

Features

- RSA sign/decrypt – key lengths from 512-2048 bits
- DSA sign/Verify – key lengths 512 & 1024 bits
 - DES/3DES encryption
 - On-card key generation
 - SHA-1 Digest functions
 - Multiple keys and certs (up to EEPROM limits)
- **Validated for:**
 - FIPS 140-2 Level 3
 - FIPS 201
 - Common Criteria EAL4+
 - PKCS #11 and MS-CAPI interface requirements
 - Diffie-Hellman key exchange
 - AES 128, 192, 256 encryption
- Convenient ISO-compliant (7816) smart card format
 - Cryptographic co-processor for improved performance and speed
- On-board DES HW co-processor for secret-key encryption
 - On-board AES co-processor
- Hardware and software protection against differential power and timing attacks
 - FIPS-validated Biometric Match-On-Card capabilities
 - User PIN unblocking
 - 64k EEPROM for secure storage of keys, passwords, certificates, application programs, and data.
 - Card unblocking
 - Secure messaging
- GSC-IS interoperability specifications
 - Identrus specifications

SafeNet Borderless Security 400 SMART CARD

Proven technology – Trusted authentication

SafeNet, the authority on strong authentication, now offers the 400 Smart Card – featuring the most powerful encryption technology available today!

SafeNet Borderless Security 400 Smart Card

SafeNet's industry-leading 400 Smart Card offers some of the most powerful cryptographic token technology available today. Validated for FIPS 201 and FIPS 140-2, with Level 3-validated security, and PIV-2 compliant, the 400 Smart Card is supported by hundreds of applications and contains optional match-on-card biometric authentication support for three-factor authentication.

The power behind SafeNet's cutting-edge smart cards is found in its smart card operating system, SCCOS (SafeNet Cryptographic Card Operating System), and embedded microcontroller, with available 64K EEPROM storage. The embedded microcontroller makes cryptography convenient to use and surprisingly fast. While the sophisticated token operating system resides in ROM, its capacity can be extended using non-volatile EEPROM memory to securely store passwords, private keys, public certificates, and other data as required.

Digitally signed executable programs extend the feature set of the operating system, providing card versions that support application specific requirements, such as those for FIPS-validated three-factor Match-on-Card biometrics, card unblocking, and Personal Identity Verification (PIV). It also has the flexibility to integrate with hundreds of applications and products from leading vendors, and provides for future cryptographic functions and data management.

Security

User Authentication

SafeNet smart cards require users to authenticate themselves before initiating



any security functions. Authentication is accomplished via password in accordance with the ISO 7816-4 smart card standard. SafeNet smart cards ensure that only authorized users can perform the cryptographic functions.

Token/Host Authentication

SafeNet smart cards provide confidence in online communications. They feature on-chip public key functions that support emerging public key challenge-response protocols, such as FIPS PUB 196.

RSA/DSA Key Generation

The integrity of public/private key pairs is fundamental to the success of any crypto system. Keys that are stored on a computer, and protected only by software, are vulnerable to hacking techniques and illicit "key-stealing" that can go undetected. Since SafeNet smart cards perform all sensitive cryptographic functions directly on the card, unauthorized users have no way of accessing a user's digital credentials without stealing the smart card and guessing the pass phrase.

RSA/DSS Digital Signature

On-chip cryptographic functions allow users to produce either RSA (PKCS #1) or DSS (FIPS 186) digital signatures with confidence in the long-term secrecy of their private keys. Only smart cards can provide this lasting confidence in digital

signature key sets.

RSA and Diffie-Hellman Key Exchange

No system is complete without support for the exchange of session encryption keys. SafeNet smart cards include both RSA key unwrapping and Diffie-Hellman key agreement and key exchange functions. The private keys used for these exchange functions are never exposed to a vulnerable host system.

Storage

All of the cryptographic functions, operational parameters, and general-purpose storage remain secure behind a "silicon firewall." This allows full customization of the smart cards to meet the requirements of specific applications. Implementation of customized security features and general purpose data storage is in accordance with the ISO 7816-4 standard.

Configurability

SafeNet smart cards provide a token configuration file that enterprise security officers can use to permanently enable or disable cryptographic functions and to configure the tokens to match the security policy of the enterprise. For additional security, the contactless interface may be enabled or disabled.

Standards

- ISO 7816-2 for dimensions and location of the contact (for smart card).
- ISO 7816-3 for electronic signals and transmission protocol type T=1.
- ISO 7816-4 for inter-industry commands of interchange security standards.
- ISO 14443 Type A contactless interface for physical access.
- FIPS PUB 186: Digital Signature Standard.
- FIPS PUB 196: Authentication using Public Key Cryptography.
- PKCS #1: RSA Encryption Standard
- PKCS #3: Diffie-Hellman.
- PKCS #11: Cryptographic Token API Standard (CRYPTOKI).

- Microsoft Crypto API.

SafeNet smart cards are easily integrated through the SafeNet Borderless Security Single Sign-On and SafeNet Borderless Security PK Client Middleware software packages. These software packages provide a standard PKCS #11 API, as well as Microsoft's CryptoAPI interface. Applications such as Netscape Communicator, Entrust Client, and Microsoft Internet Explorer automatically make use of SafeNet smart cards when they are used with SSO or PK software.

Technical Specifications

Electrical

- Power: 10 mA maximum
- Supply voltage range: 1.62-5.5 V
- Sleep mode: 200 uA max.
- ESD protection: > 4 kv.

EEPROM Memory

- Capacity: 64K
- Read cycles: Unlimited
- Write/erase cycles: 500,000
- Data retention time: 20 years minimum

Environmental

- Storage Temp: -40°C to 125°C
- Operating Temp: -25°C to 70°C

Workstation Interface Smart

- Card Readers
 - Serial reader
 - USB reader
 - PCMCIA reader
- SafeNet PK Client Middleware also supports the PC/SC standard, allowing SafeNet smart cards to be used with PC/SC compliant readers

NORDIC DISTRIBUTOR

PERICO AS

Lilleakerveien 4, Inngang 1A
0283 OSLO, NORWAY

Email: info@perico.no

Tel: +47 22 06 40 50

