STANLEY
Security Solutions

Stanley Wi-Q Communication Server Cryptographic Module FIPS 140-2 Security Policy

Prepared for:
UL/CMVP

Prepared by:
Engineering

This document is non-proprietary

Document Number: 99093
Revision: 7
Release Date: 09/30/2013

Revision History

Version	Release Date	Description of Change
1	05/07/2012	Initial Release
2	05/24/2012	Added Windows Server 2008 to tables 2 & 3. Added Table 6 Access Rights. Added CSCM software version to Introduction section.
3	06/19/2012	Modified Roles section. Modified Service Inputs and Outputs table 5. Modified Cryptographic Keys and Critical Security Parameters section.
4	06/22/2012	Modified Physical Security section.
5	02/26/2013	Modified Physical Security section. Modified Services section and Service Inputs and Outputs table 5. Modified Power-Up Tests section. Removed Conditional Tests section. Removed Critical Function Tests section.
6	04/18/2013	Modified Module and Algorithms References table 2 and references to certification numbers. Modified FIPS 140-2 Configurations table 3. Added SHA-1 KAT to power up self tests section.
7	09/30/2013	Removed references to non-approved algorithms. Updated Table 2 Split Table 3 in to 3a and 3b.

Table of Contents

Section **Page**

1 Introduction 1
2 Cryptographic Module Specification 1
2.1 Description of Approved Mode 1
2.2 Supported Algorithms 2
2.3 Description of Cryptographic Boundary 3
2.4 Block Diagram 4
3 Cryptographic Module Ports and Interfaces 5
4 Roles and Services 6
4.1 Roles 6
4.2 Services 6
4.3 Service Inputs and Outputs 6
5 Cryptographic Keys and Critical Security Parameters 7
5.1 AES Keypad & Credential Key 7
5.2 SSL Certificates 7
6 Physical Security 8
6.1 Power-Up Tests 8
7 Mitigation of Other Attacks 8

1 Introduction

This document defines the security policies of the Stanley Wi-Q Communications Server Cryptographic Module, referred to as the CSCM for simplicity.

FIPS140-2 Stanley WiQ Communication Server software version tested: 3.0.27

2 Cryptographic Module Specification

The CSCM is a software solution that provides secure key retrieval and key transfer functions within the Stanley Wi-Q Wireless Access Control System.

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

Table 1. Module Security Levels

2.1 Description of Approved Mode

Prior to operation, RSAENH.dll (Microsoft Windows) must be put into the approved mode of operation. In order to ensure that RSAENH.dll is running in the approved mode, follow the instructions provided in the Security Policies for the respective Windows Operating Systems. The CMVP certificate numbers can be found in tables 3a and 3b.

Once RSAENH.dll is running in the approved mode of operation, the CSCM must be configured to run in Approved mode only, by means of a configuration application “WiQAdminApp.exe”. The module does not support switching to any Non-Approved modes once in operation. Once the module has been configured to run in Approved mode, it is placed into operation by starting the CSCM service. Once the service successfully completes its power-on self-tests, it is considered operational and running in Approved mode. Approved mode is indicated by the following status messages within the system:

Log File Indicator – “FIPS 140 Mode is True” log file audit
Non-FIPS FIPS configuration application “WiQConfigurator.exe” – “(FIPS140)” title bar

2.2 Supported Algorithms

The following algorithms are supported by the CSCM. The algorithms are provided by the RSAENH.DLL validated to FIPS 140-2 under the certificates below.

CMVP Module Description	**Operating system / CMVP Cert. Number**	**Approved Algorithms / CAVP Cert. Number**	**Other Algorithms**

RSAENH.DLL Microsoft Enhanced Cryptographic Provider	Windows Server 2008
	Cert. #1010
		AES (Cert. #739);
		DRBG (vendor affirmed);
		HMAC (Cert. #408);
		RSA (Certs. #353 and #355);
		SHS (Cert. #753);
		Triple-DES (Cert. #656)
			RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength; non-compliant less than 80 bits of encryption strength)

Table 2. FIPS 140-2 Module and Algorithm References

2.3 Description of Cryptographic Boundary

The Stanley CSCM is a software only product, but for the purposes of the FIPS 140-2 validation, it is considered a multiple-chip standalone module. The logical cryptographic boundary is defined by the executable application file (WiQCommSvc.exe), the supporting libraries (WiQCommCore.dll, WiQPortal.dll, & WiQPortalServiceClient.dll), and Microsoft Enhanced Cryptographic Provider (RSAENH.dll). RSAENH.dll is a previously validated FIPS 140-2 module (Certs. #989, #1002, #1010, #1012, #1330, and #1337). The physical embodiment is the general purpose computer or hardware appliance on which the CSCM operates. The physical cryptographic boundary contains the general purpose computing hardware of the system executing the application. This system hardware includes the central processing unit(s), cache and main memory (RAM), system bus, and peripherals including disk drives and other permanent mass storage devices, network interface cards, keyboard, and any terminal devices.

The module was tested and found to be compliant with the FIPS 140-2 requirements on the following platforms:

Operating Environment	**Communication Server**	**RSAENH.DLL**
Windows Server 2008, SP2**	Software Version 3.0.27	Reference CMVP Cert. #1010**

Table 3a. FIPS 140-2 Tested Configurations

** CMVP Certificate #1010 was tested on version Windows Server 2008 (which is Windows Server 2008 SP 1 at release date), while the Stanley Communication Server Cryptographic Module was tested on Windows Server 2008 SP2. The testing laboratory affirms that the differences between the two service packs do not interfere with the correct operation of the module.

Stanley Security Solutions affirms that the module also executes (as described in this security policy) on the following operating systems:

Operating Environment	**Communication Server**	**RSAENH.DLL**
Windows XP Professional, SP3	Software Version 3.0.27	Reference CMVP Cert. #989
Windows Vista (Ultimate), SP1		Reference CMVP Cert. #1002
Windows Server 2003, SP2		Reference CMVP Cert. #1012
Windows 7 Ultimate Edition		Reference CMVP Cert. #1330
Windows Server 2008 (R2)		Reference CMVP Cert. #1337

Table 3b. FIPS 140-2 Vendor Affirmed Configurations

The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported and executed in an operational environment not listed on the validation certificate.

2.4 Block Diagram

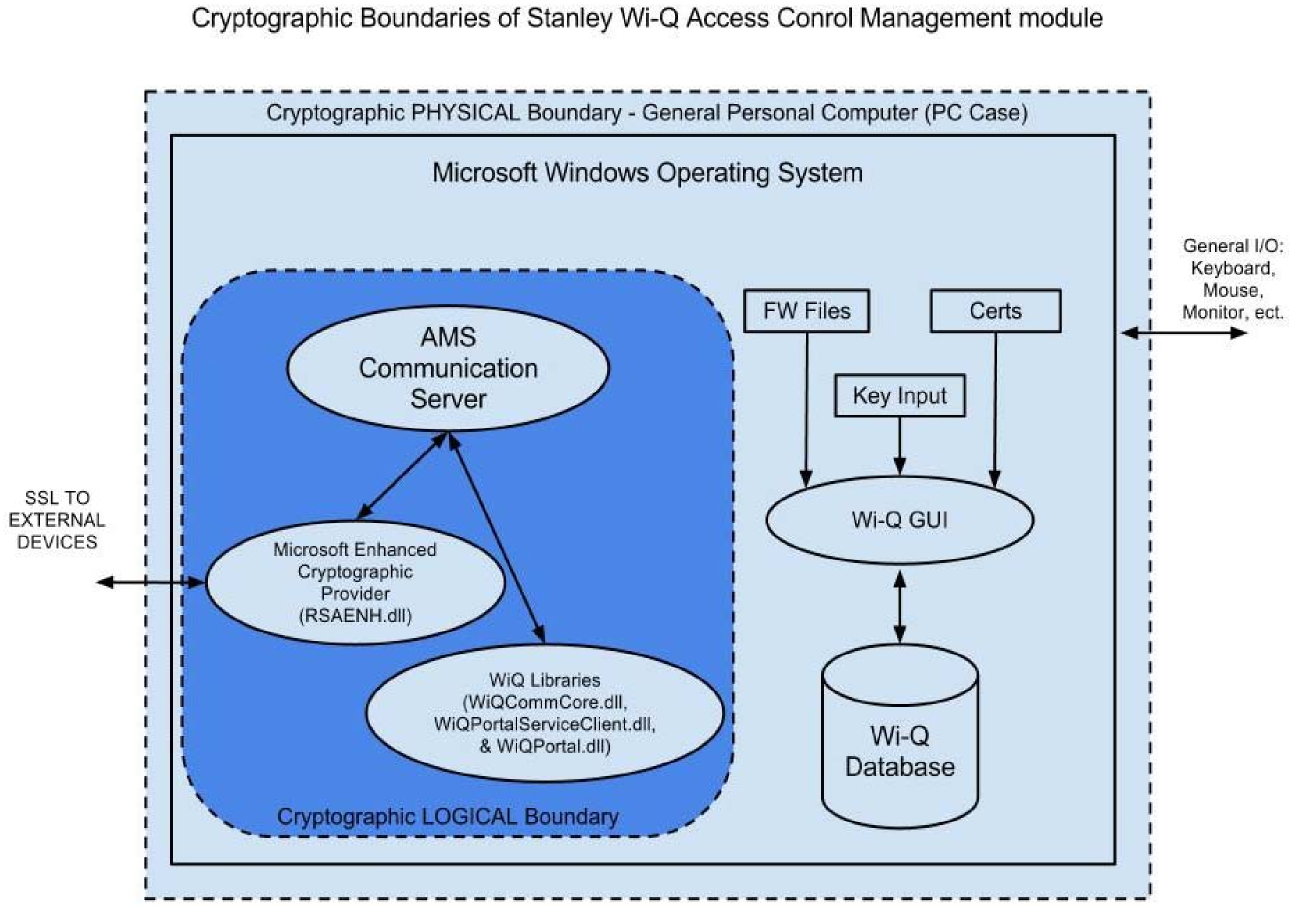
Cryptographic Boundaries of Stanley Wi-Q Access Conrol Management module
Cryptographic PHYSICAL Boundary - General Personal Computer (PC Case)
Microsoft Windows Operating System
AMS Communication Server
Microsoft Enhanced Cryptographic Provider (RSAENH.dll)
WiQ Libraries (WiQCommCore.dll, WiQPortalServiceClient.dll, & WiQPortal.dll)
Cryptographic LOGICAL Boundary
FW Files
Certs
Key Input
Wi-Q GUI
Wi-Q Database
SSL TO EXTERNAL DEVICES
General I/O: Keyboard, Mouse, Monitor, ect.

Figure 1. Block Diagram

3 Cryptographic Module Ports and Interfaces

The CSCM provides the following ports and interfaces:

CSCM Module		
Ports and Interfaces		
Interface	**Logical**	**Physical**
Data Input		
	Data read from Access Control database	GPC Disk
	Data received via Secure TCP from an external AMS Portal Gateway (PG)	Ethernet Port
	Data read from a configuration file	GPC Disk
Data Output		
	Data written to Access Control Database	GPC Disk
	Data sent via Secure TCP to an external AMS Portal Gateway (PG)	Ethernet Port
Control Input		
	Data read from Access Control database	GPC Hard Disk
	Data received via Secure TCP from an external AMS Portal Gateway (PG)	Ethernet Port
	Data read from a configuration file	GPC Hard Disk
Status Output		
	Log Files	GPC Hard Disk
	Data written to Access Control Database	GPC Hard Disk
Power Input	NA	PC Power Supply

Table 4. Ports and Interfaces

4 Roles and Services

4.1 Roles

The CSCM supports two distinct roles: Cryptographic Officer (CO) and User. The CO is the individual(s) responsible for creating and managing cryptographic keys through the key life cycle, while the User is the individual(s) who retrieves data encryption keys and uses them for secure communications. Assumption of roles is defined by selection of services in a Level 1 device. Roles are assumed by the selection of the services.

4.2 Services

- SSL session key negotiation - Negotiate secure SSL communications with Portal Gateway
- Secure data transmission – WCF SSL method calls with Portal Gateway
- Show status - Log file indicating approved mode status
- Self-test – SHA-1 Software integrity and SHA-1 KAT tests executed at startup.
- Database interaction - SQL calls to interact with the database

4.3 Service Inputs and Outputs

The CSCM roles are assumed by the selection of the following services:

Service	user	CO	data input	data output	status output
SSL session key negotiation		x	none	none	pass/fail
secure data transmission encryption	x		none	SSL encrypted	pass/fail
secure data transmission decryption	x		SSL encrypted	none	pass/fail
show status	x		none	none	plaintext
self-tests	x		none	none	pass/fail
database interaction	x		encrypted	encrypted	plaintext

Table 5. Service Inputs and Outputs

5 Cryptographic Keys and Critical Security Parameters

The CSCM provides secure management of the following CSPs:

Segment Keypad Key (AES Encrypted session key)
Segment Credential Key (AES Encrypted session key)
SSL Certificate (AES Encrypted SSL information)
SHA1 Software Integrity HASH (AES Encrypted)
AES HardCoded Key

CSP	CO Role - Access Rights	User Role - Access Rights
Segment Keypad Key	read only	read only
Segment Credential Key	read only	read only
SSL Certificate	read only	read only
SHA1 Software Integrity HASH	read only	read only
AES HardCoded Key	read only	read only

Table 6. Access Rights

5.1 AES Keypad & Credential Key

These keys (Segment Sign-On keys) are input and AES encrypted using a (non-FIPS) configuration application. The CSCM retrieves AES encrypted session keys, AES decrypts, and wraps in SSL tunnel to deliver to the external Portal Gateway devices for use in the secure wireless communication.

5.2 SSL Certificates

The certificates are generated using a (non-FIPS) configuration application. The CSCM retrieves AES encrypted certificates, AES decrypts, and uses the certificates to negotiate secure SSL communications.

6 Physical Security

The CSCM is a software only module and as such, the physical security is accomplished by installation of the software on a GPC. The GPC physical security is accomplished by production grade components.
Self – Tests

6.1 Power-Up Tests

Upon user assumption of role or manual re-start the CSCM performs known-answer tests for the following cryptographic functions:

- SHA-1 Software Integrity Test
- SHA-1 KAT

Upon successful completion of the power-up self-tests; the following is output to the log file:
"FIPS 140 Mode is True"

If power-up self-tests do not complete successfully, the following is output to the log file:
"Self Test Failed. Stopping Service". Then the module will exit.

In addition to the self-tests described above, the RSAENH.dll cryptographic module performs its own self-tests as described in the security policies associated with the RSAENH.dll Module (reference Tables 3a and 3b).

7 Mitigation of Other Attacks

The CSCM does not mitigate any attacks beyond the scope of FIPS 140-2