

Entrust Smartcard & USB Authentication

Entrust IdentityGuard smartcard- and USB-based devices allow organizations to strongly authenticate user identities before granting access to networks, facilities, devices and more.

Whether required by internal policy, industry mandates or government regulations, strong authentication is the cornerstone of securing enterprise environments.

Enhance Security, Increase Usability

Entrust IdentityGuard smartcards and devices integrate seamlessly into the software authentication platform and either Entrust Authority Certification Authority or Microsoft Certification Authority.

The Entrust IdentityGuard platform, which offers one of the widest ranges of authenticators on the market, allows organizations to issue the right authenticator for the situation, which may not always be a smartcard — maximizing security while minimizing cost.

Entrust smartcards and USBs allow companies to utilize the most advanced smartcard technology to reduce the number of authenticators while increasing security, functionality and usability.

By using the latest chip technology, Entrust cards operate up to two times faster than the competition, while incorporating the latest hardware resistant to attacks that attempt to steal identities. Entrust's multipurpose smartcards help organizations realize true physical and logical access convergence.

Secure Biometric Storage

Entrust IdentityGuard provides organizations the capability to capture and store sensitive biometric data on the smartcard via a secure, tamper-proof method. Biometric data cannot be copied or modified without detection.

Further, the sensitive information cannot be released unless the cardholder provides a PIN or the card is read by a trusted card reader.

This unique ability, available via Entrust's FIPS 201-compliant solution, enables organizations to implement a policy that requires the use of advanced biometric authentication (e.g., fingerprint scan to open a door or to reset a blocked PIN).

This technology can be extended to fight fraud in unlimited ways, including authenticating card holders before they vote, receive medical attention or even receive prescription medication at pharmacies.

Solution Details

- Enables security convergence for facilities, remote access, desktops and other applications
- Tailored for enterprise and government environments
- Smartcard and USB device mobility enables ability to digitally sign or encrypt from any location
- Based on Java Card Platform technology
- Compliant to FIPS 201 directive for PIV, PIV-I and PIV-C requirements
- Interoperable with Entrust or Microsoft CA
- Managed by award-winning Entrust IdentityGuard credential management system



Based on Java Card Platform

Entrust smartcards and USB tokens are based on the open Java Card platform. It's designed to allow for the addition of third-party applications — even after initial smartcard issuance.

Java Card technology is one of the most versatile, interoperable platforms for smartcards and secure USB tokens available. Some vendors use proprietary, in-house smartcard operating systems, which makes it difficult to buy off-the-shelf applications from trusted third-party security vendors.

This hinders advancement of the security environment and locks organizations into specific vendor hardware or software. Java Card's open approach ensures efficient upgrades are not only possible, but straightforward.

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.

The smart choice for properly securing digital identities and information, Entrust solutions represent the right balance between affordability, expertise and service. Discover how this will benefit you by contacting us at **888.690.2424**, email at **entrust@entrust.com** or visit **entrust.com**.

Feature	Benefit
Mixed deployment flexibility with secure smartcard and/or USB formats.	Employees have the freedom to use the form factor that best improves their effectiveness, without sacrificing an organization's ability to administer.
Dual-interface smartcards interoperable with both contact (ISO 7816) and contactless (ISO 14443) interfaces.	Make the investment once, then evolve where the smartcard is utilized over time. The contact interface works with low-cost desktop readers. Select the contactless interface for fast, secure facility access, or authentication and signing with NFC-enabled tablets.
Simultaneous legacy and modern PACs support for streamlined migration; issue and manage from a single Entrust IdentityGuard platform.	Reduce cost by improving security only where required. No need for complex, costly overnight replacements for physical access system. Avoid additional cost of two management systems.
Certificates seamlessly issued by Entrust IdentityGuard during smartcard issuance.	Meet PIV-I or PIV-C requirements from Entrust Managed Services PKI. Issue fully personalized smartcards with no need to involve the employee, citizen or consumer with complexities of certificate issuance or renewal.
Can be used with Entrust or Microsoft CA with very little user intervention.	Customer no longer needs to perform the expensive, time-consuming role of system integrator.

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**.

