STANLEY
Security Solutions

Stanley Wi-Q
OMW (OW2000), WAC (SDC2K), WDC, and WXC Controller Cryptographic Modules
FIPS 140-2 Security Policy

Prepared for:
UL/CMVP

Prepared by:
Engineering

This document is non-proprietary

Document Number: 99091
Document Revision: 7
Release Date: 1/24/2013

Document Revision History

Revision	Release Date	Description of Change
1	05/07/2012	Initial Release
2	05/09/2012	Modified Table 3. Ports and Interfaces. Added Controller firmware version to Introduction section.
3	06/07/2012	Modified Table 4. Service Inputs and Outputs.
4	12/20/2012	Added table 1. Hardware versions tested Removed logical boundary from Figure 1. Block diagram Added figure 2. Physical boundary configuration pictures
5	01/15/2013	Modified Description of Approved Mode section to describe Approved vs. Non-Approved mode. Modified Roles and Services section to define Non-Approved mode services. Modified Conditional Tests section to describe the firmware load test.
6	01/23/2013	Modified Role Authentication to indicate that it is not supported. Removed firmware load test as it is not applicable when only one version of firmware is approved with the initial release.
7	01/24/2013	Added WDC hardware revision 82069F for component obsolescence. Added WXC hardware revision 82376G for component obsolescence.

Table of Contents

1 Introduction

This document defines the security policies of the Stanley Wi-Q Controller Cryptographic Module, referred to as the Controller for simplicity. The Controller is a wireless end point device that communicates via proprietary 802.15.4 protocol to a Portal Gateway module.

FIPS140-2 Stanley WiQ Controller firmware version tested: 3.00.039

Controller Configuration	Hardware versions
OMW (OW2000)	12681B
WAC (SDC2K)	82065A
WDC	82069B 82069C 82069E 82069F
WXC	82376C 82376D 82376F 82376G

Table 1. FIPS 140-2 Stanley WiQ Controller hardware versions tested

2 Cryptographic Module Specification

The Controller is a hardware device that provides secure key entry and data encryption 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 and Services	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Table 2. Module Security Levels

2.1 Description of Approved Mode

The Controller may be run in either Approved Mode of FIPS operation or Non-Approved Mode. This selection is done the first time the controller is received from the factory. A special sequence entered on the keypad, followed by a manually distributed key determines which mode the controller will operate in. Once the sequence is entered, along with the key, the module will reset itself, perform all required power-on self-tests, and begin running in FIPS Mode. Once the module has successfully completed its power-on self-tests, it is in the Approved mode, which is indicated by the following status messages within the system:

Wi-Q Transactions Application – An audit event (Transaction) indicates the Controller is now in FIPS mode.
Wi-Q Controller – A light and sound sequence unique to FIPS mode will be executed.

The controller cannot be placed into a Non-Approved Mode once in Approved Mode without being zeroized back to factory default first. The non-approved mode can be invoked by performing a deep-reset which zeroizes all CSPs and causes the module to revert back to the factory mode at which point the sign-on sequence for the non-approved can be initiated.

2.2 Invoking Non-Approved Mode

Once firmware version 3.00.039 has been loaded onto the module, the following methods are used to invoke the non-approved mode:

- Controllers with keypads follow this sequence
  - sign in by entering 5678#
  - Enter the 6 digit sign on key followed by '#' (OMW and WAC omit the '#')
- Controllers with magnetic card or proximity card reader connections follow this sequence
  - Swipe temp card
  - Wait for the controller to relock (or the red light)
  - Swipe sign-on credential card
- The red and green LEDs will begin to alternate flashes and if the non-approved mode signon is successful you will see 3 green-red flashes.

2.3 Invoking Approved Mode

Once firmware version 3.00.039 has been loaded onto the module, the following methods are used to invoke the approved mode using the manually distributed keys (Segment Sign-On keys).

- Controllers with keypads follow this sequence
  - sign in by entering 1357#
  - Enter the 6 digit sign on key 2 times followed by '#' (OMW and WAC omit the '#')
- Controllers with magnetic card or proximity card reader connections follow this sequence
  - Swipe temp card
  - Wait for the controller to relock (or the red light)
  - Swipe temp card
  - Wait for the controller to relock (or the red light)
  - Swipe sign-on credential card and you will see 3 green flashes
  - Swipe sign on credential card again and you will see 5 green flashes
- The red and green LEDs will begin to alternate flashes and if the FIPS140 signon is successful you will see 5 green flashes.

2.4 Supported Algorithms

The following approved algorithms are supported by the Controller in the approved mode of operation:

- AES - Stanley Wi-Q Advanced Encryption (AES Cert. # 1802)
- SHA256 – Stanley Wi-Q Advanced Encryption (SHS Cert. # 1583)

The following algorithms are supported by the Controller in the non-approved mode of operation:

- CRC - Cyclic Redundancy Check Error-Detection Code for firmware integrity
- AES - Stanley Wi-Q Advanced Encryption (AES Cert. # 1802)

2.5 Description of Cryptographic Boundary

The Stanley Controller is considered a multiple-chip embedded module for the purposes of FIPS 140-2 validation. The Controller is an electronic hardware appliance typically mounted on a door or inside a metal cabinet, depending on version. The cryptographic boundary of the module includes all software and hardware where the physical embodiment is the outer perimeter of the circuit board, protected by the enclosure of the controller. The hardware includes the radio central processing unit, Flash and Ram memory, radio boards.

2.6 Block Diagram

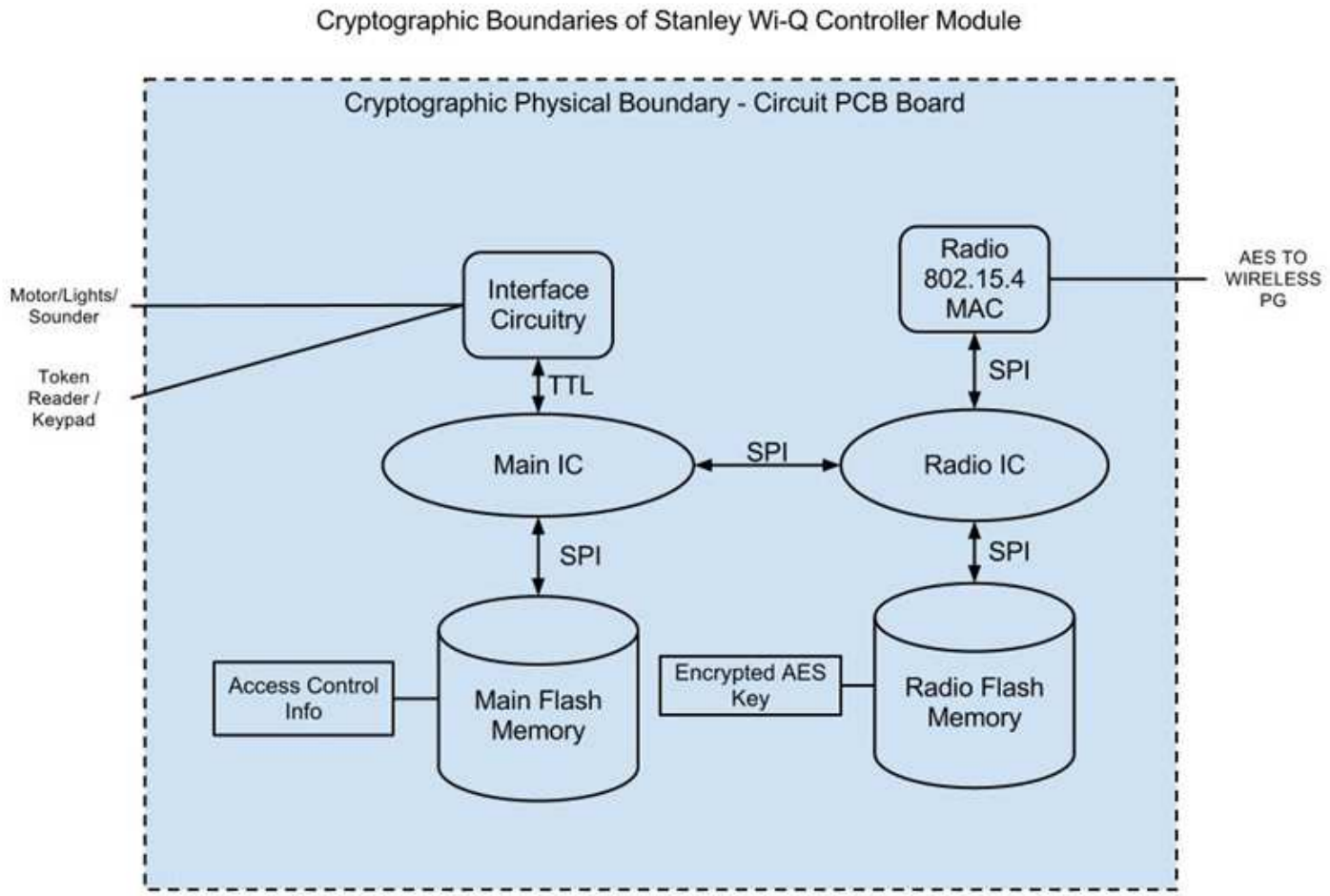

Figure 1. Block Diagram

2.7 Module Configurations

The Stanley Security Solutions, Inc. Wi-Q 3.0 Controller Cryptographic Module (Configurations WDC,WXC,WAC,OMW) is a Multi-Chip Embedded cryptographic module designed to provide user authentication and secure access control. The module under validation includes four configurations, which differ only in physical PCB board size and are logically identical.

- Configuration: WDC
- Configuration: WXC
- Configuration: SDC2K (WAC)
- Configuration: OW2000 (OMW)

WDC WXC WAC OMW

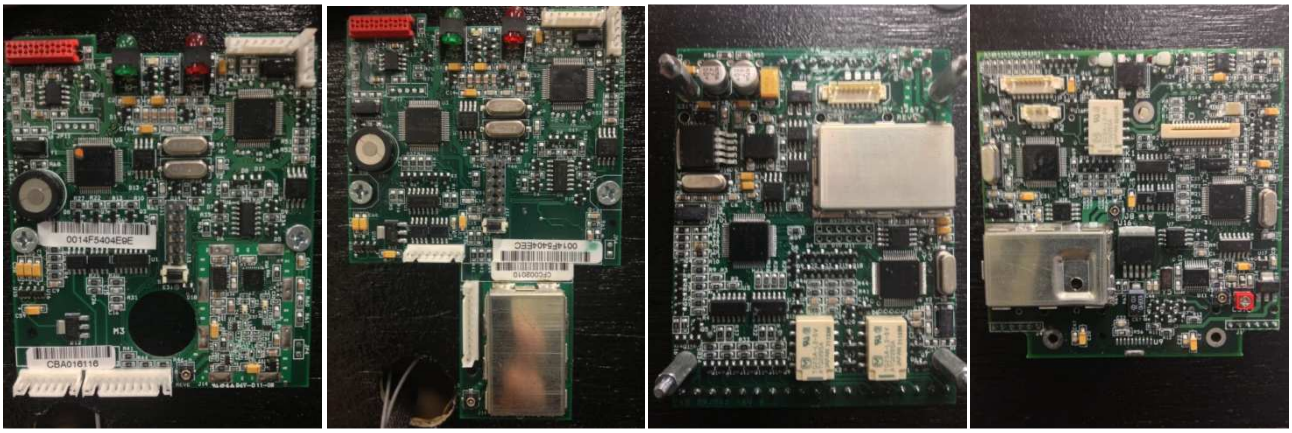

Figure 2. Cryptographic Physical Boundary, per configuration

3 Cryptographic Module Ports and Interfaces

The Controller provides the following ports and interfaces:

Interface	Logical	Physical
All Controllers		
Data Input	AES Encrypted data received from wireless Portal Gateway	Antenna connector
Control Input	AES Encrypted data received from wireless Portal Gateway	Antenna connector
Control Input	Zeroize	On-board reset Switch
Data Output	AES Encrypted data transmitted to wireless Portal Gateway	Antenna connector
Status Output	AES Encrypted transactional data transmitted to wireless Portal Gateway	Antenna connector
Power Input	NA	4AA batteries
WDC & WXC		
Data Input	Data received from keypad	Keypad connector
Data Input	Data received from magstripe reader	Magstripe reader connector
Data Input	Data received from proximity reader	Proximity reader connectors
Status Output	Visual status	On-board LEDs
Status Output	Audible status	On-board sounder
WAC		
Data Input	Data received from keypad / magstripe / proximity reader	Wiegand 0 & 1 connector
Status Output	Visual status	On-board LEDs / Off-board LED connector
Power Input	NA	power connector (9-24Vdc)
OMW		
Data Input	Data received from keypad	Keypad connector
Data Input	Data received from magstripe reader	Magstripe reader connector
Data Input	Data received from proximity reader	Proximity reader connector
Status Output	Visual status	Off-board LED connector

Table 3. Ports and Interfaces

4 Roles and Services

4.1 Roles

The controller supports two distinct roles: Cryptographic Officer (CO) and User. The CO is the individual(s) responsible for creating and managing firmware used by the controller, and managing cryptographic keys used by the controller. The User Role performs the general security services including cryptographic operations and other approved security functions.

4.1.1 Role Authentication

Role authentication is not supported by the cryptographic module.

4.1.2 Role Assumption

Assumption of roles is defined by selection of services in a Level 1 device. Roles are assumed by the selection of the services. The controller radio process only allows one Portal Gateway connection at a time. By doing that, there is always only one user at a time can use the cryptographic module.

4.2 Services

4.2.1 Services Performed in the Approved Mode of Operation

- Cryptographic key management - Encryption and decryption of critical security parameters
- Firmware management – Firmware SHA-256 validation and programming process
- Secure data transmission – AES encryption and decryption of data
- Show status – Transactions Application and LED flashing sequences
- Self-tests - KAT for AES, SHA-256, and software integrity tests executed at startup. Manual key entry test executed upon manual key entry.
- Zeroize - Clearing copies of critical security parameters

4.2.2 Services Performed in the non-Approved Mode of Operation

- Cryptographic key management - Encryption and decryption of critical security parameters
- Firmware management – Firmware CRC validation and programming process
- Secure data transmission – AES encryption and decryption of data
- Show status – Transactions Application and LED flashing sequences
- Self-Tests - CRC software integrity tests executed at startup.
- Zeroize - Clearing copies of critical security parameters

4.3 Service Inputs and Outputs

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

Service	user	CO	data input	data output	status output
segment key management		x	plaintext	none	pass/fail
firmware management		x	AES encrypted	none	pass/fail
show status	x		none	none	plaintext
self-tests	x		none	none	plaintext
zeroize	x		none	none	plaintext
Controller Radio Process					
wireless secure data transmission encryption	x		plaintext	AES encrypted	pass/fail
wireless secure data transmission decryption	x		AES encrypted	plaintext	pass/fail

Table 4. Service Inputs and Outputs

5 Cryptographic Keys and Critical Security Parameters

The controller radio process is the only process that can access the CSPs. The controller provides secure management of the following CSPs:

Controller AES Key (Hard coded AES key)
Controller Segment Keypad Key (AES Encrypted manually distributed session key)
Controller Segment Credential Key (AES Encrypted manually distributed session key)
Controller SHA256 Firmware Hash (Embedded Hash within AES Encrypted Firmware Files)

CSP	CO Role - Access Rights	User Role - Access Rights
Hardcoded AES Key	read only	read only
Segment Keypad Key	read, write, zeroize	read, zeroize
Segment Credential Key	read, write, zeroize	read, zeroize
SHA256 Firmware Hash	read, write	read only

Table 5. Access Rights

5.1 AES Keypad & Credential Key

These manually distributed keys (Segment Sign-On keys) are input using the token reader and/or keypad during the sign-on sequence of the controller. The key is stored AES encrypted. The controller module's radio IC retrieves this key and encrypts, with the manually distributed keys, all applicable communication packets with it. The key used to decode and validate any incoming wireless Portal Gateway communication for processing.

5.2 Firmware Files

Firmware loading to a firmware other than version 3.00.039 invalidates the cryptographic module.

5.3 Key Zeroization

The Controller may be zeroized via means of a deep reset switch mounted inside the module enclosure or via a command sent from the administrative console. Segment Sign-On keys in the module are held in serial flash memory and may be zeroized by a forced deep reset of the module.

6 Physical Security

As a level 1 device the Controller physical security is accomplished by production grade components.

7 Self – Tests

7.1 Power-Up Tests

On power up the controller module performs known-answer tests for the following cryptographic functions:

- AES KAT (encryption & decryption)
- SHA-256 KAT
- Firmware Integrity Test

Upon successful completion of the power-up self-tests; the following is output to the server via controller transactions: FIPS 140 CONNECTED

If power-up self-tests do not complete successfully, the module will flash the LED in a failure pattern and all further cryptographic functions will halt.

7.2 Conditional Tests

A repetitive entry manual key test is performed during the sign-on sequence to ensure accuracy of key entry. If this test fails a failure LED and sound sequence will indicate this and the controller will not attempt a portal connection. The controller will not remain in an error state and it will allow additional sign-on attempts.

7.3 Critical Functions Tests

No critical function tests occur in this module beyond the scope of startup self tests.

8 Mitigation of Other Attacks

The module was not designed to mitigate other attacks. Therefore, this section is not applicable.