Entrust® Securing Digital Identities & Information

SECURITY ON

Entrust Managed Services PKI

Device Certificates

What is a Device Certificate?
A device certificate is an electronic document that is embedded into a hardware device and can last for the life of the device. The certificate's purpose is similar to that of a driver's license or passport: it provides proof of the device's identity and, by extension, the identity of the device owner.

Why use Device Certificates?
Using device certificates helps protect your services from unauthorized access, possibly by cloned devices. Typically, an organization injects certificates into devices which are then distributed across a large user base.

For example, a university might install certificates on smart cards intended for its student body. Or, a hydro company might install certificates on smart meters installed in customers' homes.

The device then uses the certificate to authenticate itself, as well as the student or paying customer it is representing. If authentication succeeds, the device and corresponding user are granted access to the requested service — be it a university intranet, hydro service, satellite, banking system, subscription music site and so on. If authentication fails, as is the case if no certificate is present, then access is denied.

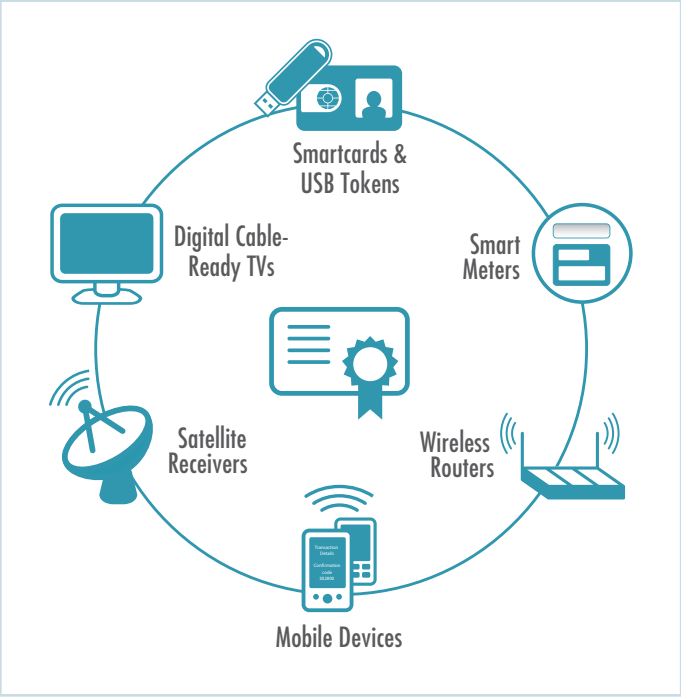

Figure 1: Devices

How can device certificates help secure my organization?

- Prevent cloning of devices
- Prevent access from rogue devices
- Reduce pirating of services such as Voice Over IP (VOIP), broadband and satellite signals
- Provide a cost-effective authentication solution; for example, smartcards with embedded certificates are cheap to print and deploy, and require very little ongoing support
- Add functionality beyond authentication; for example, a smartcard with a certificate can be used to sign and encrypt email
- Minimize support costs as the users don't have to add a certificate to their device themselves; the certificate is already on the device when a user receives it, and can continue to remain valid for the life of the device

Entrust Managed Services PKI

- Cross-certification with popular bridges such as the Federal Bridge CA
- Certificate revocation capabilities
- Private key generation at your site
- Separate trust domains using sub-CAs
- Custom Certificate Policy
- Certificate Practice Statements (CPS)

How Does it Work?
Figure 2 shows the high-level process for adding a certificate to a device. Following the figure are detailed examples of how to add certificate to smart meters and smart cards. These processes can be automated and customized.

Scenario 1 — Adding a Certificate to a Smart Meter

1. The smart meter manufacturer sends Entrust a file with 40,000 serial numbers — one serial number per smart meter.
2. Entrust generates one key pair (private and public) and one certificate per serial number.
3. Entrust returns a file containing the key pairs and certificates within 24 hours. The certificates have a 15- to 20-year life.
4. The manufacturer injects a certificate into the appropriate smart meter. The certificate can now be used to authenticate the smart meter device, which represents a paying customer.

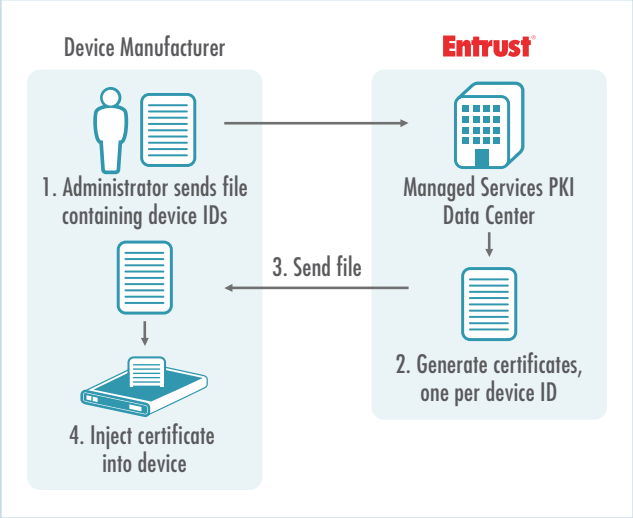

Figure 2: Issuing a certificate to a device

Scenario 2 — Adding a Certificate to a Smart Card

1. A university sends Entrust a file with 40,000 student numbers.
2. Entrust generates one key pair (private and public) and one certificate for each student.
3. Entrust returns a file containing the key pairs and certificates within 24 hours. The certificates typically have a four- to five-year lifespan matching the life of the smartcard or the student's tenure.
4. A printer with a smartcard-encoder prints the student's photo and name while simultaneously placing the certificate onto the smart card. The smartcard is then given to the student.
5. The certificate can now be used to authenticate the smartcard, and the corresponding student, to the university website. The ID can also be used for building access.

The Hands-Off Approach: Entrust Managed Services PKI

Entrust Managed Services PKI is the cost-effective approach for your device certificate needs.

Turnkey, Fast Deployment. You'll receive certificates within 24 hours of supplying your device IDs.

Simple to Deploy. All hardware and software required to generate certificates is hosted by Entrust in a 24x7x365 state-of-the-art facility.

Cost-Effective. Entrust offers certificates at a significantly lower cost than other vendors.

Scalable. Easily add more devices as your requirements evolve.

Compliant. Entrust issues PKI-based X.509 certificates.

[1] Optionally, you can generate the key pair on your premises and send the public key portion to Entrust for certificate creation. The private key stays at your site. Another option is to create the certificate yourself using your own in-house Entrust PKI.

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

23860/4-10