Arcot Core Security Module 2.0
Security Policy

September 25, 2008

Arcot Systems, Inc.
455 West Maude Ave.
Sunnyvale, CA 94085

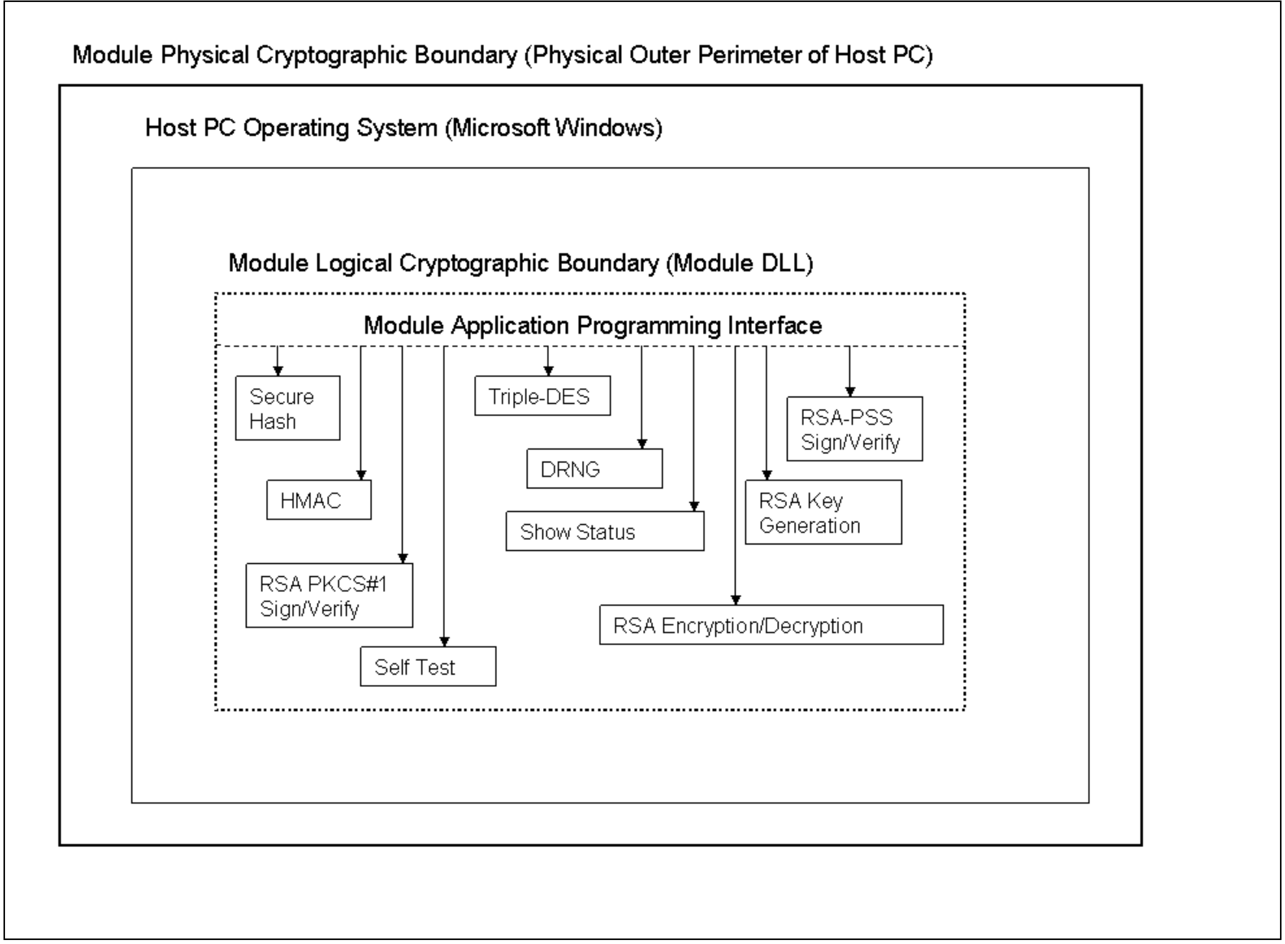
1. OVERVIEW OF MODULE

The Arcot Core Security Module is a software cryptographic module that is implemented as a software library. This software library provides cryptographic services to all Arcot Systems' products. The module provides FIPS-Approved cryptographic services for encryption, decryption, digital signing, verification of digital signatures, key generation, secure hashing, HMAC message authentication codes, and random number generation. This document describes version 2.0 of the Arcot Core Security Module.

The Arcot Core Security Module is classified as a multi-chip standalone module for FIPS 140-2 purposes. The physical cryptographic boundary is the outer perimeter of the host PC which is running an operating system as well as external components such as a keyboard, mouse, monitor, floppy drive, CD-ROM drive, DVD-ROM drive, speaker, serial ports, parallel ports, USB ports, and power plug. The logical cryptographic boundary consists of the module's dynamically-loadable library file which provides cryptographic services through a C-language API (Application Programming Interface.) The roles and services provided by the API are described later in this document.

Below is a diagram of the Arcot Core Security Module:

Diagram of Arcot Core Security Module


Module Physical Cryptographic Boundary (Physical Outer Perimeter of Host PC)
Host PC Operating System (Microsoft Windows)
Module Logical Cryptographic Boundary (Module DLL)
Module Application Programming Interface
Secure Hash
HMAC
RSA PKCS#1 Sign/Verify
Self Test
Triple-DES
DRNG
Show Status
RSA-PSS Sign/Verify
RSA Key Generation
RSA Encryption/Decryption

The module supports the following operating system versions:

- Windows XP Professional SP2
- Windows Server 2003 SP1

As per FIPS 140-2 Implementation Guidance, the cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any general purpose computer (GPC) provided that the GPC uses the specified single user operating system/mode specified on the validation certificate (i.e. an operating system specified above), or another compatible single user operating system including (but not limited to) the following:

- Windows Vista 32-bit
- Windows Vista 32-bit, SP1
- Windows Vista 64-bit
- Windows Vista 64-bit, SP1
- Windows 2003, SP2
- Windows XP, SP2

The module meets the requirements applicable to Level 1 security of FIPS 140-2:

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

2. MODES OF OPERATION

Configuration of mode of operation

The module may be configured for FIPS mode using a “mode of operation” software configuration setting. A user of the library can obtain the mode of operation using a “Show Status” library function.

Before installation, the operating system shall be configured in the single user mode of operation.

To install and configure the module in FIPS mode, the user must follow the following steps:

- Install the module DLL and configuration file onto the operating system of the host PC.
  a. Copy the file “ArcotCM.dll” to the following directory on the system drive on the host PC: “\WINDOWS\system32”.

b. On the system drive of the host PC, create the following directory: "\Program Files\Common Files\Arcot Shared\Conf".

c. Copy the file "fips.ini" to the following directory on the system drive on the host PC: "\Program Files\Common Files\Arcot Shared\Conf".

d. Double-click the file "Arcotregistry.reg". This adds registry settings which store the location of the directory where the above "fips.ini" file is stored.

e. If the name of the system drive of the host PC is not "C:", then you will need to use the "regedit" utility to change the registry setting to point to the correct location of the "fips.ini" file. You will need to edit the following registry settings to point to the correct location of the "fips.ini" file and its parent directory:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Arcot Systems\General]

        "ConfigDir"="C:\Program Files\Common Files\Arcot
        Shared\conf"

        "ArcotCommonHome"="C:\Program Files\Common Files\Arcot
        Shared"
```

- Edit the module configuration file, "fips.ini" and ensure it contains the setting "enabled=1". This ensures that the module is configured for the FIPS Approved mode of operation.

FIPS Approved mode of operation

In FIPS mode, the module supports the following FIPS Approved cryptographic algorithms:

Algorithm	**Certificate Number**
Triple-DES: ECB, CBC, OFB (64-bit), CFB (64-bit).	499
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	558
RSA PKCS#1 (sign/verify): Modulus sizes: 1024, 2048, 4096. SHS: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.	201
RSA-PSS (sign/verify). Modulus sizes: 1024, 2048, 4096. SHS: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.	201
HMAC. SHS: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.	242
ANSI X9.31 Pseudo-Random Number Generation (PRNG).	268

In FIPS mode, the module also supports the following non-FIPS Approved cryptographic algorithms:

- RSA encryption and decryption (for key wrapping). The module allows these algorithms in FIPS mode because they meet all requirements described in "Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2."
- RSA PKCS#1 key generation (Modulus sizes: 1024, 2048, 4096).

Non-FIPS Approved mode of operation

In non-FIPS mode, the cryptographic module also provides non-FIPS Approved hash algorithms as follows:

- MD5
- MD4
- MD2
- RIPEMD-160

The above hash algorithms will only execute when the module is in non-FIPS mode, and only when they are used as the hash algorithm for RSA signing and RSA verification operations.

3. Ports and Interfaces

The module provides a logical interface to software applications running on the PC operating system. This logical interface is a C-language Application Programming Interface (API) that is mapped to the FIPS 140-2 logical interfaces: data input, data output, control input, and status output. The API is mapped to FIPS logical interfaces as follows:

FIPS 140-2 Logical Interface	**Mapping to Module API**
Data Input Interface	Data passed into the module during API function calls.
Data Output Interface	Data returned by the module as a result of API function calls.
Control Input Interface	The invocation of an individual API function is itself a control input. In addition, control input is specified through the control arguments of individual API functions.
Status Output Interface	Status information returned by the API which provides details about what functions were

	performed by the API as well as any error information.

4. Identification and Authentication Policy

For FIPS 140-2 Level 1, a module is not required to utilize authentication mechanisms to control access to the module. The Arcot Core Security Module does not support authentication mechanisms to access the module. Instead the module relies on the security of the underlying operating system to control the ability of applications to access the module.

5. Roles and Services

The module supports two roles: "User" and "Cryptographic Officer." The module allows any user of the module to act as both roles. This is acceptable to meet the requirements of FIPS 140-2 Level 1.

The below table describes which services are a part of the "User" role and which services are a part of the "Cryptographic Officer" role:

Service	**Description**	**Role**	**Allowed in FIPS mode**
Secure Hash	Provides secure hash functionality using SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.	User	Yes
Non-approved Hash	Provides hash functionality using the following non-FIPS Approved hash functions: MD5, MD4, MD2, RIPEMD-160.	User	No. Does not execute if module is in FIPS mode.
HMAC	Provides message authentication code functionality using HMAC SHA using the following SHA variations: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.	User	Yes
Triple-DES	Provides encryption and decryption functionality using Triple-DES with ECB, CBC, OFB, and CFB modes.	User	Yes
RSA PKCS#1 signing and verification	Provides signing and verification functionality using RSA PKCS#1.	User	Yes

Service	**Description**	**Role**	**Allowed in FIPS mode**
RSA PSS signing and verification	Provides signing and verification functionality using RSA PSS.	User	Yes
RSA PKCS#1 key generation	Provides RSA key generation compliant with PKCS#1.	User	Yes
RSA encryption and decryption	Provides RSA encryption and decryption for key wrapping. Modulus sizes: 1024 , 1536 , 2048, 3072 , 4096.	User	Yes. (Only for key wrapping and key establishment.)
PRNG	Provides ANSI X9.31 Pseudo-Random Number Generation using the TDES-2Key core algorithm.	User	Yes
Show Status	Shows the module's status information.	Cryptographic Officer	Yes
Self Test	Instructs the module to perform self-tests.	Cryptographic Officer	Yes

6. CRYPTOGRAPHIC KEYS AND CSP'S

The Arcot Core Security Module does not provide long-term storage of cryptographic keys. If the user chooses to store keys, the user is responsible for storing keys returned by the module.

Keys and Critical Security Parameters (CSP) are stored only in short-term volatile memory. All key and CSP data resides in internal module data structures and can only be retrieved using the module's defined API functions.

The module relies on the security of the operating system to prevent the module's memory from being directly accessed by unauthorized users. The user of the module should follow the steps outlined in the documentation to ensure sensitive data is protected by zeroizing the data from memory when it is no longer needed.

The keys and CSP's used by the module are listed below. For each service, the keys and CSP's are indicated along with type of access. "R" signifies that the key or CSP is read or referenced by the module. "W" signifies that the key or CSP is written or updated by the module.

Keys and CSP's used by Arcot Core Security Module:

Service	**Name of Key or CSP**	**Access Control. (R: Read, W: Write)**
Secure Hash	N/A	
Non-approved Hash	N/A	
HMAC	HMAC key	R
Triple-DES	Triple-DES encryption key	R
RSA PKCS#1 signing and verification	RSA PKCS#1 signing key	R
	RSA PKCS#1 verification key	R
RSA PSS signing and verification	RSA PSS signing key	R
	RSA PKCS#1 verification key	R
RSA Key Pair Generation	RSA private key	W
	RSA public key	W
RSA Encryption and Decryption	RSA private encryption key	R
	RSA public decryption key	R
PRNG	Random number seed CSP	R, W
Show Status	N/A	
Self Test	N/A	

Note: RSA key pairs generated by the module may be used for RSA encrypt/decrypt and also RSA sign/verify, including both PKCS#1 and PSS signatures.

7. Operational Environment

The software module is stored on disk in compiled binary form. The module relies on the access controls of the underlying operating system to prevent against unauthorized tampering with the module and control which users and applications can access the module.

8. SELF TESTS

The Arcot Core Security Module performs two types of self tests: power-up self tests and conditional self-tests. If a self-test fails, the module returns an error and prevents any further cryptographic operations.

Self Test Type	Self Test Category	Test Description
Power-up	Known Answer Test	Triple-DES encryption and decryption
Power-up	Known Answer Test	Secure Hashing test using SHA-256 and SHA-512.
Power-up	Known Answer Test	ANSI X9.31 PRNG
Power-up	Pair-wise consistency test	RSA-PKCS#1 sign and verify
Power-up	Pair-wise consistency test	RSA-PSS sign and verify
Power-up	Module integrity test	Verify integrity of module software using HMAC-SHA1 with a 256 byte key.
Conditional	Key Generation	Pair-wise consistency tests: RSA-PKCS#1 Signing/Verification using RSA key pair. RSA-PSS Signing/Verification using RSA key pair. Encryption/Decryption using RSA key pair.
Conditional	PRNG	Continuous Random number generation test.

9. PHYSICAL SECURITY POLICY

Not applicable since it is a software module.

10. MITIGATION OF OTHER ATTACKS POLICY

Not applicable since the module does not implement mitigation against any other attacks.

11. Definitions and Acronyms

ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining encryption mode.
CD-ROM	Compact Disc Read-Only-Memory
CFB	Cipher Feedback encryption mode.
ECB	Electronic Code Book encryption mode
FIPS	Federal Information Processing Standards
HMAC	Keyed-Hash Message Authentication Code
MD2	MD2 message digest algorithm
MD4	MD4 message digest algorithm
MD5	MD5 message digest algorithm
OFB	Output Feedback encryption mode
PC	Personal Computer
PKCS	Public Key Cryptography Standards
PRNG	Pseudo-Random Number Generator
PSS	Probabilistic Signature Scheme
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	RSA public key cryptography algorithm
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
TDES-2Key	Two-Key Triple Data Encryption Standard
Triple-DES	Triple Data Encryption Standard
USB	Universal Serial Bus