# Rosetta™
## Security Policy

# Rosetta™
# Security Policy

512-100000-01

September 1999

# Contents

# Introduction

The Rosetta security module contains the SPYRUS Card Operating System (SPYCOS™), which provides initialization, configuration, and cryptographic services. It features high assurance security techniques to properly isolate applications and application data, public key cryptographic techniques for industry standard sign/verify operations, and advanced operating system and chip features.

Rosetta is part of a flexible high-assurance system that facilitates the development of new multi-application functions and provides a complete development environment. The Rosetta security module is embedded in the Rosetta Smart Card, which the U.S. Government will use in its Defense Messaging System (DMS).

# Product Overview

The strength of Rosetta is in the high assurance mechanisms of SPYCOS. By using the security features of the SPYRUS PCMCIA form factor devices high-grade hardware security products, Rosetta provides a secure environment for application developers.

SPYCOS security mechanisms include:

- File and application based secure access controls
- Secure messaging and authentication
- Security manager for policy enforcement
- Anti-tearing failsafe linkage
- Public key cryptographic support
- Algorithm Agile™ cryptographic functions
- Digital Signature Algorithm (DSA) FIPS PUB 186-2
- Data Encryption Standard (DES) FIPS PUB 46-3
- RSA Signature and Verification[1]

[1] Not available in FIPS 140-1 mode, based on policy.

# Cryptographic Functions

This section describes the cryptographic capabilities of Rosetta. Before using these cryptographic features, Rosetta provides initialization and configuration services of modules. These services have been designed to provide two separate roles, one for initialization and configuration of the module (Crypto-officer), and the second for general use (User).

| **Encryption & Decryption** |
|---|
| DES (ECB64, CBC64)**{**xe "Data Encryption Algorithm (DEA, DES)"**}** |
| Triple DES (2 Key and 3 Key)[2]**{**xe "Data Encryption Algorithm (DEA, DES)"**}** |
| Skipjack (ECB64) (internal use only)**{**xe "Skipjack"**}** |
| **Key Wrap & Unwrap** |
| DES (ECB64, CBC64)**{**xe "Data Encryption Algorithm (DEA, DES)"**}** |
| Triple DES (2 Key and 3 Key)[2]**{**xe "Data Encryption Algorithm (DEA, DES)"**}** |
| **Digital Signatures** |
| DSA**{**xe "Digital Signature Algorithm (DSA, DSS)"**}** |
| RSA (512-1024 bit)[2]**{**xe "RSA"**}** |
| **Digital Signature Verification** |
| RSA (512-1024 bit)[2]**{**xe "RSA"**}** |
| **Key Transport / Key Agreement** |
| RSA (512-1024 bit)[2]**{**xe "RSA"**}** |
| KEA[3] (Primitives on**{**xe "Key Exchange Algorithm (KEA)"**}**ly) |

**Table 1. Rosetta Supported Algorithms**

[2] Not available in FIPS 140-1 mode, based on policy.

[3] Primitives only. The final steps of the KEA key agreements are performed off the token. All private operations are performed on the token.

## Commands Supported

The following table shows commands supported by the Rosetta module and the SPYCOS file system. These commands are separated into three sections: ISO 7816-4, SPYCOS, and general cryptographic commands.

| ISO 7816-4 Commands | Cryptographic Commands | SPYCOS Commands |
|---|---|---|
| Get Response | Change PIN | Create File |
| Read Binary | Check PIN | Delete File |
| Select File | Decrypt (DES) | Directory |
| Update Binary | DSA Sign | Extend |
| Verify | Encrypt (DES) | Invalidate (Disable) |
| | Extract X | Rehabilitate (Enable) |
| | Generate Ra | Status |
| | Generate Random | |
| | Generate TEK | |
| | Generate X | |
| | Install X | |
| | Load Cryptographic Data | |
| | Load Key | |
| | Load Secure RSA Private | |
| | Load X | |
| | Relay X | |
| | RSA Sign | |
| | RSA Unwrap Key | |
| | RSA Verify Signature | |
| | RSA Wrap Key | |
| | Set Key | |

# Roles

Rosetta supports two roles, Crypto-officer (or Site-Security Officer (SSO)) and User, and enforces the separation of these roles by restricting the services available to each one. Access is controlled by Personal Identification Number (PIN) verification on the card prior to performing any services. When verifying the PIN, the role must be explicitly selected by entering the pin index. Index 0 is selecting when logging in as SSO and index 1 when authenticating as User.

The following table outlines the commands available to the different roles.

| **Both User and SSO** | **SSO Only** |
|---|---|
| Check PIN (Verify) | Change PIN[4] |
| Create File | Extract X |
| Decrypt (DES) | |
| Delete File | |
| Directory | **User Only** |
| Encrypt (DES) | DSA Sign |
| Extend | Generate TEK |
| Generate Ra | |
| Generate Random | |
| Get Response | |
| Invalidate (Disable) | |
| Load Cryptographic Data | |
| Load Key | |
| Read Binary | **Crypto-officer or User (affects privileges of the private key)** |
| Rehabilitate (Enable) | Generate X |
| RSA Sign | Install X |
| RSA Unwrap Key | Load X |
| RSA Verify Signature | |
| RSA Wrap Key | |
| Select File | |
| Set Key | |
| Status | |
| Update Binary | |

[4] The module may be configured to restrict the Change PIN functionality so it may only be accessed by the Crypto-officer.

## Crypto-officer Role

The Crypto-officer is responsible for initializing the Rosetta module. Initialization is typically performed using a Certificate Authority Workstation (CAW) that is secured according to the site security policy of the deploying organization.

Before issuing a token to an end user, the Crypto-officer initializes the token with private keying material and certificate information. Rosetta validates the Crypto-officer role via the PIN before accepting any initialization commands.

Following is a list of the initialization steps for the Rosetta Module:

1. The Crypto officer will change the default SSO and User PINs.
2. The Crypto officer will then load the trusted certificate of the certificate hierarchy .
3. The Crypto officer may then generate public/private key pairs, loads the user's certificates, and loads the user's certificate authority's certificates into the card.

   (Note: The Crypto-officer is responsible for obtaining all certificate material in accord with the security policy of the organization.)

## User Role

The User role is available after Rosetta has been loaded with a User PIN. The cryptographic functions are enabled, with the exception of Change PIN Phrase (based on policy) and Extract X.

The exclusion of these commands is the mechanism for separating the Crypto-officer and User roles. Rosetta validates the User role via a PIN before access is granted. When the user has been successfully authenticated, he or she can then choose one of the available personalities on the card. Each personality corresponds to a separate public/private key pair plus other information. The Crypto-officer may set up these user personalities during the initialization process.

# Services

## Power-On Self Tests

During a reset of Rosetta, the module performs a series of checks on the required cryptographic algorithms and on the integrity of the code. These tests verify that the FIP140-1 approved cryptographic algorithms, resident on the card, are functioning properly. Each cryptographic algorithm performs a known answer test to verify proper functioning. An error with any of the power-on self-tests results in an error being output and the cryptographic module going into an error state in which no commands are accepted or processed.

## Initialization

The Crypto-officer initializes Rosetta before distributing it to a user. Initialization consists of the following:

- Authenticating the Crypto-officer based on PIN input
- Loading the Initialization parameters
- Loading an X.509 certificate into a *trusted certificate* space
- Generating public/private key pairs for the user
- Obtaining and loading X.509 certificates for the user
- Specifying a user PIN

Upon completion of the Initialization process, Rosetta provides encryption/decryption, key transport, digital signature, and key management cryptographic services.

## Encryption/Decryption

The Rosetta module can perform encryption and decryption services for several different modes of DES: ECB64 and CBC64. Both the Encrypt and Decrypt commands support several modes of processing for user data. A key must be generated or loaded and set before these commands can be executed prior to executing these commands a key must be loaded into a key register(s). For the cipher block modes of the selected algorithms, the Generate IV or Load IV command must have been previously executed.

### Key Transport

The Rosetta module exchange process can use symmetric key cryptography to encrypt (*wrap*) the key used in the encryption algorithm. The wrapped key can then be securely transmitted to the recipient. Key exchange allows only the intended recipient to unwrap the needed key to decrypt data. The Rosetta module supports DES for this key exchange process.

Rosetta also supports the primitives of the KEA algorithm. Users may perform all KEA private key operations on the Rosetta module and then use the results to derive the symmetric keying material to be used on the host.

### Digital Signature

A digital signature allows a message originator to sign data and provides a recipient a means of verifying the originator's identity (authentication and non-repudiation). Any change in the data causes a change in the hash value. A recipient can then use the cryptography to verify the originator's digital signature over the hash value to verify the integrity of the data. Rosetta supports digital signature with the Digital Signature Algorithm (DSA).

Digital signatures do not encrypt, transform, or otherwise alter data, so sensitive data is usually signed and then encrypted. The signature may or may not be encrypted. Alternately, a digital signature can be used as an integrity check value (ICV) wherein the data is encrypted before signing. However, this method is not routinely implemented.

### Key Management

The primary key management responsibility of Rosetta is the administration of the RSA[5], DSA, and KEA private keying material. The key management concept employed in Rosetta provides a robust yet practical solution. The card provides key generation[6] and key archival functions and allows a user to perform revocation, expiration, notification, and authentication functions. The key management functions of Rosetta also provide the functionality for secure key archival, extraction, and relay.

[5] Based on policy and not available in FIPs mode
[6] For DSA and KEA

## Matrix of Cryptographic Functions

Table 2 summarizes the services performed by Rosetta, including the roles for which the service is available and whether the service performs cryptographic functions. The functionality listed in the *Cryptographic Functions* section may be achieved by a single command or by a combination of the commands listed below.

| | Roles | | Cryptographic Functions | |
|---|---|---|---|---|
| **Services** | **Crypto-Officer** | **User** | **Yes** | **No** |
| Block Pin | X | | | X |
| Change PIN Phrase | X | | X | |
| Check PIN Phrase | X | X | X | |
| Decrypt | X | X | X | |
| Delete File | X | X | | X |
| Delete Key | X | X | | X |
| DSA Sign | | X | X | |
| Encrypt | X | X | X | |
| Extract X | X | | X | |
| Generate IV | X | X | X | |
| Generate Mek | X | X | X | |
| Generate Ra | X | X | X | |
| Generate Random Number | X | X | X | |
| Generate TEK | | X | X | |
| Generate X | X | X | X | |
| Install X | X | X | X | |
| Load DSA Parameters | X | X | | X |
| Load IV | X | X | | X |
| Load X | X | X | X | |
| Relay | X | X | X | |
| RSA Sign | X | X | X | |
| RSA Verify Signature | X | X | X | |
| Secure Key Load | X | X | X | |
| Self-test | X | X | X | |
| Set Key | X | X | | X |
| Set Personality | X | X | | X |
| Unblock Pin | X | | X | |
| Zeroize | X | X | X | |

**Table 2. Matrix of Services, Roles, and Cryptographic Functions**

# Key Lifecycles

This section describes the lifecycle of the keys that are generated, stored, and used by Rosetta.

## Storage Key - Ks

The storage key (Ks) is the module's long term key encryption key. This key is loaded at initialization time by the SSO. The key is unwrapped on the card at the start of every session by a cryptographic function using the PIN. The storage key is used **only** for the purpose of internally wrapping the asymmetric private keying material. Ks may never be extracted or used for any other purpose.

## DES Keys

The Rosetta module provides DES as a basic cryptographic service. DES may be used by the Encrypt and Decrypt commands. DES keys may be loaded into the card in their plaintext form, or may be randomly generated. A DES key resides in one of nine internal key registers. After a DES key is loaded in or generated on the card, its plaintext value is never exposed. When power is removed from the card, the contents of the key registers are lost.

## KEA/DSA Keys

KEA is an asymmetric algorithm used for key exchange and the generation of Token Encryption Keys (TEKs). DSA is an asymmetric algorithm used for the generation and verification of digital signatures. DSA and KEA keys consist of two discrete but related parts, the private (X) value and the public (Y) value. KEA/DSA private keys may be randomly generated on the card using the Generate_X function or may be loaded directly on the card in their plaintext form using the Load_X command. After a KEA/DSA private key is loaded on the card, its plaintext value is never exposed. When a KEA/DSA private key must be extracted from the card, it must first be wrapped using the Extract X command. An extracted private key is restored to the card using the Install X command. When a private key is extracted, it is encrypted with a TEK and a password, protecting the contents of the original private key. When power is removed from the card, the contents of all private keys stored in non-volatile memory are maintained. These private keys can be deleted only when the Zeroize or Delete File commands are issued.

## RSA Keys

RSA is an asymmetric algorithm used for both key exchange and the generation and verification of digital signatures. RSA keys consist of discrete but related parts, the private (X) value and the public key comprised of the public modulus and the public exponent. RSA private keys may be loaded directly in the card in their plaintext form or may be loaded securely wrapped in a DES key. After an RSA private key is loaded, its plaintext value is never exposed outside the card. When power is removed from the card, the private key contents stored in non-volatile memory are maintained. These private keys can be deleted only when the Zeroize or Delete File commands are issued.

# Physical Security

The Rosetta module may be packaged in the smart card form factor. The Rosetta Smart Card packaging complies with the ISO 7816 standard. This packaging is tamper evident but is not tamper proof. If there is evidence of physical tampering or if the card is lost, the user should report the incident at once to the Crypto-officer or Certificate Authority.

# Related Documents

*Firmware Implementation Guidelines for the FORTEZZA Crypto Card*. Version 1.0, July 8, 1995

*FORTEZZA Application Implementor's Guide*. Revision 1.52., March 5, 1996

*FORTEZZA Cryptologic Interface Programmer's Guide*. Revision 1.52, January 30, 1996

*SPEX/ Application Program Interface for the FORTEZZA Crypto Card and Lynks Privacy Card.* February 10, 1998

*SPYCOS Interface Control Document Version 2.0*

*ISO/IEC 7816* : *Identification cards – Integrated circuit(s) cards with contacts*

Part 3 : Electronic signals and transmission protocols, 1989-9-15

AMENDMENT 1 : Protocol type T=1, asynchronous half duplex block transmission protocol, 1992-12-01

AMENDMENT 2 : Revision of protocol type selection, 1994-12-1

Part 3 : Inter-industry commands for interchange, 2nd ed., 1997-12-15

Part 4 : Inter-industry commands for interchange, 1995-9-1

# Revision History

| REV. # | DATE | DESCRIPTION |
|---|---|---|
| 01 | June - July 1999 | Draft |
| 02 | October 1999 | Compiled user inputs |
| | | |
| | | |