

Features

Borderless Security

330 Smart Card Supports:

- RSA sign/decrypt - key lengths from 512 bits to 2048 bits
 - DES/3DES encrypt
- On-card key generation
- SHA-1 cryptographic functions
 - Multiple keys and certs (up to EEPROM limits)
- Validated to FIPS 140-2 Level 2
 - PKCS#11 and MS-CAPI interface requirements
- GSA interoperability specifications
 - User PIN unblocking

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 Borderless Security 330 SMART CARD

For Multiple Applications

Locking the virtual door to unsecured online information and communications

SafeNet Borderless Security 330 Smart Card

SafeNet's industry-leading smart card offers 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.

