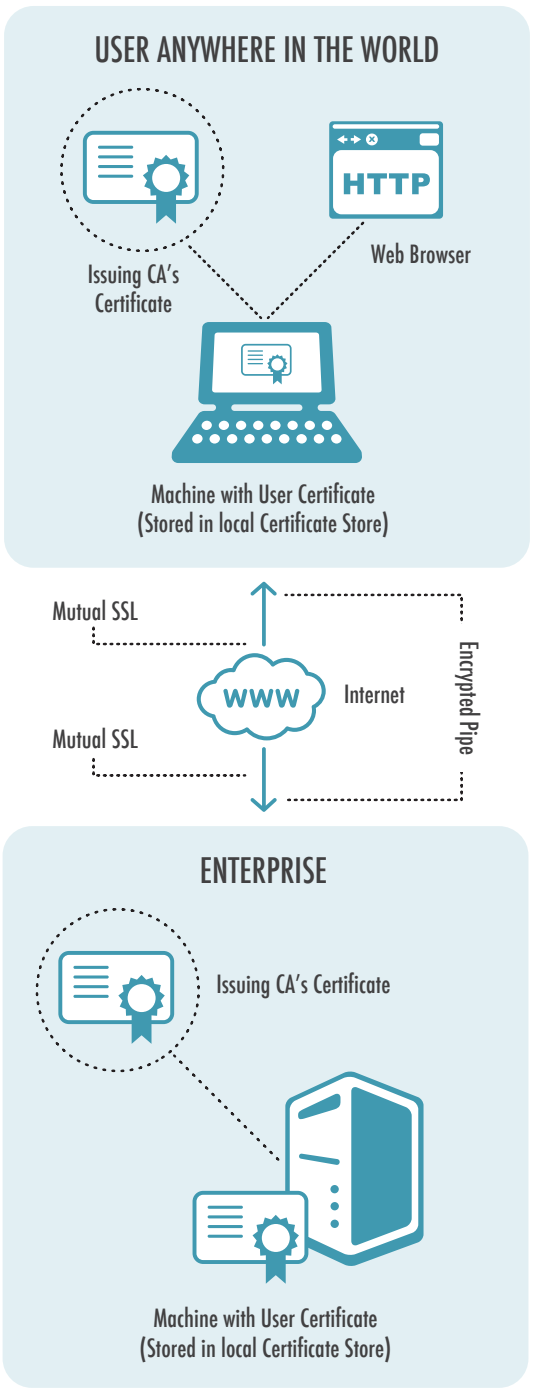
The certificate contains a copy of the user's public key, which is bound to the identity of the certificate holder. The certificate is signed by the certification authority (CA) to establish trust.

The certificate cannot be altered in any way without destroying the signature of the issuing CA, thereby invalidating the certificate and rendering it useless.

When a user attempts to access a network where certificate-based authentication is required, the authentication mechanism checks the credentials of the user.

This involves communication between the machine with the certificate, the authentication mechanism, and the authentication server. The user cannot access the protected side of the network until its credentials are verified by the authenticator.

Certificates issued outside the network authenticate to your network over the Internet and encrypt data between the client and server.



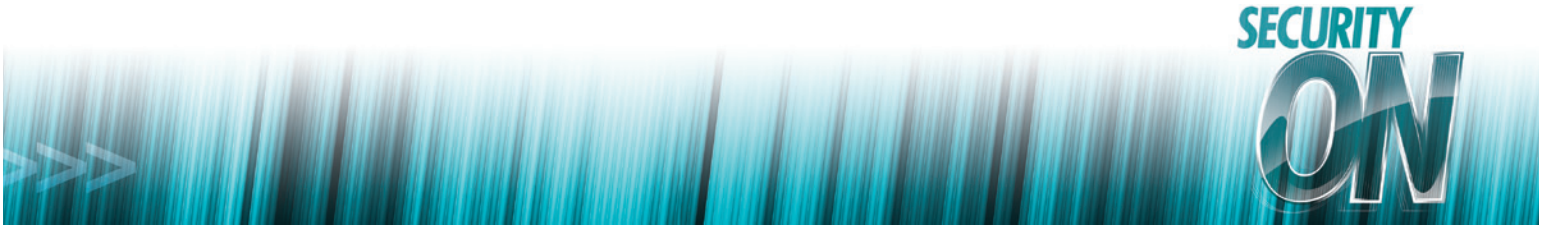
The value of Entrust Managed Services PKI
Entrust Managed Services PKI operates over the Web. It is designed to issue certificates to people or machines both inside and outside the enterprise, using a variety of different enrollment methods.

This is an advantage over a Microsoft CA, which cannot easily issue certificates outside the enterprise due to its dependence upon Microsoft Active Directory for storing users.

With Entrust Managed Services PKI, you can easily issue certificates outside the enterprise and effortlessly import them into the required certificate store.

Administrators have configurable control over certificate issuance with the option of approving all certificate requests. Administrators can also view reports identifying all issued certificates and the status of each certificate, on servers and clients, such as a wireless access point or a UNIX server.

Entrust Managed Services PKI provides an easy-to-use, feature-rich solution for protecting your network from unauthorized access outside the enterprise at a significantly lower cost than other vendors.



Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but affordable in today's uncertain economic climate.

More Information

For more information on Entrust Managed Services PKI, contact the Entrust representative in your area at **888-690-2424** or visit **entrust.com/managedpki**.

Company Facts
Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 globally

Headquarters
Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, TX 75240 USA

Sales
North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

About Entrust
A trusted provider of identity-based security solutions, Entrust secures governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL. For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Entrust® Securing Digital Identities & Information

23781/4-10