SRKCRYPTO™

(SRKCrypto.dll)

Security Policy

FIPS 140-2

V 3.4.1
March 27, 2006

Table of Contents

Related Documents

Title	Location	Description
FIPS Technical Documentation		Document to be submitted along with module for FIPS certification.

1. Background

1.1 Purpose

This is the non-proprietary FIPS 140-2 security policy for the SRKCRYPTO™ software Cryptographic Module developed by Tutarus Corporation (T.C.). This T.C. Security Policy details the secure operation of the SRKCRYPTO™ Module as required in Federal Information Processing Standards Publication 140-2 (FIPS 140-2) as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

1.2 References

For more information on the SRKCRYPTO™ module, please visit http://www.tutarus.com. For more information on the FIPS 140-2 cryptographic module validation program and the validation process or information on NIST, please visit http://csrc.nist.gov/cryptval.

2. Overview

The SRKCRYPTO™ module is a software module package as a Dynamic-link Library (DLL) on the Microsoft Windows XP SP2 operating system. The library can be used on Microsoft Windows NT™, 2000, and XP™ operating systems. It has been tested against the FIPS 140-2 requirements on the Microsoft Windows XP™ SP2 operating system.

2.1 FIPS 140-2 Compliance

The SRKCRYPTO™ module provides high-level encryption for Tutarus's suite of security products and has because SRKCRYPTO has been designed and implemented against the FIPS 140-2 requirements, the SRKCRYPTO module needs no special configuration to operate in a FIPS compliant manner. Put another way, the SRKCRYPTO module functions in a FIPS compliant manner at all times.

2.2 Access to the Module

Because the SRKCRYPTO module is a software library, an operator or calling application accesses the module via API calls. Calling applications will implicitly chose a role based on the module service requested. Moreover, a calling application will assume only one role in a particular instance in time.

2.3 FIPS-Approved Algorithms

The SRKCRYPTO™ module provides confidentiality, integrity, and message services. It supports the following algorithms: AES, RSA PKCS v1.5, SHA-1, and SHA-256. In addition, the module performs random number generation using the PRNG described in appendix A.2.4 of ANSI X9.31.

2.4 Data Management

The calling application supplies all keys that the module will use while performing services. The module will use the supplied keys to encrypt or decrypted data, generate pseudo-random

number, or verify RSA PKCS#1 digital signatures and will then immediately destroy (zeroize) those keys upon completion.

Table 1 –Key Management Table

Module Keys

KEY	Description/ Usage	Generation	Storage	Entry/ Output	Destruction	Establishment
256-bit AES	Key used to encrypt or decrypt information	The module does not generate keys.	Plaintext in RAM.	Keys are entered as plaintext but never output.	All keys are zeroized.	Not established.
112-bit PRNG seed key	Key used in PRNG	The module does not generate keys.	Plaintext in RAM.	Keys are entered as plaintext but never output.	All keys are zeroized.	Not established.
2048-bit RSA PkCS#1 public key	Key used to verify PKCS#1 signatures	The module does not generate keys.	Plaintext in RAM.	Keys are entered as plaintext but never output.	All keys are zeroized.	Not established.

3. Security Specification

This section describes the Tutarus Corporation SRKCRYPTO™ module, version 2.2, and details the applicable security rules and specifications. As per the FIPS 140-2 publication requirements, the SRKCRYPTO™ module is a FIPS 140-2 level 1 software module and is implemented as a multi-chip standalone module.

As a multiple-chip standalone module, it consists of the following generic components:

- A commercially available, general-purpose hardware computing platform that conforms to FCC standards.
- The SRKCRYPTO module has been tested and validated on the Microsoft Windows™ XP SP2. In addition, the module will maintain its FIPS 140-2 validation compliance when executed on the compatible operating systems listed here:
    - Microsoft Windows™
        - NT Workstation 4.0 Service Pack 6
        - 2000 Service Pack 4
        - XP Home Service pack 2

Table 2 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module	1
Module Interfaces	1
Roles and Services	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Key Management	1
Cryptographic Algorithms	1
EMI/EMC	1
Self Test	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3.1 Cryptographic Boundary and Physical Interfaces

The module's logical cryptographic boundary includes the executable image of the module upon disk and the module's machine code executing in memory. As the module is a defined as a multiple-chip standalone module, the module also possesses a physical boundary, and this physical cryptographic boundary includes the generic PC upon which the module executes.

The module's interfaces also consist of both logical interfaces and physical ports; however, because the module is a software cryptographic library, the module does not transmit any information across the physical ports of the computer upon which it runs, rather, the module's interfaces are all logical ones, provided through the SRKCRYPTO API, which a calling application can use.

Calls to these API functions constitute the module's control input interface, with the input arguments to these API functions forming the module's data input interface. Likewise, the return codes and output parameters form the module's data output interface. Moreover, the module provides a status output function that provides a calling application with the details of the module's current state. By logically separating the information according to the defined API, the module can always distinguish between control and data inputs and between data and status outputs.

4. Roles and Services

As required by the FIPS 140-2 requirements, the SRKCRYPTO module supports the following two operator roles:

- User Role
- Cryptographic Officer Role

4.1 User Role

The module provides the User role with the following services:

4.1.1 Helper Services

These services provide the calling application with helper functions to convert between ASCII text and base64 encodings.

4.1.2 Encrypt Data:

This service utilizes the FIPS-197 AES function to perform data encryption.

4.1.3 Decrypt Data:

This service utilizes the FIPS-197 AES function to perform data decryption.

4.1.4 Hash Data functions

This service utilizes the SHA-1 and SHA-256 functions to hash data.

4.1.5 Random Number Generation

This service utilizes the module's PRNG to generate random numbers.

4.1.6 Show Status:

This service outputs the module's current status.

4.2 Cryptographic Officer Role

The module provides the Crypto-officer role with all User services as well as one additional service:

4.2.1 Verify RSA signatures:

This service utilizes the RSA PKCS #1 v1.5 function to perform verification of RSA signatures.

5. Security Rules

This section documents the security rules enforced by the SRKCRYPTO module to implement the security requirements of this FIPS 140-2 Level 1 module when used in conjunction with the specified hardware and software.

5.1 Roles

The cryptographic module's primary role during operation shall be that of the user role providing access to the module.

5.2 Keys

The module does not generate, establish, or output keys. Operators (calling applications) enter keys as input parameters for the particular service requested, the module then uses those keys for the duration of that service request, and when complete, the module zeroizes the keys.

5.3 Key Entry

Calling applications enter CSPs electronically and keys are entered in plaintext form into the module through input parameters associated with a given function. The SRKCRYPTO module does not output any keys and when the module has finished with a given cryptographic operation, it will zeroize the key before returning.

5.4 Pseudo Random Number Generator (PRNG) Continuous Test

The module performs a continuous self-test to insure that the random numbers generated by the module's PRNG are not the same. For more details regarding the continuous self-test, please see section 5.7.

5.5 Power Up Self-Test State

While the module performs its power up self-tests, no cryptographic services are available to operators.

5.6 Power Up

Upon power-up, the SRKCRYPTO™ module performs the following tests:

- SHA-1 Algorithm KAT (Known Answer Test)
- RSA Verify KAT (Known Answer Test)
- Integrity Test: the module verifies its integrity by verifying its RSA PKCS #1 v1.5 with SHA-1 signature at power-up.
- SHA-256 Algorithm KAT (Known Answer Test)
- AES-256 Encryption and Decryption Algorithm KAT
- PRNG Algorithm KAT: a known seed is passed to the ANSI X9.31 algorithm and the result is compared internally to a known answer.

Upon successful completion of the self-tests, the module sets the 32-bit unsigned state variable to the "READY" state. If any of the above known answer tests (KAT) fail, by producing an unexpected result, or if the software integrity test fails due to a failure to verify the RSA signature, or if any conditional test fails, the SRKCRYPTO™ module will go into an error state and not accept input or produce output until it is reinitialized and successfully passes its self-tests. Any keys present in the module will be zeroized, and the status will be returned to the caller application indicating the error. To exit the error state, the module must be unloaded and reloaded.

If the User desires to run the power-up self-tests, the User may do so by unloading and reloading the module.

5.7 Continuous Self-test

Prior to using any values from a PRNG, a continuous self-test is performed. The test consists of generating two values from the PRNG and insuring that those two values are different. Once this test has passed, the second value is used.

5.8 Zeroized Transitions

The SRKCRYPTO™ module will zeroize cryptographic keys upon completion of requested service.

5.9 Module Status

The SRKCRYPTO™ module status will be determined by a state variable that will be available to the caller application.

5.10 Concurrent Users

The SRKCRYPTO™ module does not support concurrent users; rather, each calling application would receive its own instance of the module.

5.11 Definition of Critical Security Parameters (CSP):

The following are critical security parameters contained in the SRKCRYPTO™ Module:

- PRNG Seed Keys

- AES encryption/decryption keys
- RSA Public keys

The module does not store any of these User supplied keys, and instead, the module zeroizes these keys when it has completed the cryptographic operation requested by the User. During the key zeroization process, the module cannot perform other functions.

5.12 Error State:

When the module enters an error state (for example, due to a self test failure) the following steps occur:

5.12.1 CSPs zeroization:

The module will zeroize any CSPs in memory.

5.12.2 Set Fault Flag:

The module sets a “fault” flag to indicate a fault has occurred.

5.12.3 Error Code:

The module returns the applicable error code to the calling application via the status output interface.

After entering an error state, the module will prevent the use of cryptographic operations as follows:

5.12.4 Fault Flag:

All data input interface methods of the module check the fault flag before processing the data request. The error code is returned to the caller application via the status output interface if the fault flag is set.

5.12.5 Get State:

This function will report the current state of the module and will report if the module is in an error state.

5.12.6 Fault Flag Reset:

The only way to reset the fault flag is to reload the module (i.e. unload the module from memory and reload it).

6. Roles, Access Control, and Services

6.1 Role and Services with Access Rights

Referring to section 4.0 and 5.0 the Roles and Services can be summarized as follows:

Table 4 – Roles, Services, and Access Rights

Module Keys

Role		Service	CSP Modes of Access
User	C.O.		
X	X	Helper Services	None
X	X	Encrypt/Decrpyt Data	AES keys input & zeroization
X	X	Hashing Services	None
X	X	Random Number Generation	PRNG Seed key input & zeroization
X	X	Show Status	None
	X	RSA Signature Verification	RSA public key input & zeroization

6.2 Mitigation of Other Attacks

Tutarus Corporation does not claim the SRKCRYPTO module mitigates any other attacks.

7. Appendix A

7.1 Definitions

ANSI	American National Standards Institute
CSP	Critical Security Parameter
DEK	Data Encryption Key
DLL	Dynamic-link Libraries
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
OS	Operating System
PC	Personal Computer
PRNG	Pseudo Random Number Generator
SHA	Secure Hash Algorithm
TC	Tutarus Corporation

Change History

Date	Description	Stakeholder
2/01/05	Outline created	Kelly Nelson/Bryan Haddock
2/08/05	Body Edited and Elaborated	Kelly Nelson/Bryan Haddock
2/09/05	Body Edited and Elaborated	Kelly Nelson/Bryan Haddock
2/11/05	Body Edited	Kelly Nelson/Ray Clayton
2/15/05	Body Edited	Kelly Nelson
3/14/05	Body Edited	Kelly Nelson
3/15/05	Body Edited	Kelly Nelson/Ray Clayton/Eli Mendoza
7/26/05	Body Edited	Kelly Nelson/Ray Clayton
9/26/05	Body Edited	Kelly Nelson/Ray Clayton
9/29/05	Body Edited in response to comments by Atlan Labs	Kelly Nelson/Ray Clayton
3/10/06	Body Edited in response to CMVP comments (updated name)	Ray Clayton
3/27/06	Body Edited in response to CMVP comments	Ray Clayton