Entrust Identity Enterprise Smart Card and USB Authentication

HIGHLIGHTS

Entrust Identity Enterprise smart card and USB-based devices allow organizations to leverage strong certificate-based authentication of user identities before granting logical access to networks or physical access to facilities, all from a single authenticator.

The latest chip technology saves minutes on card issuance and allows for authentication and sign operations on tablets to be well under a second, providing a quick tap-and-sign experience.

BENEFITS / RESULTS

- Enables security convergence for facilities, remote access, desktops and other applications
- Tailored for enterprise and government environments
- Smart card 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 Identity Enterprise platform

Entrust Identity Enterprise Smart Card and USB Authentication

Gain speed, longer lifetimes

- Industry-leading Entrust FIPS 201-compliant card
- Elliptic Curve Suite B-compliant
- Operates at up to two times the speed of competitors
- Long certificate lifetime and long-life card construction avoids re-issuance costs

Elite counter measures

- Best-in-class counter measures fight differential power analysis, simple power analysis, fault injection, and future laser-light attacks through partnerships with leading chip vendors
- Help thwart attacks that would otherwise steal identities and private information

Up to standards

- Our smart cards are fully compliant to FIPS 201 directive for PIV, PIV-I, and PIV-C requirements
- FIPS 140 and FIPS 201 certifications provide assurance to cardholder that the card is secure, resistant to attacks, and will interoperate with any other FIPS 201-compliant product

,

Entrust Identity Enterprise Smart Card and USB Authentication

TECHNICAL SPECIFICATIONS

Below is an outline of the various technical specifications for both smart card- and USB-based devices. This information demonstrates cryptographic performance, PIV compliance, advanced capabilities, and more.

FORM FACTORS		BEST OPTIONS
Smart cards	SC200 series smart cards	SC300 series smart cards
USB	USB200 series USB tokens	USB300 series USB tokens
Physical Access Options		
MIFARE option	No	No
Low frequency 125 kHz proximity option	Orderable option	Orderable option
PIV Compliance		
PIV-C (CIV)	Yes	Yes
PIV, PIV-I	Yes - historical	No – chip + applet combination not FIPS 140-2 certified
EEPROM Memory		
Capacity	Suitable for PIV and non-PIV applications	Suitable for PIV applications
Read cycles	Unlimited	
Write/erase cycles	500,000	
Data retention time	25 years	
Hardware System		
Co-Processors	DES, AES, RSA, ECC	
Compatible Connectivity (Low Frequency Versions are –L)		
Contact (ISO 7816)	SC200C	SC300D
Contactless (ISO 14443)	Not available	SC300D-L
Dual interface	Not available	SC300D
Certification and Approvals		
FIPS 140-2 level 2	Certification expired	Chip only
Common criteria	EAL5+ (chip & OS)	
Customization		
Card customized with organization logo	Available on request	

Entrust Identity Enterprise Smart Card and USB Authentication

APPLICATION OPTIONS

APPLICATION	NON-PIV	PIV
Cryptography		
Asymmetric Key		
Key generation	RSA-1024, 2048	RSA-1024, 2048 ECC P256, ECC P384 (SC250 only)
Digital signature	RSA-1024, 2048	RSA-1024, 2048 ECC P256, ECC P384 (SC250 only)
Key exchange	RSA-1024, 2048	RSA-1024, 2048 ECC P256, ECC P384 (SC250 only)
Diffie-Hellman	No	ECDH
Application	Non-PIV	PIV
Symmetric Keys		
	AES 128, 192, 256, 3DES	AES 128, 192, 256, 3DES
Hash Digest		
	SHA-1, 256, 384, 512 MD2, MD5	SHA-1, 256, 384, 512 MD2, MD5
Smart Card Capabilities		
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., driver's license data)	No	Yes
Data privacy protected by PIN	Yes	Yes
FIPS 201 application	No	Yes
Driver		
A small mini-driver utilized for logical access	Yes (Downloads automatically from Microsoft site)	Yes (Included in Microsoft Windows 7 and later, Apple OS 10.5+, BlackBerry)
Certificate Renewal		
Certificate issuance and renewal	Entrust Entelligence Security Provider, administration services, Microsoft client	Entrust Identity Enterprise
Physical Access		
Modern physical access	No	Yes (included in PIV application)

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact