



## Entrust Managed Services PKI™ Smart Card Logon

Document issue: 1.0  
September 2009

### What is Smart Card Logon?

Smart Card Logon is an optional Windows feature that enables users to log in to the Windows operating system using a smart card and PIN (figures 1 and 2). It replaces the default user name and password login mechanism. Smart Card Logon is considered a two-factor authentication method because:

- Users must present something they have (the smart card) and
- Users must present something they know (the PIN)

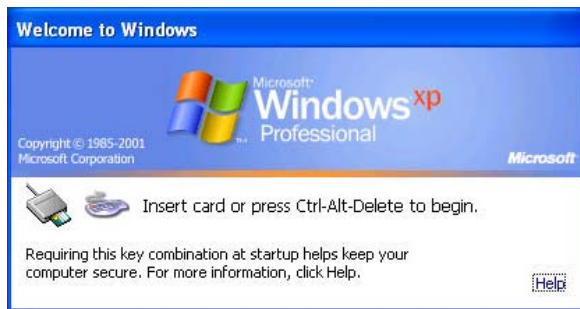


Figure 1: Smart Card Logon locked dialog

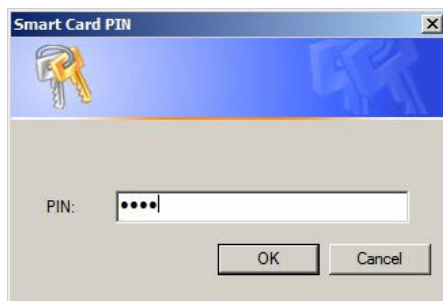


Figure 2: A PIN entry dialog

### Why a user name and password is not enough

User name and password authentication is considered too insecure by many organizations because:

- User names can be easily guessed or deduced from public information such as an email address, business card, or pay stub. With the user name

determined, only a password is left to protect your sensitive data.

- Memorable passwords are typically short and often don't include numbers or special characters. They're easy to remember, but also easy to crack by a brute force attack.
- Long passwords with a good mix of letters, numbers and special characters are hard to crack; however, they're also hard to remember. People tend to write them down, on a piece of paper, in a notebook, or in other indiscrete areas.

Because of the vulnerabilities inherent in user name and password authentication, many organizations are opting to use a second-factor authentication mechanisms such as Smart Card Logon to achieve greater security.

### How can Smart Card Logon help my organization?

Smart Card Logon helps your organization in these ways:

- **Greater protection of administrator accounts.** Administrator accounts have 'power-user' permissions that the average user account doesn't. For example, administrator accounts can change user passwords, remove user accounts, change people's access rights, take Web sites offline, and so forth. If an attacker were to gain access to such an account, he could bring down your entire network. Relying on user name and password to protect these sensitive accounts is simply too risky. Smart Card Logon provides a much more secure option because an attacker would have to steal the smart card and know the PIN in order to log in to the account.
- **Improved remote access security.** Remote users are not subjected to the same physical access controls as local users. For example, local users must be physically recognized to gain access to your office building. They might also need to swipe an ID badge. These controls are not in

place for remote users, so organizations use Smart Card Logon to fill the gap. With Smart Card Logon, physical control is achieved through the smart card, which remote users must have in their possession in order to log in.

- **Higher integrity for logon credentials.** Smart Card Logon requires that there be a certificate embedded on the smart card. A certificate is an electronic document that identifies the user, and is validated whenever a user logs on. A certificate carries the same authoritative weight as a passport, and therefore includes many layers of protection to make it highly resistant to forgery.
- **Increased accountability.** Just as it is extremely hard for an imposter to pose as you because they must steal your smart card and know your PIN, it is similarly hard for you to deny that you logged in with your smart card. Users are more closely bound to their actions when Smart Card Logon is in use.
- **Memorable PINs without compromising security.** Unlike a password, a PIN doesn't have to be long and random because an attacker would have to physically obtain the smart card before they could even attempt to crack the PIN. Put another way, any shortcomings in the PIN's length or randomness are more than compensated for by the requirement of physical possession of the smart card. Moreover, PINs never leave the smart card itself, and therefore cannot be intercepted by packet sniffers on your network.
- **Multi-purpose uses.** You can integrate smart cards with physical access controls such as door locks, turnstiles, and elevators. Smart cards can also be used to encrypt email and digitally sign data such as Word documents and Adobe PDFs.

## How to get certificates onto smart cards

Figure 3 illustrates the process for getting a certificate onto a smart card using Entrust Managed Services PKI. This process can be customized.

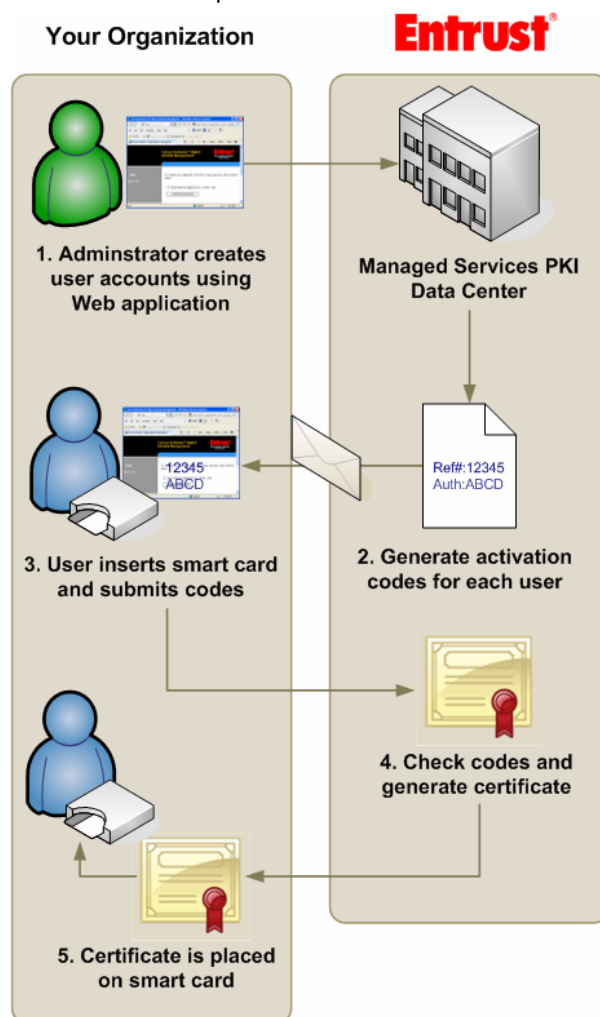


Figure 3: Issuing certificates to smart cards

## The value of Entrust Managed Services PKI

Entrust Managed Services PKI provides the mechanisms for adding certificates to smart cards for use with Smart Card Logon. Entrust's offering delivers these benefits:

- **Wide variety of certificate deployment options to suit every budget.** Entrust offers complete automation, self-service, bulk-loading, client-side software options, and more.
- **Compliant.** Entrust supports any Personal Computer/Smart Card (PC/SC)-compliant smart cards and any Plug and Play smart card readers.
- **Turn key deployment with no complex software.** All hardware and software required to add

certificates to smart cards<sup>1</sup> is hosted by Entrust in a 24X7X365 state-of-the-art facility.

- **Low cost.** Entrust offers certificates at a significantly lower cost than other vendors.
- **Scalable.** Add more users as-needed. Entrust scales as your organization grows.
- **Revocation.** Built-in mechanisms for revoking lost or stolen smart cards are available.

### References

*Secure Access Using Smart Cards Planning Guide* available at <http://technet.microsoft.com>.

**Contact:** Call: 888-690-2424, email: [entrust@entrust.com](mailto:entrust@entrust.com)

**For more information,** see [http://www.entrust.com/managed\\_services](http://www.entrust.com/managed_services).

<sup>1</sup> Excluding smart cards and smart card readers.