Entrust®

+1-888-690-2424
entrust@entrust.com
entrust.com

@Entrust
+entrust
/EntrustVideo
/EntrustSecurity

DOWNLOAD
THIS DATA SHEET

Entrust Smartcard & USB Authentication

Technical Specifications

Entrust IdentityGuard smartcard- 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.

Using the latest chip technology translates to saving 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.

Gain Speed, Longer Lifetimes

The industry-leading Entrust FIPS 201-compliant card provides Elliptic Curve Suite B compliance, operating at up to two times the speed of competitors. This provides the cardholder with a long certificate lifetime and long-life card construction, avoiding costly card re-issuance.

Elite Counter Measures

By partnering with leading chip vendors, Entrust smartcards have best-in-class counter measures to fight Differential Power Analysis, Simple Power Analysis, Fault Injection and future laser-light attacks. If successful, these attacks could steal identities and private information.

Up to Standards

Entrust smartcards are fully compliant to FIPS 201 directive for PIV, PIV-I and PIV-C requirements. In addition, FIPS 140 and FIPS 201 certifications provide assurance to the cardholder that the card is secure, resistant to attacks and will interoperate with any other FIPS201-compliant product.

Know the Specs

The following pages outline the various technical specifications for both smartcard- and USB-based devices. This information demonstrates cryptographic performance, PIV compliance, advanced capabilities and more.

Solution Benefits

- 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 platform

Windows 8 Compatible
Compatible with Windows 7
CERTIFIED FOR Windows Vista
Designed for Microsoft® Windows® XP

Smartcards		
Model	**SC100 Series Smartcards**	**SC200 Series Smartcards**
Cryptographic Performance Entrust real-world benchmarks include the full round-trip from computer to card and back.		
RSA-1024, 2048		
Key Generation	< 5 seconds < 50 seconds	< 4 seconds < 45 seconds
Digital Signatures	0.47 seconds 1.02 seconds	0.171 seconds 0.623 seconds
Decryption	0.37 seconds 1.13 seconds	0.13 seconds 0.601 seconds
Elliptic Curve Cryptography (ECC)		
Digital Signature/Verification	192-bit sign — 0.32 seconds 192-bit verify — 0.60 seconds	192-bit sign — 0.101 seconds 192-bit verify — 0.82 seconds
AES 256		
Decryption	0.25 seconds	0.29 seconds
Triple DES		
Decryption	0.40 seconds	0.23 seconds
Physical Access Options		
Mifare Option	1k, 4k	Orderable Option
125 kHz Proximity Option	Yes	Yes
PIV Compliance		
PIV-C (CIV)	N/A	Yes
PIV, PIV-I	N/A	Yes (on GSA APL)
EEPROM Memory		
Capacity	80 Kb	144 Kb
Read Cycles	Unlimited	
Write/Erase Cycles	500,000	
Data Retention Time	25 Years	
Hardware System		
Co-Processors	DES, AES, RSA, ECC	

Smartcards		
Model	**SC100 Series Smartcards**	**SC200 Series Smartcards**
Connectivity		
Contact (ISO 7816)	SC100C	SC200C
Contactless (ISO 14443)	SC100CL	SC200CL
Dual Interface	SC100D	SC200D
Certification & Approvals		
FIPS 140-2 Level 2	Chip only; requires 200 series for full-device certification	
Common Criteria	EAL5+ (Chip & OS)	
EMVCo	Yes (Chip & OS)	
RoHS	Yes	Yes
China RoHS	Yes	Yes
Customization		
Card Customized with Organization Logo	Available on request	

Application Options		
Application	**Non-PIV**	**PIV**
Cryptography		
Asymmetric 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

Application Options		
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
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
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 8, Apple OS 10.5+, BlackBerry)
Certificate Renewal		
Certificate Issuance & Renewal	Entrust Entelligence Security Provider, Administration services, Microsoft client	Entrust IdentityGuard
Physical Access		
Modern Physical Access	No (Requires Desfire application)	Yes (Included in PIV application)

USB Tokens		
Model	**USB100 Series/USB Tokens**	**USB200 Series/USB Tokens**
Cryptographic Performance Entrust real-world benchmarks include the full round-trip from computer to card and back.		
RSA-1024, 2048		
Key Generation	< 5 seconds < 50 seconds	< 4 seconds < 45 seconds
Digital Signatures	0.47 seconds 1.02 seconds	0.171 seconds 0.623 seconds
Decryption	0.37 seconds 1.13 seconds	0.13 seconds 0.601 seconds
Elliptic Curve Cryptography (ECC)		
Digital Signature/ Verification	192-bit sign — 0.32 seconds 192-bit verify — 0.60 seconds	192-bit sign — 0.101 seconds 192-bit verify — 0.82 seconds
AES 256		
Decryption	0.25 seconds	0.29 seconds
Triple DES		
Decryption	0.40 seconds	0.23 seconds
PIV Compliance		
PIV-C (CIV)	N/A	Yes
PIV, PIV-I	N/A	Yes (on GSA APL)
EEPROM Memory		
Capacity	80Kb	144Kb
Read Cycles	Unlimited	
Write/Erase Cycles	500,000	
Data Retention Time	25 Years	
Hardware System		
Co-processors	DES, AES, RSA, ECC	
Connectivity		
USB 1.1/2.0	N/A	Yes

USB Tokens		
Model	**USB100 Series/USB Tokens**	**USB200 Series/USB Tokens**
Certification & Approvals		
FIPS 140-2 Level 2	Chip only; requires 200 series for full-device certification	
Common Criteria	EAL5+ (Chip & OS)	
EMVCo	Yes (Chip & OS)	
RoHS	Yes	Yes
China RoHS	Yes	Yes
Customization		
Card Customized with Organization Logo	Available on request	

Application Options		
Application	**Non-PIV**	**PIV**
Cryptography		
Asymmetric 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	
Symmetric Keys		
	AES 128, 192, 256, 3DES	Available but not utilized by PIV
Hash Digest		
	SHA-1, 256, 384, 512 MD2, MD3, MD5	Available but not utilized by PIV

Application Options		
Application	**Non-PIV**	**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
Data privacy protected by PIN	Yes	Yes
Only release information to authenticated reader	No	Optional
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 8, Apple OS 10.5+, BlackBerry)
Certificate Renewal		
Certificate Issuance & Renewal	Entrust Entelligence Security Provider, Administration services, Microsoft client	Entrust IdentityGuard
Physical Access		
Modern Physical Access	No (Requires Desfire application)	Yes (Included in PIV application)

Entrust offers software authentication platforms that strengthen security in a wide range of identity and transaction ecosystems. Government agencies, financial institutions and other enterprises rely on Entrust solutions to strengthen trust and reduce complexity for consumers, citizens and employees.

Now, as part of Datacard Group, Entrust offers an expanded portfolio of solutions across more than 150 countries. Together, Datacard Group and Entrust issue more than 10 million secure identities every day, manage billions of secure transactions annually and issue a majority of the world's financial cards. For more information about Entrust solutions, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Company Facts
Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 globally

Headquarters
Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, TX 75240 USA

Entrust®

24274/8-14