Entrust[®] Securing Digital Identities & Information

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.

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.

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.

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.

The 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 FIPS-201-compliant product.



SECURITY

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	< 3 seconds < 65 seconds	< 7 seconds < 50 seconds	
Digital Signatures	0.126 seconds 0.47 seconds	0.15 seconds 0.619 seconds	
Decryption	0.116 seconds 0.476 seconds	0.142 seconds 0.63 seconds	
Elliptic Curve Cryptography (ECC)			
Digital Signature/ Verification	P256 sign — 0.117 seconds P256 verify — 0.133 seconds (FIPS 201 Only)	P256 sign — 0.119 seconds P256 verify — 0.138 seconds (FIPS 201 Only)	
AES 256			
Decryption	0.025 seconds	0.027 seconds	

Smartcards		
Model	SC100 Series Smartcards	SC200 Series Smartcards
Triple DES		
Decryption	0.024 seconds	0.020 seconds
Physical Access Options		
Mifare Classic	Available on Request	Available on Request
Mifare Desfire	No	Available on Request
125 kHz Proximity Option	Available on Request	Available on Request
PIV Compliance		
PIV-C (CIV)	Yes	Yes
PIV, PIV-I	No	Yes
EEPROM Memory		
Capacity	80 Kb	80 Kb
Read Cycles	Unlimited	Unlimited
Write/Erase Cycles	500,000	500,000
Data Retention Time	25 Years	25 Years
Hardware System		
Co-Processors	DES, AES, RSA, ECC	DES, AES, RSA, ECC
Connectivity		
Contact (ISO 7816)	SC100C	SC200C
Contactless (ISO 14443)	SC100CL	SC200CL
Dual Interface	SC100D	SC200D
Certification & Approvals		
FIPS 140-2 Level 2	Chip Only	Full-Device Certification
Common Criteria	EAL5+ (Chip & OS)	EAL5+ (Chip & OS)
EMVCo	Yes (Chip & OS)	Yes (Chip & OS)
RoHS	Yes	Yes
China RoHS	Yes	Yes
NIST NPIVP (FIPS 201 Compliant)	No	Yes (SC200D)
Customization		
Card Printed with Organization Logo	Available on Request	Available on Request



Smartcards		
Model	SC100 Series Smartcards	SC200 Series Smartcards
Cryptography		
Asymmetric Key		
Key Generation	RSA-1024, 2048 ECC P256 (when used with the FIPS-201 application)	RSA-1024, 2048 ECC P256 (when used with the FIPS-201 application)
Digital Signature	RSA-1024, 2048 ECC P256 (when used with the FIPS-201 application)	RSA-1024, 2048 ECC P256 (when used with the FIPS-201 application)
Key Exchange	RSA-1024, 2048 ECC P256 (when used with the FIPS-201 application)	RSA-1024, 2048 ECC P256 (when used with the FIPS-201 application)
Diffie-Hellman	No	ECDH (when used with the FIPS-201 application)
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





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	< 3 seconds < 65 seconds	< 7 seconds < 50 seconds		
Digital Signatures	0.126 seconds 0.47 seconds	0.15 seconds 0.619 seconds		
Decryption	0.116 seconds 0.476 seconds	0.142 seconds 0.63 seconds		
Elliptic Curve Cryptography (ECC)				
Digital Signature/Verification	P256 sign — 0.117 seconds P256 verify — 0.133 seconds (FIPS 201 Only)	P256 sign — 0.119 seconds P256 verify — 0.138 seconds (FIPS 201 Only)		
AES 256				
Decryption	0.025 seconds	0.027 seconds		
Triple DES				
Decryption	0.024 seconds	0.020 seconds		
PIV Compliance				
PIV-C (CIV)	Yes	Yes		
PIV, PIV-I	No	No		
EEPROM Memory				
Capacity	80Kb	80Kb		
Read Cycles	Unlimited	Unlimited		
Write/Erase Cycles	500,000	500,000		
Data Retention Time	25 Years	25 Years		
Hardware System				
Co-Processors	DES, AES, RSA, ECC	DES, AES, RSA, ECC		



USB Tokens		
Model	USB100 Series USB Tokens	USB200 Series USB Tokens
Connectivity		
USB 1.1/2.0	Yes	Yes
Certification & Approvals		
FIPS 140-2 Level 2	Chip Only	Full-Device Certification
Common Criteria	EAL5+ (Chip & OS)	EAL5+ (Chip & OS)
EMVCo	Yes (Chip & OS)	Yes (Chip & OS)
RoHS	Yes	Yes
China RoHS	Yes	Yes
Customization		
USB Customized with Organization Logo	Available on Request	Available on Request
Cryptography		
Asymmetric Key		
Key Generation	RSA-1024, 2048 ECC P256 (when used with the FIPS-201 application)	RSA-1024, 2048 ECC P256 (when used with the FIPS-201 application)
Digital Signature	RSA-1024, 2048 ECC P256 (when used with the FIPS-201 application)	RSA-1024, 2048 ECC P256 (when used with the FIPS-201 application)
Key Exchange	RSA-1024, 2048 ECC P256 (when used with the FIPS-201 application)	RSA-1024, 2048 ECC P256 (when used with the FIPS-201 application)
Diffie-Hellman	No	ECDH (when used with the FIPS-201 application)
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





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 elD 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**.

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 or trademarks of their respective owners. © 2012 Entrust. All rights reserved.