Model 330 Smart ID Cryptographic Smart Card

SafeNet smart cards — Locking the virtual door to unsecured online information and communications

In addition to a robust and extensible cryptographic operating system, SafeNet smart cards offer the most advanced security available today in a smart token, including:

- Variable RSA key length from 512 bits to 2048 bits.
- Variable DSA key length from 512 bits to 1024 bits.
- Diffie-Hellman key agreement with primes from 512 bits to 2048 bits and exponents from 128 bits to 256 bits.
- On-token key generation for all of the above algorithms and key lengths.
- SHA-1 cryptographic functions
- GSA interoperability specifications

Model 300 Smart Card

SafeNet's industry-leading smart card offers the some of the most powerful cryptographic PKI token technology available today. SafeNet smart card-based information security products continue to support industry standards such as PKCS #11 and Microsoft CryptoAPI, allowing for seamless integration with applications and products from leading PKI vendors.

The power behind SafeNet's cutting-edge PKI smart cards is found in its smart card operating system, DKCCOS (Datakey Cryptographic Card Operating System), and embedded microcontroller — which contains a modular arithmetic processor and 32K 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 nonvolatile 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 Identrus, Match-on-Card biometrics, card unblocking, and GSA. Plus, it has the flexibility to provide for future cryptographic functions and data management.

Security Services of SafeNet Smart Cards

User Authentication

SafeNet smart cards require users to authenticate themselves before initiating any security functions. Authentication is accomplished through the use of a 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 a number of hacking techniques and illicit "key-stealing" programs that can run undetected. Since SafeNet smart cards perform all sensitive cryptographic functions directly on the card — including public/private key generation, digital signature creation, and cryptographic session key unwrapping — 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 long-term 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.

Secure 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.

Technical Specifications

Electrical

Power: 10 mA maximum.
Supply voltage range: 5Vdc +/- 10%.
Sleep mode: 200 uA max.
ESD protection: > 4 kv.

EEPROM Memory

Capacity: 32K
Read cycles: Unlimited
Write/erase cycles: 100,000

Environmental

- Storage Temp: -40ºC to 125ºC
- Operating Temp: -25ºC to 70ºC

Workstation Interface — Smart Card Readers

Serial reader
USB reader
PCMCIA reader
SafeNet CIP also supports the PC/SC standard, allowing SafeNet smart cards to be used with PC/SC compliant readers

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.
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).

Features

Convenient ISO-compliant (7816) smart card format.

Cryptographic co-processor for improved performance and speed.

On-board DES hardware co-processor for secret-key encryption.

32K smart card operating system in ROM.

32K EEPROM for secure storage of keys, passwords, certificates, application programs and data.

Implements public key functions:

– RSA/DSA key generation.
– RSA for digital signature.
– DSA for digital signature.
– RSA key exchange.
– Diffie-Hellman key exchange.

Hardware and software protection against differential power attacks and timing attacks.

Validated for FIPS 140-2 Level 2.

GSC-IS V2.1 Compliance

Digitally signed executable programs provide card versions to support

– Identrus specifications.
– GSA multi-pin architecture.
– Biometric algorithms.
– Card unblocking

SafeNet smart cards are easily integrated through the SafeNet Axis and SafeNet CIP (Cryptographic Interface Provider) 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 Axis or CIP software.

Developer's Tool Kit —
SafeNet CIP Tools

To assist software engineers and designers in implementing smart card security within their specific PKI applications, SafeNet offers a Developer's Tool Kit. The Tool Kit — SafeNet CIP Tools — comes complete with the necessary components to "smart-token enable" business-critical information systems. Please contact a SafeNet representative for more information.

Supported Operating Systems

Windows 98, NT, 2000, XP, 2003

For More Information

SafeNet (SFNT:Nasdaq) is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property and digital identities, and offers a full spectrum of products including hardware, software, and chips. ARM, Bank of America, Cisco Systems, the Departments of Defense, and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit www.safenet-inc.com.

Corporate Headquarters:
4690 Millennium Drive, Belcamp, Maryland 21017 USA
Phone USA and Canada (800) 533-3958
Phone Other Countries (410) 931-7500
Fax (410) 931-7524
E-mail info@safenet-inc.com
Website www.safenet-inc.com

SafeNet
The Foundation of Information Security