THE
DATA
PROTECTION
COMPANY

SafeNet 330 Smart Card

For Multiple Applications

PRODUCT BRIEF

Benefits

High Capacity

- Multiple keys and certs (up to EEPROM limits)
- 32K EEPROM for secure storage of keys, passwords, certificates, application programs and data

Broad API Support

- PKCS#11, MSCAPI, Microsoft PC/SC, and Apple Native PC/SC

Improved Performance

- Cryptographic co-processor for improved performance and speed

Security

- Hardware and software protection against differential power attacks and timing attacks
- On-card key generation
- Validated for FIPS 140-2 Level 2

Increased Capabilities

- Digitally signed executable programs provide card versions to support
- IdenTrust compliant Key Storage Mechanism (KSM)
- Generates IdenTrust compliant digital signatures
- GSA multi-pin architecture
- Biometric algorithms
- Card unblocking

SafeNet's industry-leading smart card offers some of the most powerful cryptographic PKI token technology available today. SafeNet 330 Smart Card continues to support industry standards such as PKCS #11, Microsoft CryptoAPI, and Apple Native PC/SC 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 microcontrolle—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 crypto-graphic function and data management.

User Authentication

SafeNet 330 Smart Card requires 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 330 Smart Card provides 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 330 Smart Card performs 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.

Technical Specifications

System Requirements

Operating Systems Supported:

- Microsoft Windows 2000, 2003, XP, and Vista
- Apple Mac OS 10.4.6 (Tiger)

Cryptographic APIs

- PKCS #11 v2.01
- Microsoft CryptoAPI (CAPI) 2.0
- Microsoft PC/SC
- Apple Native PC/SC

Cryptographic Performance

- RSA encrypt/decrypt key lengths 512 to 2048 bit

Cryptographic Functions & Algorithms

Asymmetric Key

- RSA

Symmetric Key

- DES, 3DES

Digital Signing

- RSA, DSA

Hash Digest

- SHA-1

Key Exchange

- RSA
- Diffie-Hellman

On-card Key Generation

On-board DES hardware co-processory for secure key generation

EEPROM Memory

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

Electrical

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

Environmental

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

Workstation Interface Smart Card Readers

- Serial reader
- USB reader
- PCMCIA reader
- Any reader that includes Microsoft PC/SC standards compliant reader drives

FIPS 140-2 Level 2 certified

ISO 7816 compliant

GSC-IS v2.1

RSA and Diffie-Hellman Key Exchange

No system is complete without support for the exchange of session encryption keys. SafeNet 330 Smart Card includes 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 330 Smart Card provides 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.

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).
- Microsoft Crypto API.

Software Support

SafeNet 330 Smart Card is easily integrated using included robust client middleware and drivers or with the SafeNet Borderless Security Single Sign-On strong authenti-cation and single sign-on software product.

Applications such as Netscape Communi-cator, Entrust Client and Microsoft Internet Explorer automatically make use of SafeNet smart cards when they are used with supporting client middleware software.

The SafeNet Family of Authentication Solutions

SafeNet's suite of authentication solutions includes certificate-based, OTP, hybrid and software authenticators. All authenticators, together with SafeNet's extensive management platforms and security applications, empower you to:

Conduct business securely and efficiently• and open new market opportunities with innovative products that enable secure remote access and advanced security applications such as certificate-based authentication, digital signing and pre-boot authentication.

Reduce risk with strong authentication solutions that prevent fraud and data theft and enable compliance to industry regulations.

To learn more about SafeNet's complete portfolio of authentication solutions, please visit our website at www.SafeNet-inc.com

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected

©2012 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet.
All other product names are trademarks of their respective owners. PB (EN)-03.14.12