

## Datakey's Model 330J smart card

The Model 330J is Datakey's multi-application 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 Datakey's JCCOS operating system application (Java-based 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).

Datakey'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.

### The Model 330J 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)
- Designed to meet FIPS 140-2 Level 2 requirements
- PKCS #11 and MS-CAPI interface requirements.
- GSA interoperability specifications
- PIN unblocking

## Security Services of Datakey Smart Cards

### User Authentication

Datakey 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. Datakey smart cards ensure that only authorized users can perform the cryptographic functions.

### Token/Host Authentication

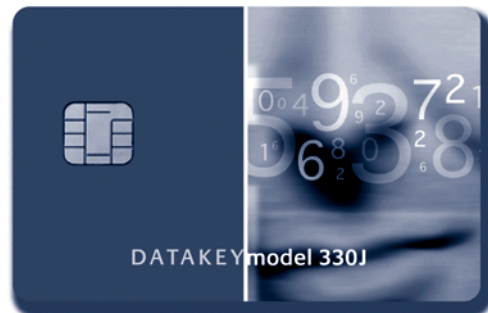
Datakey smart cards allow for confidence in online communications. They feature on-chip public key functions that support emerging public key challenge-response protocols such as FIPS PUB 194.

### 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 Datakey 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 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.



### RSA Key Exchange

No system is complete without support for the exchange of session encryption keys. Datakey smart cards include RSA key unwrapping 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

Datakey 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.

## Typical Applications

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

## Model 330J Architecture

Datakey 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 Datakey 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.

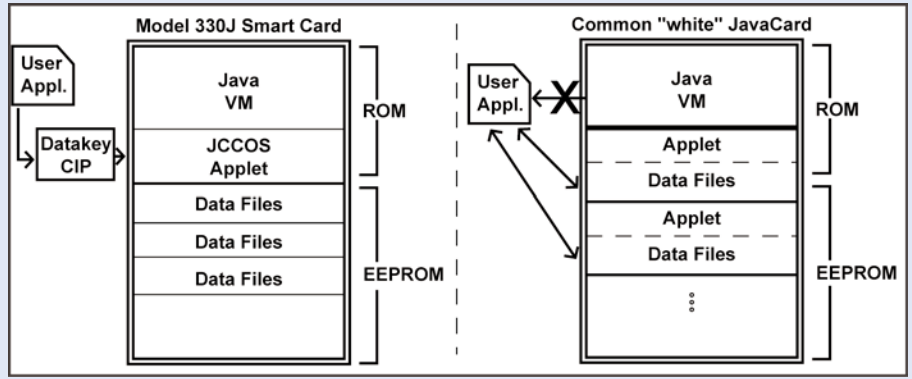


Figure 1: Comparisons of smart card architectures

- Reduced deployment time - The Java 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 Datakey CIP software - Leverages proven interoperability with a broad range of information security and e-business applications.

## 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.
- Compliant to FIPS 140-2 Level 2.

## 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
- Datakey CIP also supports the PC/SC standard, allowing Datakey smart cards to be used with PC/SC compliant readers

## Standards

### ISO 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 #11: Cryptographic Token API Standard (CRYPTOKI).

## Software Support

Datakey smart cards are easily integrated through the Datakey CIP (Cryptographic Interface Provider) software package. This software package provides 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 Datakey smart cards when they are used with CIP software.

## Developer's Tool Kit — Datakey CIP Tools

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

## Supported Operating Systems

Windows 95, 98, NT, 2000, XP.

## Corporate Headquarters

407 West Travelers Trail  
 Minneapolis, MN 55337  
**Phone:** (952) 890-6850  
**Toll-free in United States:** 1-888-328-2539  
**Fax:** (952) 890-2726  
**Web:** www.datakey.com  
**E-mail:** info@datakey.com

## European Offices

### Germany

Am Kronberger Hang 2, D-65824  
 Schwalbach/Ts., Frankfurt, Germany  
**Phone:** +49-(0)-6196-950 40 0  
**Fax:** +49-(0)-6196-950 40 28

### United Kingdom

Cleeve Court, Cleeve Road  
 Leatherhead, Surrey, KT22 7UD  
 United Kingdom  
**Phone:** +44 (0) 1372 371470  
**Fax:** +44 (0) 1372 378087

