



< Let's Talk

Entrust Smartcard & USB Authentication

Entrust IdentityGuard smartcards 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 Entrust IdentityGuard versatile authentication platform and Entrust Authority PKI. The platform, which offers one of the widest ranges of authenticators on the market, allows companies to broaden coverage, while minimizing the impact on employees, customers and partners.

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. 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 and the card is read by a trusted card reader.

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

Based on Java Card Platform

Entrust smartcards and USB tokens are based on the open Java Card platform. It's designed to streamline changes to card applications and configurations — even after initial smartcard issuance.

Java Card technology is one of the most versatile, interoperable platforms for smartcards and secure USB tokens available. Organizations also can increase efficiency with backward compatibility and cross-platform, cross-vender interoperability.

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.

Solution Details

- Enables convergence of security for facilities, remote access, desktops and 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



Form Factor Options		
Model	SC100 Series Smartcards	USB100 Series USB Tokens
Cryptographic Performance		
<i>Entrust real-world benchmarks include the full round-trip from computer to card and back.</i>		
RSA-1024, 2048		
Key Generation	Less than 5 seconds for 1024 / Less than 50 seconds for 2048	
Digital Signature	0.47 seconds for 1024 / 1.02 seconds for 2048	
Decryption	0.37 seconds for 1024 / 1.13 seconds for 2048	
Elliptic Curve Cryptography (ECC)		
Digital Signature / Verification	192-bit sign — 32 ms / 192-bit verify — 60 ms	
AES 256		
Decryption	< 12 us	
Triple DES		
Decryption	< 40 us	
Physical Access Options		
Mifare Option	1k, 4k	1k, 4k
125 kHz Proximity Option	Y	N
PIV Compliance		
PIV-C	Yes	
PIV, PIV-I	Requires 200 series*	
EEPROM Memory		
Capacity	80 Kb	
Read Cycles	Unlimited	
Write/Erase Cycles	500,000	
Data Retention Time	25 Years	
Hardware System		
Co-processors	DES, AES, RSA,ECC	
Connectivity		
Contact (ISO 7816)	Model SC100C	Model USB100C
Contactless (ISO 14443)	Model SC100CL	Model USB100CL
Dual Interface	Model SC100D	Model USB100D
USB 1.1/2.0	Not Applicable	Yes
Certification & Approvals		
FIPS 140-2 Level 3	Chip only; requires 200 series for full-device certification	
Common Criteria	EAL5+ (Chip & OS)	
EMVCo	Yes (Chip & OS)	
RoHS	Not Applicable	Yes
China RoHS	Not Applicable	Yes
Customization		
Card Customized with Organization Logo	Available on request	

* Model 200 includes Model 100 capabilities plus FIPS 140 and FIPS 201 certifications.

< Let's Talk

Application Options		
Application	X.509	PIV
Cryptography		
Assymmetric Key		
Key Generation	RSA-1024, 2048	RSA-1024, 2048 ECC P256
Digital Signature	RSA-1024, 2048	RSA-1024, 2048 ECC P256
Key Exchange	RSA-1024, 2048	RSA-1024, 2048 ECC P256
Diffie-Hellman	No	ECDH
Symmetric Keys		
	AES 128, 192, 256, 3DES	AES 128, 192, 256, 3DES (for challenge-response authentication)
Hash Digest		
	SHA-1, 256, 384, 512 MD2, MD4, MD5	Available but not utilized by PIV
Capabilities		
Smartcard		
Fingerprint, IRIS scan digitally signed	No	Yes
Facial image digitally signed	No	Yes
Anonymous but authentic card authentication	No	Yes
Authentication, sign and encryption for user	Yes	Yes
Additional containers of data (e.g., drivers license data)	Yes (requires P11 driver)	Yes
Data privacy protected by PIN	Yes	Yes
Only release information to authenticated reader	No	Optional
FIPS 201 certification	Not applicable	In progress
Driver		
A small mini-driver utilized for logical access	Yes (Downloads automatically from Microsoft site)	Yes (Included in Microsoft Windows 7, Apple OS 10.5, RIM)
Certificate Renewal		
Certificate Issuance & Renewal	Entrust Security Provider, Administration Services, Entrust IdentityGuard, Microsoft Client	Entrust IdentityGuard
Physical Access		
Modern Physical Access	Yes (Requires Desfire EV1 application)	Yes (Included in PIV application)

< Let's Talk

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 the company's ability to administer.
Dual smartcards interoperable with both contact (ISO 7816) and contactless (ISO 14443) interfaces	Make the investment once, then evolve where the card is utilized over time. The contact interface works with low-cost desktop readers. Select the contactless interface for fast, secure facility access.
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 replacement of physical access system. Avoid additional cost of two management systems.
Certificates seamlessly issued by Entrust IdentityGuard during smartcard issuance	Issue fully personalized cards with no need to involve the employee, citizen or consumer with complexities of certificate issuance or renewal. For customers interested in PIV or PIV-I, Entrust also issues certificates from the appropriate managed service CA.
Can be used with Entrust or Microsoft CA with very little user intervention	Customer no longer needs to perform expensive, time-consuming role of system integrator.

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** or via email at **entrust@entrust.com**.

About Entrust

A trusted provider of identity-based security solutions, Entrust empowers enterprises, governments, financial institutions, citizens and websites in more than 4,000 organizations spanning 60 countries. Entrust's customer-centric focus is the foundation to delivering organizations an unmatched level of security, trust and value. For strong authentication, credentialing, physical and logical access, mobile security, digital certificates, SSL and PKI, call 888-690-2424, email entrust@entrust.com or visit www.entrust.com. Let's talk.

Entrust[®] Securing Digital Identities & Information

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited in certain countries. All other company names, product names and logos are trademarks or registered trademarks of their respective owners. © Copyright 2011 Entrust. All rights reserved.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 4,000
Offices: 10 globally

Headquarters

One Lincoln Centre
5400 LBJ Freeway, Suite 1340
Dallas, Texas 75240 USA

Sales

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