SignaSURE™ Security Policy

SignaSURE 330 Model Smartcard

A Description of Datakey's Information Security Products and Solutions, their Functions and Capabilities

April 19, 2000

Datakey, Inc.
407 West Travelers Trail
Burnsville, MN 55337

Table of Contents

SignaSURE™ Security Policy

Abstract

The Model 330 SignaSURE Smart Card is compliant with parts 1 through 4 of the ISO 7816 standard and contains an eight-bit microcontroller, a math accelerator for public key cryptographic functions, a hardware accelerator for Triple DES symmetric encryption, a ROM for containing the token operating system, a RAM for I / O registers, and a programmable memory. The Model 330 is targeted for compliance with FIPS (Federal Information Processing Standard) 140-1 Security Level 2.

PIN or pass Phrase authentication provides role based access control, protection the cryptographic functions of the module, functions like public key pair generation (RSA and DSS), digital signature generation (RSA and DSS), unwrapping of session encryption keys, user authentication, symmetric encryption/decryption (DES and TDES) and on-line authentication (mutual challenge / response).

The Datakey Crypto Card Operating System (DKCCOS) v2.0 is the proprietary operating system used with the Model 330 smart card. Although this operating system is unchangeably embedded in the ROM of the processor chip, it does incorporate a feature in the form of downloadable / executable files (EXFs) that allows for the augmentation and extension of the operating system. Currently there are no FIPS-validated EXFs that are available, but such EXFs are planned for future use.

1.0 The Business Information Environment Today

Today, organizations understand that information has become a critical asset. Whether it’s details of financial transactions, market development plans, new product specifications, or E-mail and other daily communications, information and its secure, efficient movement and use are critical to an organization’s success.

But even as secure, accurate and confidential assets assume greater importance, the list of security threats increases. From hackers to viruses, disgruntled employees to criminal activity, information assets may come under attack from without and within.

The adversarial activity is of greater concern because there is so much more information on the networks to target today than a few years ago. The explosive growth of communications and data processing technology presents a major challenges to data security. Advances in local and wide-area networking and infrastructure as well as innovations such as E-mail, distributed server technology and open architectures have revolutionized computing. But they have also created security problems that were unimaginable when independent systems were the dominant computing paradigm.

2.0 Datakey, Inc.'s SignaSURE™ Information Security Products and Solutions

To ensure that users of open networks can achieve the level of security necessary to transact sensitive business without the use of dedicated, private lines, Datakey has designed the SignaSURE™ family of token-based information security products and solutions.

A basic principle embodied in this family of solutions is that the most sensitive security operations shall be performed within a hardware security module under authenticated access by the operator, while non-sensitive, or less sensitive, operations may be performed within a software security module.

Members of the SignaSURE™ family include the following:

- **Secure Hardware Tokens**

  Tokens are provided in two formats, ISO 7816-compliant smart cards and functionally-equivalent, environmentally rugged smart keys.

  For the purposes of this policy, all reference shall be interpreted as the Model 330 SignaSURE Smart Card and the Model 380 SignaSURE Smart Key.

  The smart cards are compliant with parts 1 through 4 of the ISO 7816 standard, which define the physical characteristics, contact arrangement / location, electrical characteristics, interface protocol, file structure and command set.

  The smart keys are built in the form of a plastic door key with contacts in the slots of the key. The electrical characteristics, interface protocol, file structure and command set are identical to those of the smart card.

  The chip used in both types of tokens has an eight-bit microcontroller, a math accelerator for public key cryptographic functions, a hardware accelerator for Triple DES symmetric encryption, a ROM for containing the token operating system, a RAM for I / O registers, and a programmable memory.

  The token end-user is authorized to perform sensitive functions in the token via PIN or pass Phrase authentication. These functions include digital signature generation and unwrapping of session encryption keys, i.e., those functions that require the use of the closely guarded private key of the user's public key pair. The enterprise Security Officer (SO) may also authenticate himself / herself to the token with a separate PIN or pass phrase in order to perform sensitive operations such as the initial entry of the end-user's PIN, pass phrase or encryption keys.

The tokens are capable of performing a variety of cryptographic functions, including public key pair generation (RSA and DSS), digital signature generation (RSA and DSS), unwrapping of session encryption keys, user authentication, and on-line authentication (mutual challenge / response).

Although the token includes a hardware accelerator for the DES symmetric encryption algorithm including 3DES, encryption and decryption of large records in the token would be rather slow due to the communications baud rate and clock of the smart card system. For this reason, a random number generated in the token is used as a one-time session encryption key in the software security module of the client workstation to encrypt the file to be transmitted. That session encryption key is then wrapped by the public key of the intended receiver. This is generally considered a limited exposure to compromise because of the short life of the session encryption key. It is possible to perform the file encryption within the token at the expense of encryption rate performance.

The Datakey Crypto Card Operating System (DKCCOS) v2.0 is the proprietary operating system used with the Model 330 smart card and the Model 380 smart key tokens. Although this operating system is unchangeably embedded in the ROM of the processor chip, it does incorporate a feature in the form of downloadable / executable files (EXFs) that allows for the augmentation and extension of the operating system. It should be noted that there are currently no FIPS approved EXFs and that downloading of EXFs is not currently supported.

With a jump table arrangement it can accommodate patches or changes on major functions or commands. It also allows the addition of new or custom algorithms. The use of EXFs as an adversarial attack channel is prevented by signing the EXF file in the Datakey Signing Facility, and allowing it to execute in the token only if the signature is verified in the token with the signing facility public key embedded in ROM.

- **Token Read / Write Devices**

  Several types of read / write devices are available to provide the smart card interface to the host computer.

  A cable-connected serial port device operating on an RS-232 protocol can be used at baud rates up to 38.4 K baud. This is largely a pass-through device, which supplies power to the token and clock, reset, and I/O interface functions in compliance with ISO 7816. A read / write device of this type also exists for the smart key token.

For the lap-top users and for those desk-top computers equipped with PCMCIA slots, it is possible to perform the smart card interface to the host computer via a PCMCIA to smart card adapter device and the associated card / socket services within the host computer.

The third smart card interface device is the Smarty. It is a battery-powered smart card adapter in the form of a 3 ½ inch floppy disk. It allows the smart card to communicate with host computer via the electromagnetic transducer built into the 3 ½ inch floppy disk drive. The baud rate is less than 5 K baud.

- **SignaSURE™ CIP 4.0 - Cryptographic Interface Provider**

This product combines the products previously marketed as the SignaSURE CIP - Cryptoki Interface Provider and a CSP - Cryptographic Service Provider for MicroSoft Crypto API applications. The product is layered and can be called from either of two APIs.

It allows CAPI-compliant applications to automatically upgrade to token-based information security. The CryptoAPI is a high-level interface between those applications and a standards-based, core cryptographic functionality, and is the foundation technology for the Microsoft Security Framework. This top layer is internally connected to the lower layer, which also has its own API - the Cryptoki API (defined by PKCS #11).

The Cryptoki interface is a medium-level, hardware-independent token interface developed by RSA Data Security, Inc. and its licensees. In the Datakey product, cryptographic calls from the application program to the API and its extensions are translated and passed either to the token or to the software security module embedded in the product for execution.

When a token is first sensed in a read / write port by SignaSURE CIP, all public objects of the token are cached in software, so that any operations involving those objects can be performed in software. Operations involving sensitive objects are required to be performed within the token.

SignaSURE CSP works through CIP, and uses Datakey's smart tokens in a public key infrastructure to process and store private cryptographic data that enables. When these critical operations are performed within the hardware token, a much higher level of information security can be achieved than can be provided by software-only systems.

The Model 330 smart card is capable of performing all private, public, and secret key functions on the smart card. However, performance of all cryptographic functions on the card is not always practical or desirable. When used in conjunction with SignaSURE CIP, all private key functions are performed on the smart card including generation of digital signatures. All public key functions are performed within the security module embedded within SignaSURE CIP. Secret key functions are performed both on the card and in CIP depending upon the application requesting the secret key function.

The security module that is embedded within SignaSURE CIP is the RSA Data Security, Inc. B-Safe software cryptographic toolbox, which contains a collection of symmetric key and public key cryptographic algorithms, hashing algorithms, and key exchange / key agreement algorithms. Other cryptographic algorithms may be added as required to support application requirements.

SignaSURE CIP is therefore a product that is capable of providing user identification and authentication, secure data exchange, and information validation functions to applications written for either the Microsoft CAPI or the Cryptoki API whenever these critical functions require a much higher level of information security than can be provided by software-only systems.

- **SignaSURE™ ESS - Enterprise Security Suite**

The Enterprise Security Suite is Datakey's end-to-end information security solution for the enterprise. ESS works through SignaSURE CIP and uses Datakey's smart cards or smart keys to provide full-function hybrid cryptosystem services to commonly used application software. ESS is integrated seamlessly into Microsoft Office products such as Word, Excel, and Windows Explorer, and runs under Windows 95 and NT.

The basic ESS client package includes the following modules:

- Secure File Services: This module provides the ability to encrypt, and assign read / write privileges to data generated or stored at the workstation (desktop or laptop) thus eliminating the risk of unauthorized access to sensitive company data.

- Web Browser: Netscape Navigator is the client mechanism for requesting and receiving public key certificates. Navigator's security functions are enhanced with SignaSURE smart tokens, allowing the exchange of sensitive information with electronic business partners with the highest confidence in the security of private keys.

- Workstation Token Manager: This application allows users to change passwords and view token objects when the utility is not provided by an application.

- User Mail Package: This package enhances Netscape's Messenger by token-enabling this full-featured, simple-to-use E-mail application.

Datakey markets the full range of Netscape server products.

The following optional server modules provide the infrastructure for the enterprise to support the transmission of secure documents:

- Certificate Server: This module has been designed by Netscape and has been integrated into SignaSURE ESS. It provides the certificate requested by the user via a straightforward graphic user interface.

- Directory Server: This module, also designed by Netscape, is a method for distributing and making public the enterprise's certificates.

One additional module for secure administration of the SignaSURE ESS solution is required:

- SignaSURE Security Control Center: This stand-alone Windows NT workstation is used for the administration and management of the token-based security solution. It provides for the personalization of tokens with the necessary individual user information, PINs, passwords and cryptographic keys. It is also the point in the enterprise system where the critical process related to key recovery begins.

3.0 Comprehensive Security Services

In order to address and deter the threats to compromise the confidentiality, integrity and non-repudiation of files and communications of a typical business enterprise, Datakey's SignaSURE products and solutions apply a broad spectrum of security services based on both symmetric key and public key cryptography. Some of these products and solutions, such as client workstations and smart tokens, are oriented to individuals within the enterprise, while others, primarily servers, support the entire enterprise.

It is noted again that the security (cryptographic) modules are contained both in the secure tokens (in the form of hardware), and in the Cryptographic Interface Provider (in the form of software), and that security functions are executed within these two modules according to the sensitivity of the function. It is reiterated that all private key functions are performed on the secure token and that public key functions are performed in the CIP software.

Other SignaSURE solution components described in section 2, such as SignaSURE ESS, are considered applications. They make cryptographic calls to the Cryptoki API, but all of the cryptographic functions are executed within the cryptographic modules.

The SignaSURE products and solutions provide the following security services:

- **User Authentication**

  User authentication is a process by which an individual may identify himself / herself as the proper owner or user of a device such as a smart token. Typically, a secure token is capable of executing minimal, non-sensitive functions until it is placed into an authenticated state as a result of this activating process.

  Two-factor authentication (based on possession of the token + knowledge of a secret pass phrase) may be accomplished with the secure token either by the enterprise Security Officer (SO) or by the end user.

  "Role-based access" is accomplished by means of security nibbles associated with all files in the token, providing read / update / write / delete / execute access permission to anyone, the enterprise SO, the user, or to no one, depending on the sensitivity of the information contained in the file.

  Under DKCCOS, the PIN file contains either a 20-byte PIN (padded if necessary) or the SHA.1 hash of the pass phrase. The latter provides a higher level of security in the authentication process because the hash of the pass phrase can be initialized to the token without the need for the owner to disclose the pass phrase itself. This method is used as the transport key during the early life cycle of the token while the processor module / token passes through a chain of custodians.

  Three-factor authentication, based on the addition of biometric reference data to the token memory and an external biometric transducer and matching function, is provided by some Datakey business partners.

- **On-line Authentication**

  On-line authentication is a process by which a mutual authentication can be effected between a smart token and the on-line data base of the token issuing system. This type of authentication normally takes the form of a cryptographically-based challenge-response protocol.

  ANSI X9.17 describes a DES-based protocol that utilizes a key shared between the token and the issuing system. A challenge in the form of a random number is passed in one direction, and when received is encrypted by the shared key and the result is returned as the response. The response is then decrypted with the shared key and compared with the original random number. The procedure can then be reversed. This protocol can be implemented using SignaSURE smart tokens. This function is not implemented as a method of authenticating a user to a SignaSURE smart token.

FIPS Publication 196 describes an equivalent challenge-response protocol based on the use of digital signatures. SignaSURE tokens can perform this protocol. As with ANSI X9.17, this method of authentication is not implemented to authenticate a user to the SignaSURE smart token.

- **Hybrid Cryptosystem**

SignaSURE products and solutions utilize a hybrid cryptosystem, that is, a cryptographic system made up of both symmetric key and public key cryptographic algorithms. This is done in order to benefit from the strongest features of both types of algorithms in combination.

For example, symmetric key systems such as DES are very fast and computationally efficient in encrypting / decrypting large data files, and are widely used to protect the integrity of transmitted documents and files independent of encryption. The disadvantages of symmetric key systems are:

1) They require that the communicating parties share cryptographic keys that must be kept secret. Key management for large symmetric key-only systems, comprising the creation, transportation, storage, recovery, and revocation / destruction of keys, is complex and expensive.

2) Effective non-repudiation of the source of messages and files cannot be built with symmetric key systems.

Public key cryptography is complementary to symmetric key cryptography, and the two are used in combination to provide a full set of cryptographic functions.

The most commonly used public key algorithms in use today, RSA and DSS, are computationally intensive, and are therefore limited in use to digital signatures and key exchange / key agreement. (DSS was designed only for digital signatures). Execution time with these algorithms are held within reasonable ranges through the constraint of operations to short data digest (hash) lengths or key length data blocks.

Public key cryptosystems are based on the existence of a pair of keys for each user or entity; these two keys are mathematically related such that a short data block encrypted by one of the two keys can only be decrypted with the other. One of the keys, the private key is securely held and used by its owner, but it is never disclosed , even to himself. The other key, the public key, is broadly distributed to anyone who wishes to communicate securely with its owner.

These characteristics of a public key cryptosystem are ideal for processing digital signatures, and for exchanging symmetric encryption keys with individuals and organizations with whom no previous key sharing relationship had existed.

Digital Signatures

The digital signature is intended to provide the same (or higher) level of confidence and trust when placed on an electronic document as a physical handwritten signature on a printed document. The content of the message, file or document to be "signed" is first hashed, or digested, by a secure one-way function to a small (e.g., 20-byte) hash value. A digital signature is produced by processing the hash value by the highly-protected private key of the originator of the message, file or document. Because the private signature key exists in only one secure repository where it is used, the property of non-repudiation can confidently be attributed to any message, file or document accompanied by a digital signature produced by that private key. The digital signature, to be of any value, needs to be verified by the receiver. The receiver needs only the sender's public key and the same non-secret hashing function.

Symmetric Key Exchange

The other extremely useful function that public key cryptography brings to a hybrid cryptosystem is the ability to provide the two parties involved in an encrypted exchange with the symmetric key used to encrypt the message, file or document being transmitted.

A random number is generated in the sender's cryptographic module and this random number is used as the one-time session encryption key to encrypt the item to be transmitted. The sender's cryptographic module also encrypts the random number with the intended receiver's public key (from a directory) and appends the result to the encrypted item to be transmitted. The intended receiver is the only one who has the intended receiver's private key, and alone can recover the session key, and then decrypt the transmission.

Diffie-Hellman Key Agreement is another algorithm that is used to develop a symmetric session key between two parties. It requires parameter contributions from both parties which can then be combined mathematically by either (or both) parties to derive the session key.

- **Random Number Generation**

  A SHA.1-based pseudorandom number generator is implemented in the Model 330 smart card and Model 380 smart key. A hardware random number generator (HW RNG) is included within the Philips P8WE5032 crypto-processor. The HW RNG is used to add entropy to the FIPS 186-1 pseudorandom number generator built into DKCCOS v2.0.

The pseudorandom number generator built into DKCCOS maintains 16 bytes of secret internal state. When a pseudorandom number is needed, this secret internal state and the output of the HW RNG are hashed with a one-way function to produce a

20-byte hash, four bytes of which are used as pseudorandom output, while the remaining 16 bytes become the new secret internal state. Additional uncertainty can be introduced through an additional entropy file each time a pseudo RN is requested. The contents of this file are hashed along with the secret internal state during the update process.

- **Data Encryption / Decryption**

  Data encryption and decryption, as applied to messages, files and documents is performed with symmetric key algorithms.

  The most commonly used symmetric key algorithm is the Data Encryption Standard (DES). It is block cipher algorithm, which uses a 56-bit key and 8-bit parity, and can operate in a number of modes, including electronic code book (ECB) and Cipher Block Chaining (CBC).

  Stronger versions of DES include triple-DES and DESX. Triple-DES performs three 56-bit operations (encrypt / decrypt / encrypt) using either a double-length or a triple-length key. DESX uses a 56-bit DES operation both preceded and followed by white masking.

  Other commercially-available and proprietary symmetric key encryption algorithms, such as RC2, RC4, CAST and IDEA, are in common use. Several of these algorithms are included within SignaSURE CIP. Any can be added to the Datakey tokens via an EXF.

  These algorithms can run in hardware or software with widely ranging performance (i.e., hundreds of bytes per second in an 8-bit smart card microcontroller, hundreds of thousands of bytes per second on an Intel 80486 PC, and megabytes per second on a DES accelerator chip). For this reason, the preference in a token-based system is to encrypt / decrypt within the software security module, rather than in the token. As indicated above, this is not considered a security exposure because the encryption / decryption is performed using a one-time session key.

  The software security module contained within SignaSURE CIP can perform DES in the ECB and CBC modes, DESX, triple-DES, RC2, RC4 and RC5. Although data encryption within the token is infrequently requested, requests for these functions are supported by the token.

- **Message Authentication**

  Message authentication are cryptographically-based algorithms for protecting the content integrity of messages, files and documents. Message authentication can be implemented in symmetric key or public key systems.

A DES-based message authentication method define in ANSI X9.9 is commonly used to protect wholesale banking funds transfers from alteration during transmission. It uses DES in CBC mode with feedback to generate a Message Authentication Code (MAC) that is appended to the message. It can be used with or without encryption.

Message authentication with public key cryptography uses digital signatures. Successful digital signature verification by the receiver provides proof that no message alteration could have occurred.

Both SignaSURE CIP and the SignaSURE smart tokens can perform either method..

- **Public Key Functions and Public Key Pair Generation**

  SignaSURE solutions support the use of public key cryptography in two primary functions - digital signatures and key management (exchange / agreement) for symmetric encryption keys.

  While a single RSA key may be used for both functions, there is a strong rationale behind the trend to use separate keys:

  - The digital signature is an individual, personal and private entity, and the private key that is used to generate digital signatures must be safeguarded such that it can never be used by anyone other than the owner in an authenticated environment. If this level of safeguarding is not afforded the signature private key, then the masquerading of one individual by another would be possible, thereby compromising the property of non-repudiation.

    It is an absolute requirement by many user establishments that the private signature key be generated *within a secure token, by the token end-user* (who is also the owner of the key token), thus providing the token end-user with the total confidence that no other person has ever seen the key. It is also required that the end-user cannot know the private key in order to use it, and that the secure token operating system will not permit the private key to be exported from the token.

    This treatment of the signature private key provides no means for backup, escrow or recovery. If the end-user loses his / her token, or if the token becomes locked because of multiple erroneous PIN entries, that signature key pair is dead, then any certificates based on it must be revoked.

  - It is broadly accepted that the public key pair used for session encryption key exchange needs to be recoverable by an authorized key recovery agent. This requirement is normally imposed by the user enterprise in order to protect availability to its intellectual property, and may additionally be imposed by the government for law enforcement reasons.

SignaSURE tokens provide for the injection of public key pairs that are generated outside the token in order to accommodate secure backup procedures. This is a primary function of the Security Control Center. The backup must be done prior to key injection; otherwise it is not possible to access the private key. The tokens may be configured to allow either the enterprise security officer and / or the end-user to inject keys, and to allow the end-user to generate keys in the token.

SignaSURE CIP provides for RSA key pair generation in software.

- **Digital Signature Generation and Verification**

  The need for secure generation of digital signatures was addressed in the previous section. However, digital signature verification is normally performed in software because it is a non-sensitive public key operation.

  The cryptographic module within SignaSURE CIP is able to perform hashing functions using SHA.1, MD2 and MD5 and to perform digital signature functions in DSS and RSA. When digital signature generation is performed within the SignaSURE token, the hash function is first performed in software.

  The SignaSURE tokens can perform SHA.1 hashing, but for performance reasons is used predominantly with EXF signature verification, random number generation and for pass phrase authentication. In addition, digital signature verification can be performed on the token if desired.

- **Session Encryption Key Exchange**

  The process performed by the sender involves encryption of the random session key ("wrapping") with the public key of the intended receiver. Because this is a public key function, it is normally done in software. Key exchange based on RSA or Diffie-Hellman Key Agreement can be performed within the SignaSURE CIP.

  The process performed by the receiver involves decryption of the random session key ("unwrapping") with the private key of the intended receiver, and is therefore done within the intended receiver's secure token.

  An enterprise that chooses to absorb the performance degradation and perform data encryption and decryption within the token, may also perform key wrapping in the token.

4.0 SignaSURE™ Token Early Life Cycle

The early life cycle that a token and its processor device experiences is significant from the standpoint of the protection that is provided against adversarial scenarios such as the loading of "Trojan horse routines" and interception of shipments / counterfeit issue. The phases of the life cycle described here are typical for all SignaSURE tokens, but variations in the latter phases may occur. This process is representative of the one implemented for the Model 330 smart card.

Microelectronics Manufacturer

It all begins with the microelectronics manufacturer, who produces the processor chip with the DKCCOS operating system contained in its ROM. Also embedded in the ROM at the time of manufacture are:

- a fabrication key which contains the SHA.1 hash of a pass phrase that the next custodian of the device or token will use to gain authenticated access. The pass phrase is known only to Datakey.
- the SHA.1 hash of the public key associated with the Datakey EXF signing facility.
- the code necessary to perform the Power-On Self Test (POST) of all major processor functions.

All processor chips are tested at the wafer level (prior to dicing into chips).

The microelectronics manufacturer normally packages the processor chip into smart card modules or other token packages, or supplies raw die (used to produce the Model 380 Smart Key).

Token Manufacturer (Datakey or Certified Vendor)

The token manufacturer is the second custodian of the device. At this phase the processor module (or raw die) is fabricated into the smart card (or smart key).

Authenticated access is obtained by entering the secret pass phrase. The token file system is formatted, and the hash of the next custodian's pass phrase is entered.

Token Initialization Center (Datakey or Certified Vendor)

At this phase user enterprise batch data is entered into the token, written onto a magnetic stripe (if present), or printed on the surface of the token.

Authenticated access is obtained by entering the current custodian's pass phrase. Files such as the ATR (answer-to-reset) File, DKIS File, User Entropy File and the Token

Configuration File are created and initialized. The hash of the next custodian's pass phrase is entered. Normally this would be the user enterprise security officer.

It is conceivable that this phase would be performed by a certified initialization center and that the user enterprise would contract with the initialization center to enter user specific data (name, account number / employee number, expiration date, PINs / pass phrases, cryptographic keys and photograph) in / on the token in addition to the batch data described above.

User Enterprise Security Officer

Here is where the scenarios diverge.

The first scenario is one in which the enterprise security officer receives all tokens from the initialization center and takes a strong role in the personalization and issuance of the tokens to the end users, through the use of the SignaSURE Security Control Center.

Authenticated access to a token is obtained by entering the security officer's pass phrase. After entering user-specific data, one of the SO's first tasks is to write the enterprise override conditions to the Configuration File defaults, as required and permitted.

Setting up the token for user authentication can be handled in two ways:

- Receive from the user the hash of his / her pass phrase (if the user has the ability to provide it) and enter the hash into the token.

- Generate a random initial user PIN and enter it into the token, and subsequently deliver the initial PIN to the user via some secure procedure.

The User's Confidentiality public key pair is generated in the SCC, backed up as required for key recovery, and injected into the token.

The token is then delivered to the end user.

Other scenarios involve the delivery of token directly from the initialization center to the end users and an equivalent set of functions performed by the SO between the Security Control Center and the user's client workstation.

End User

Authenticated access to the token is achieved either by entering his / her predetermined pass phrase, or by entering the initial user PIN communicated by the SO, and immediately changing it.

The user then generates the user’s signature key pair within the token by invoking the function in the application supported by SignaSURE 4.0. The user then follows enterprise procedures for obtaining digital certificates.

An EXF may be installed or removed during this process, transparent to the user and under control of SignaSURE CIP.

5.0 Key Management

The module provides the following types of keys:

- Single DES
- 2key Triple DES
- RSA public and private keys
- DH/DSA keys

The Security Officer Role is able to generate a DES key. The SO Role may also load an EXF, which will use an RSA public key stored in ROM to verify the signature. Access to the EXF public key is controlled by the LoadEXF command. The User Role is able to generate and access any key type allowed on the card. The User Role may also load an EXF thereby providing access to the EXF public key. In FIPS mode, there is no ability to generate or access cryptographic keys from an unauthenticated mode.

Each of these keys is stored in plaintext in the module’s non-volatile memory (EEPROM) and access to each key is governed by the file permissions. The keys may be zeroized at any time by calling the Recycle command. This command will delete all files in the EEPROM except for the SHA-1 protected Configuration file, ATR file, and the SO PIN file.

Additionally, this subject is addressed in the sections of this document labeled:

- Hybrid Cryptosystem
- Public Key Functions and Public Key Pair Generation
- Session Encryption Key Exchange

6.0 PIN / Pass Phrase Management

This subject is addressed in the sections of this document labeled:

- User Authentication
- SignaSURE Token Early Life Cycle

7.0 Roles and Services

The Datakey Model 330 smart card provides two roles, the Security Officer (SO) and the User role. The Security Officer is tantamount to the Crypto-officer in FIPS 140-1 terminology. Each role is assigned various services.

Security Officer Role

The SO role is responsible for configuring the card (specifying which algorithms are allowed on the card, which keys may be generated, who may generate keys, etc.) and setting up the User's password. Specifically, the SO is allotted to following services:

- ChangeConfiguration
- CreateFile
- DeleteFile
- EndSession
- GenerateDESKey
- GenerateRandomNumber
- GetStatus
- LoadEXF
- ReadBinary
- Recycle
- SelectFile
- SHA1
- UpdatePIN
- WriteBinary

User Role

The User role is essentially the end user and thus has access to all of the cryptographic functions of the module, but does not have the access (that the Security Officer has) to the card configuration functions. Specifically, the User is provided the following services:

- CreateFile
- Crypt
- DeleteFile
- DH/DSAGenerateKey
- DHKeyAgreement
- DSASign
- DSAVerify
- EndSession
- Format
- GenerateDESKey
- GenerateRandomNumber
- GetStatus
- LoadEXF
- ReadBinary
- Recycle
- RSADecrypt
- RSAEncrypt
- RSASign
- RSAVerify
- SelectFile
- SHA1
- UpdatePIN
- WriteBinary

Additionally, two command are available without authentication, Verify and GetStatus, commands which only provide general card status and do not provide access to cryptographic services or objects on the card. Furthermore, the Datakey Model 330 smart card implements a method of restricting access to data and objects based upon the role authenticated. Each data or key object is stored as a file, and each file has an associated security nibble in the file header. The security nibble determines whether the SO, User, anyone, or no one has access to read, write, update, execute (use a key), or delete the file. This subject is addressed in the SignaSURE Token Early Life Cycle section of this document and in the section that follows.

8.0 User Enterprise Security Policy

Enterprise security policy varies widely depending on the type of business involved and the value of intellectual property and other assets addressed by the policy. The SignaSURE information security solutions have been designed, and have evolved, to accommodate the diversity of security policy in a manner that does not compromise a restrictive policy nor impose unnecessary requirements on a more permissive policy.

Because SignaSURE solutions are token-based, it follows that some policy issues are dictated by how the token is designed and how it is configured. This is best illustrated with some specific examples:

- Associated with all files in the token are security nibbles that assign access permissions relative to read, update, write, delete and execute to never, SO, user, and anyone.

- Cryptoki (PKCS #11) is a commonly-used cryptographic token API. When a token is first sensed under this API, all public objects are cached in host PC software, so that any operations involving those objects can be performed at host processing speed in software. In some applications, under specific circumstances, private keys can be considered “non-sensitive” objects, and if the application design allows it, that private key file may allow an authenticated read permission, thereby facilitating a private key operation in the host software security module.

  To protect the restricted policy environments, the token operating system was designed to perform private key operations within the token only if the private key file has only “never” access permissions.

- The Configuration File in the token allows for the enabling / disabling of cryptographic algorithms, algorithm modes and key lengths. Some of these bits are important for tokens to be exported. Other bits in the Configuration File relate to the enterprise security policy such as:

  - Is a “would-be security officer” allowed to issue a recycle command to a token in his / her possession, and become the de-facto SO, as opposed to being required to enter the pre-designated pass phrase?

  - Is the SO authorized to update a user’s PIN on a locked card?

Each of the bits in the Configuration File has a companion bit in a mask, which if set to 0 prevents any further change to the configuration bit during the life of the token, and if set to 1 allows override by the enterprise SO. The mask bit can also be changed from 1 to 0, but not from 0 to 1.

9.0 Rules of Operation

To operate the module in a FIPS compliant manner the following rules should be observed.

- Only FIPS approved EXFs should be loaded while in FIPS-mode
- Use of the RSA algorithm should be limited to signature generation/verification (PKCS#1) and key exchange. RSA should not be used for encryption/decryption while in FIPS-mode.

10.0 Physical Security

The Datakey Model 330 smart card has special physical security mechanisms to allow the end user to detect attempts to tamper with the card. Specifically the user should check for the following tamper evidence.

- Scratches, deformed plastic, or cuts in the plastic surrounding the IC contacts
- Deformation or creases in the plastic of the card beyond normal wear
- Torn or broken plastic on the back side of the card near the contacts

If tamper evidence is detected, the user should discontinue use of the card and contact their Security Officer.