Entrust® Securing Digital Identities & Information

SECURITY ON

Entrust Managed Services PKI
Machine Certificates Inside the Enterprise

By issuing certificates to machines, you permit authorized machines to access the network by authenticating to other machines, devices or servers — in either Microsoft® Windows,® Linux or UNIX environments — using a certificate. This allows authorized machines to access and share confidential data.

Other solutions for securing networks, including firewalls or network isolation (which prevents access to the Intranet/Internet), are either susceptible to attack or are not practical. Using certificate-based authentication for machines is the best way to secure a network.

The diagram below illustrates network connections where certificates can be used to secure the network through authentication and communication encryption. Digital certificates can be placed on each of the machines indicated, regardless of which operating system they run.

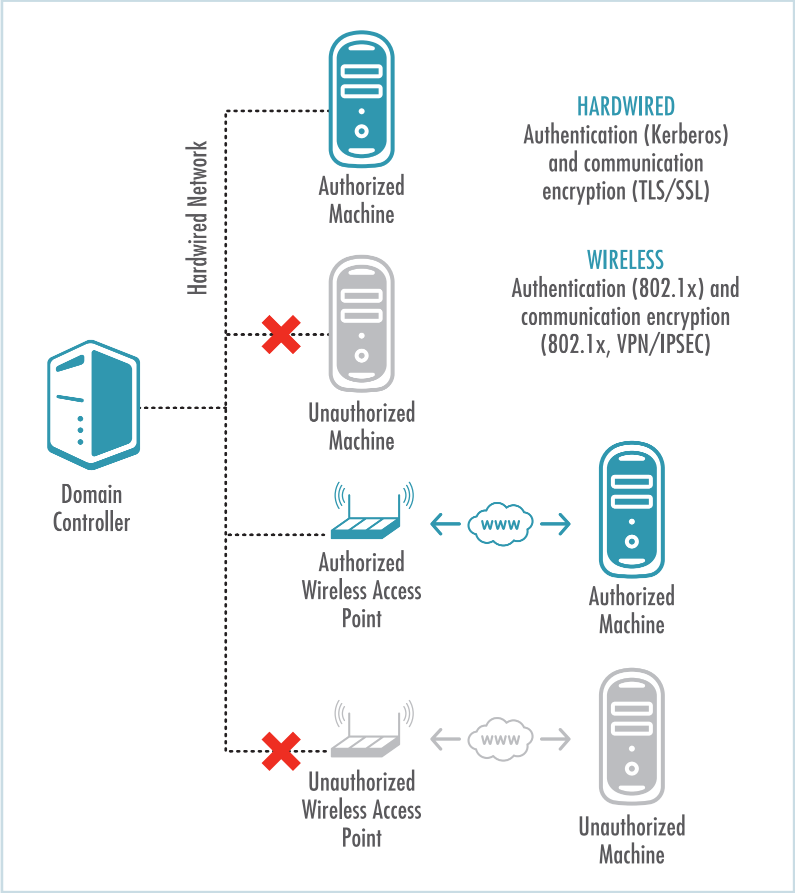

Hardwired Network
Authorized Machine
HARDWIRED
Authentication (Kerberos) and communication encryption (TLS/SSL)
WIRELESS
Authentication (802.1x) and communication encryption (802.1x, VPN/IPSEC)
Unauthorized Machine
Domain Controller
Authorized Wireless Access Point
www
Authorized Machine
Unauthorized Wireless Access Point
www
Unauthorized Machine

Figure 1: Securing the Network via Digital Certificates

How can certificates issued to machines help my organization?

- Prevents unauthorized machines from accessing your network
- Encrypts machine-to-machine communication
- Permits machines, both attended and unattended, to authenticate to the network over a wired or wireless network connection
- Enables machines not capable of participating in Kerberos protocol, such as UNIX servers, to authenticate to the network

Increase Security, Reduce Costs

Without certificate-based machine authentication, your network, intellectual property and customer data is susceptible to attack.

This can be a malicious attack with the intent to steal data, or an accidental attack, where an individual logs in to the network through a personal device that has a virus (not protected by the corporate virus software) that infects other machines on the network.

Organizations that use certificate-based machine authentication reduce developmental, acquisition, deployment and overall operational spending.

To reduce cost and risk of service outage from an expired certificate, Entrust offers the tools to automate the management of any certificate.

How Machine Certificates Work

Both Windows and non-Windows users request a certificate (private/public key pair) for each machine through a Web-based application provided by Entrust.

The certification authority (CA) signs each machine's public key, which is used by other machines in the network to establish trust for authentication purposes. The application places the certificate, along with its public key, in the machine's local certificate store.

When a machine attempts to access a network where certificate-based authentication is required, the authentication mechanism checks the machine for valid credentials.

This involves communication between the machine (and its credentials), the authentication mechanism and the authentication server. The machine cannot access or connect to the protected side of the network until its credentials are verified.

Machine credentials identify the machine, ensure the integrity of the machine and bind the machine to the transaction.

USER AUTHENTICATION ALONE IS NOT ENOUGH

Many different industries, such as health care, need to authenticate machines independently of users — user authentication alone is not enough. A situation where machine authentication is necessary to sustain a secure networking environment involves the transmission of sensitive data from one machine to another.

User authentication alone is not satisfactory, as the user can log in to the network from an unprotected computer. With machine-based authentication, the authentication mechanism (e.g., 802.1x for a wireless network connection) authenticates the machine to, for example, a wireless access point.

Once authenticated, it can be determined whether or not the sensitive data should be transmitted to the target machine. This prevents data from being sent to rogue machines.

Other examples where machine authentication, over user authentication alone, is necessary to achieve a secure networking environment are outlined in the following three scenarios.

Example 1:

A user accessing a Web server over a browser to obtain sensitive data.

An SSL certificate issued to a Web server allows the user to determine whether the connection is to the correct, authenticated Web server and whether the connection is from a machine that is protected from security threats (e.g., malware and cached browser pages).

User authentication cannot identify the authenticity of the Web server or determine whether the connecting machine is suitable for transmission of sensitive data.

Example 2:

An autonomous (independent) machine, such as a portable patient monitor used in the health care industry, sending data to another machine.

As is the case with portable patient monitors, or any other independent, mobile machine that needs to be operational from various locations (whether manned or unmanned), using network addresses as a means to permit communication over the network is not a satisfactory solution.

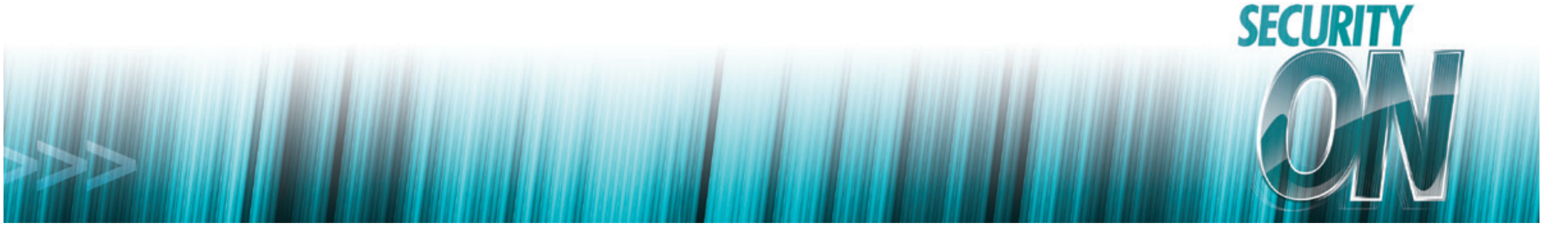
A machine certificate would ensure that the autonomous machine is sending the data to an identified and authenticated machine and that the received data is being sent from an authenticated machine. User authentication alone cannot provide sufficient network access security for autonomous machines.

Example 3:

An authenticated user logging in to an unknown machine within the network, such as a public access kiosk, to obtain sensitive data.

Even though the user is authenticated, the type of information requested, or communication desired, by the user is determined to be risky as a result of the non-authenticated machine being used.

Without a machine certificate, the machine cannot authenticate to the network, even if the user can provide personal credentials. This prevents sensitive data from being sent to unknown machines.



Entrust Managed Services PKI

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

Users can easily create machine certificates, effortlessly import them into a machine's local certificate store and execute management tasks, like automatic updates, against certificates.

The administrator has configurable control over certificate issuance, including administrator approval of certificate requests.

The software application provided to Microsoft Windows users allows the certificate creation process to be automated, which is useful if you need to deploy certificates to a large number of machines, or to machines spread across different locales.

When the client is installed on the machine that needs the certificate, it detects that a certificate is missing from the computer and communicates with Entrust Managed Services PKI to generate one automatically.

Administrators can also view reports identifying all issued certificates and the status of each certificate, on Windows and non-Windows servers and clients, such as a wireless access point or a UNIX server.

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