

Datakey's Cryptographic Smart Card

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

Datakey's industry-leading smart card offers the most powerful cryptographic PKI token technology available today. Datakey 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 Datakey'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 non-volatile 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 for future cryptographic functions and data management.

In addition to a robust and extensible cryptographic operating system, Datakey 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.

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/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 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/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. Datakey 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

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 330 Card Performance

Performance

Operation	RSA Key Pair Generation ¹	DSA Key Pair Generation Exponent=160 bits	RSA Digital Signature ² RSA Decrypt	DSA Digital Signature ²	Diffie-Hellman Key Agreement Exponent = 128 bits	Diffie-Hellman Key Agreement Exponent=160 bits	Diffie-Hellman Key Agreement Exponent = 200 bits	DES Key Generation	DES Encryption
Key Length	512 bits	512 bits	512 bits	p=512 bits	p=512 bits	p=512 bits	p=2048 bits	8 or 16 bytes	8 bytes, single DES ECB
	1024 bits	1024 bits	1024 bits	p=1024 bits	p=768 bits	p=768 bits			8 bytes, single DES CBC
	1536 bits		1536 bits			p=1024 bits			16 bytes, triple DES ECB
	2048 bits		2048 bits			p=1536 bits			16 bytes, triple DES CBC
Time in Serial Port	13 seconds	2.0 seconds	.53 seconds	1.0 seconds	1.2 seconds	1.3 seconds	2.6 seconds	.24 seconds	.14 seconds
	23 seconds	2.5 seconds	.77 seconds	1.2 seconds	1.4 seconds	1.4 seconds			1.1 seconds
	76 seconds		1.2 seconds			1.6 seconds			.14 seconds
	180 seconds		2.0 seconds			2.0 seconds			1.1 seconds

Note 1: This process includes the non-deterministic process of finding prime numbers, which can take longer than this average time.

Note 2: These times are exclusive of hashing times, which become significant with files of 250 Kbytes.

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.
 - ECDSA for digital signature.*
 - ECC key generation.*
- Hardware and software protection against differential power attacks and timing attacks.
- Validated for FIPS 140-1 Level 2.

*optional capability

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 100°C
- Operating Temp: -25°C to 85°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.
- FIPS PUB 186: Digital Signature Standard.
- PKCS #1: RSA Encryption Standard.
- PKCS #3: Diffie-Hellman.
- 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 PKI 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.

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 Office

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

