Benefits

Model 330J 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 specfications
- User PIN unblocking

Typical Applications

- Encrypting and digitally signing e-mail
- Authenticating identity for network log-on and for secure access to VPNs, extranets, intranets or private websites
- Securing Internet-based transactions
- Signing electronic forms

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.
- 96K smart card operating system in ROM.
- 32K EEPROM for secure storage of keys, passwords, certificates, application programs and data.

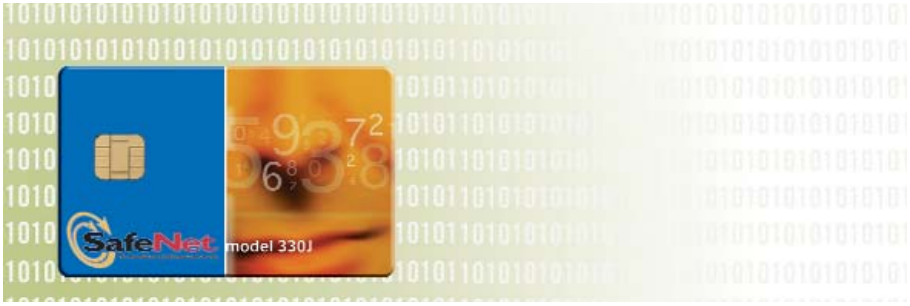
Implements public key functions:

- RSA key generation.
- RSA for digital signature.
- RSA key exchange

- Hardware and software protection against differential power attacks and timing attacks.
- JavaCard 2.1.1 and Global Platform V2.0.1 compliant

330 Java Card

For Multiple Applications



The Model 330J is SafeNet's multi-application Java smart card, designed to the JavaCard v2.1.1 and Global Platform v2.0.1 specifications. It provides increased security by incorporating built-in, ROM-based cryptographic and data container storage functions.

SafeNet Model 330J Java Card

The Model 330J is SafeNet's multi-application Java smart card, designed to the JavaCard v2.1.1 and Global Platform v2.0.1 specifications. It provides increased security by incorporating built-in, ROM-based cryptographic and data container storage functions. The built-in capabilities enable a more efficient use of the card's 32K EEPROM memory where user-defined applications and data are stored. The Model 330J smart card features SafeNet's JCCOS operating system applet (Java Cryptographic Card Operating System).

In addition to supporting Global Platform v2.0.1 for applet loading and deletion, the card's architecture allows for simple management of digital credentials in the field by giving users the ability to modify the data-only contents of their own card (as defined by an organization's security policy).

SafeNet's Model 330J also meets GSA CAC native card-edge interface requirements. GSA's smart card interoperability standard ensures "any card, any software" operation. All current and future GSA applications will interoperate with any card adhering to the GSA specification. For agencies or U.S. government organizations within the GSA CAC program, this means the Model 330J smart card will seamlessly and directly plug-and-play with their applications.

Smart Card Security Services

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.

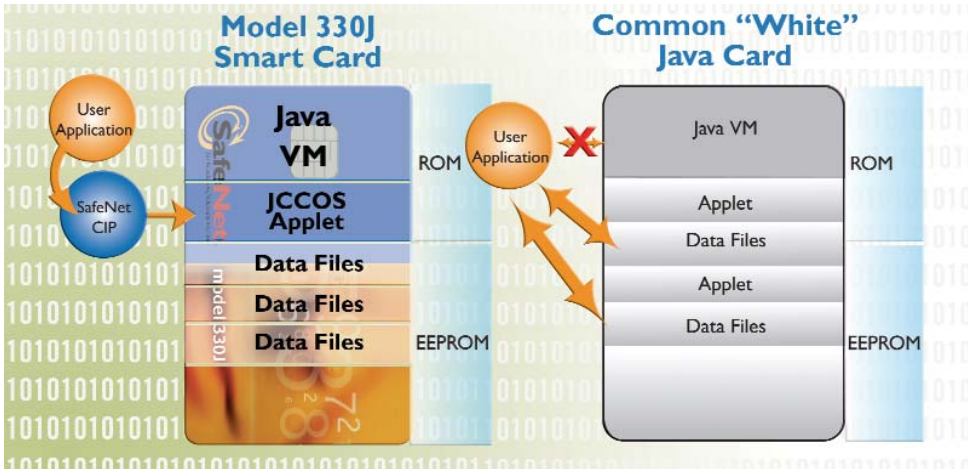
Token/Host Authentication

SafeNet smart cards allow for 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 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.

SafeNet®
The Foundation of Information Security



RSA Digital Signature

On-chip cryptographic functions allow users to produce RSA (PKCS #1) 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.

Model 330J Architecture

SafeNet designed the Model 330J to provide built-in cryptographic and data container management functions while giving enterprises the ability to add new applications in the future. So SafeNet created a high security, high performance cryptographic application that is embedded in ROM instead of EEPROM, providing many advantages from a security, use or memory, deployment and card management perspective, including:

- Efficient use of memory - Only the data objects created and used by the built-in cryptographic application are stored in EEPROM; no memory space is used as overhead for cryptographic applets
- User manageability of the contents of the smart card - Users can easily load and delete data objects on their smart card, without requiring a return to an issuing station or compromising the Open Platform security model.
- Reduced deployment time - The Java JCCOS application resides in ROM, not EEPROM. This saves time during the personalization process because the application already resides on the smart card.
- Compatibility with current SafeNet CIP and Axis software - Leverages proven interoperability with a broad range of information security and e-business applications.

Software Support

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 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.

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

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.
- PKCS #1: RSA Encryption Standard.
- PKCS #3: Diffie-Hellman.
- PKCS #11: Cryptographic Token API Standard (CRYPTOKI).

Supported Operating Systems

- Windows 98, NT, 2000, XP, 2003

Corporate: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: **+1 410.931.7500** or 800.533.3958 **email: info@safenet-inc.com**

www.safenet-inc.com

Australia +61 3 9882 8322
Brazil +55 11 3392 4600
Canada +1 613.723.5077
China +86 10 8266 3936
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852.3157.7111
India +91 11 26917538
Japan(Tokyo) +81 3 5719 2731
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore (2) +65 6297 6196
Taiwan +886 2 27353736
UK +44 1276 608 000
U.S. (Massachusetts)
+1 978.539.4800
U.S. (New Jersey)
+1 201.333.3400
U.S. (Virginia) +1 703.279.4500
U.S. (Irvine, California)
+1 949.450.7300
U.S. (Santa Clara, California)
+1 408.855.6000
U.S. (Torrance, California)
+1 310.533.8100
U.S. (Minneapolis, Minnesota)
+1 888.238.2539

Distributors and resellers located worldwide.

SafeNet®
The Foundation of Information Security