STANLEY
Security Solutions

Stanley Wi-Q
Portal Gateway
Cryptographic Module
FIPS 140-2 Security Policy

Prepared for:
UL/CMVP

Prepared by:
Engineering

This document is non-proprietary

Document Number: 99092
Revision: 6
Release Date: 06/11/2013

Revision History

Version	Release Date	Description of Change
1	05/07/2012	Initial Release
2	05/24/2012	Added Table 4 Access Rights Added PG firmware version to Introduction section.
3	07/27/2012	Modifications to several sections following UL final review comments. Added OpenSSL Algorithm Cert #s
4	02/20/2013	Added hardware version tested. Removed logical boundary from Figure 1. Block diagram. Added figure 2. Physical boundary configuration pictures. Removed firmware load test as it is not applicable when only one version of firmware is approved with the initial release.
5	05/09/2013	Renamed supported algorithms. Modified self-test descriptions.
6	06/11/2013	Added additional information to CSPs Clarified KATs performed

Table of Contents

1 Introduction

This document defines the security policies of the Stanley Wi-Q Portal Gateway Cryptographic Module, referred to as the PG for simplicity. The PG is a wireless gateway device that communicates via wired network to the CSCM (Stanley Wi-Q Communications Server Cryptographic Module) and communicates via proprietary 802.15.4 protocol to a wireless access controller device.

FIPS140-2 Stanley WiQ Portal Gateway firmware version tested: 3.017.156
FIPS140-2 Stanley WiQ Portal Gateway hardware version tested: 12562C

2 Cryptographic Module Specification

The PG is a hardware device that provides secure key retrieval and key transfer functions within the Stanley Wi-Q Wireless Access Control System. The incoming commands / interrupts from the CSCM are handled in the same process, the PG communication process. The incoming commands / interrupts from the Controllers are handled in the same process, the PG radio process. Therefore, there is no other process can interrupt the cryptographic module during execution.

Security Component	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	1
Cryptographic Keys and Critical Security Parameters	1
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

The PG only runs in Approved Mode of FIPS operation when firmware version 3.017.156 is loaded on the module. The module will start in FIPS mode and complete its power-on self-tests. 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:

- PG Status Webpage –Portal Gateway firmware version 3.017.156 indicated.

2.2 Supported Algorithms

The following algorithms are supported by the PG

- AES - Stanley Wi-Q Advanced Encryption (AES Cert. # 1802)
- SHA256 – Stanley Wi-Q Advanced Encryption (SHS Cert. # 1583)
- SHA1, 224, 256, 384, 512 - Stanley Wi-Q Advanced Encryption (SSL-SHS) (SHS Cert. #1845)
- Triple-DES - Stanley Wi-Q Advanced Encryption (SSL-TDES) (TDES Cert. #1356)
- RSA - Stanley Wi-Q Advanced Encryption (SSL-RSA) (RSA Cert. #1096)

2.3 Description of Cryptographic Boundary

The Stanley PG is considered a multiple-chip embedded module for the purposes of FIPS 140-2 validation. The PG is an electronic hardware appliance. The cryptographic boundary of the module includes all software and hardware where the physical embodiment is the outer perimeter of the main circuit board, protected by the enclosure of the PG. The hardware includes the central processing unit, Flash and Ram memory, network interface circuits, excluding the radio boards.

2.4 Block Diagram

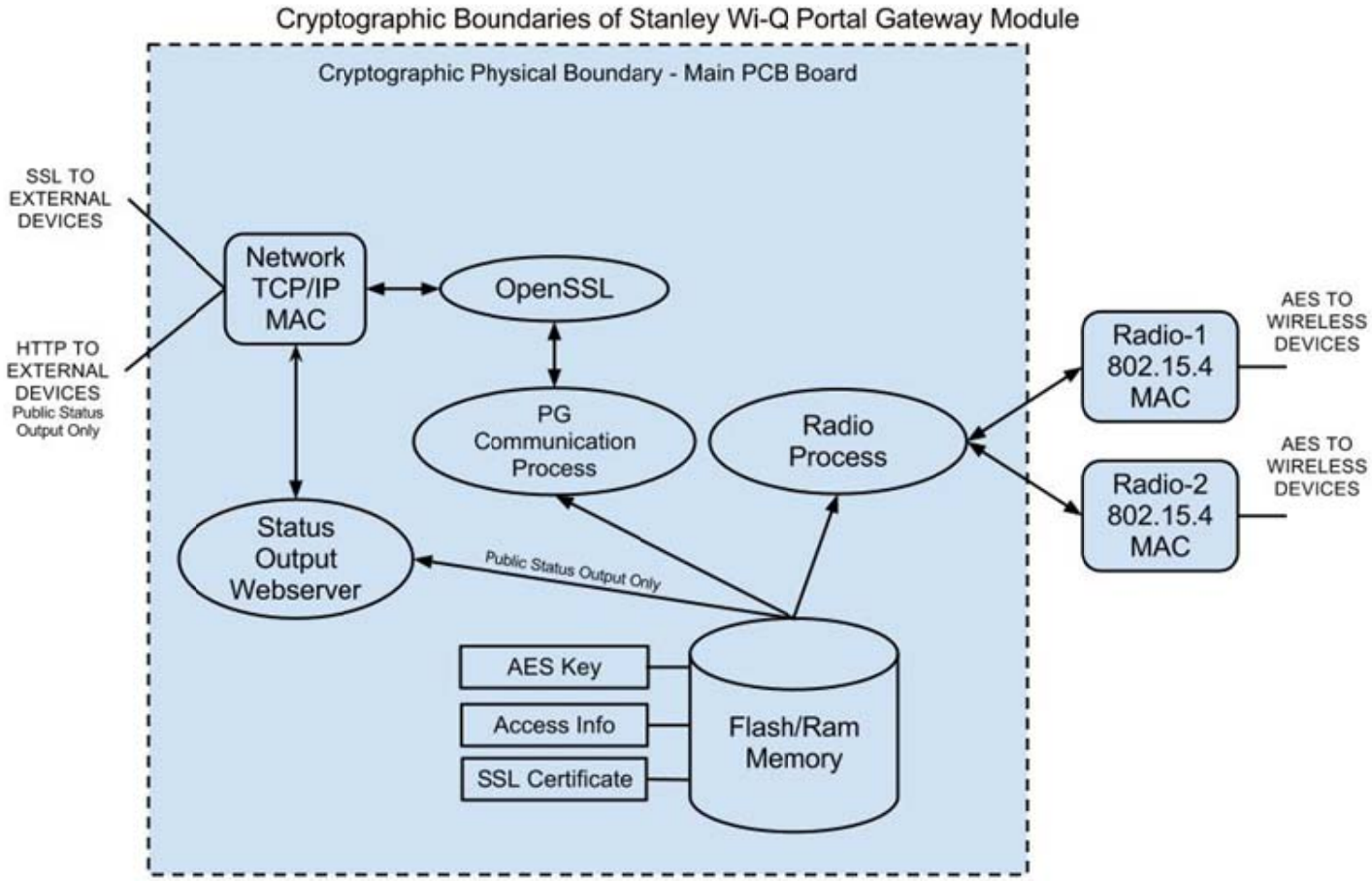

Figure 1. Block Diagram

2.5 Physical Boundary

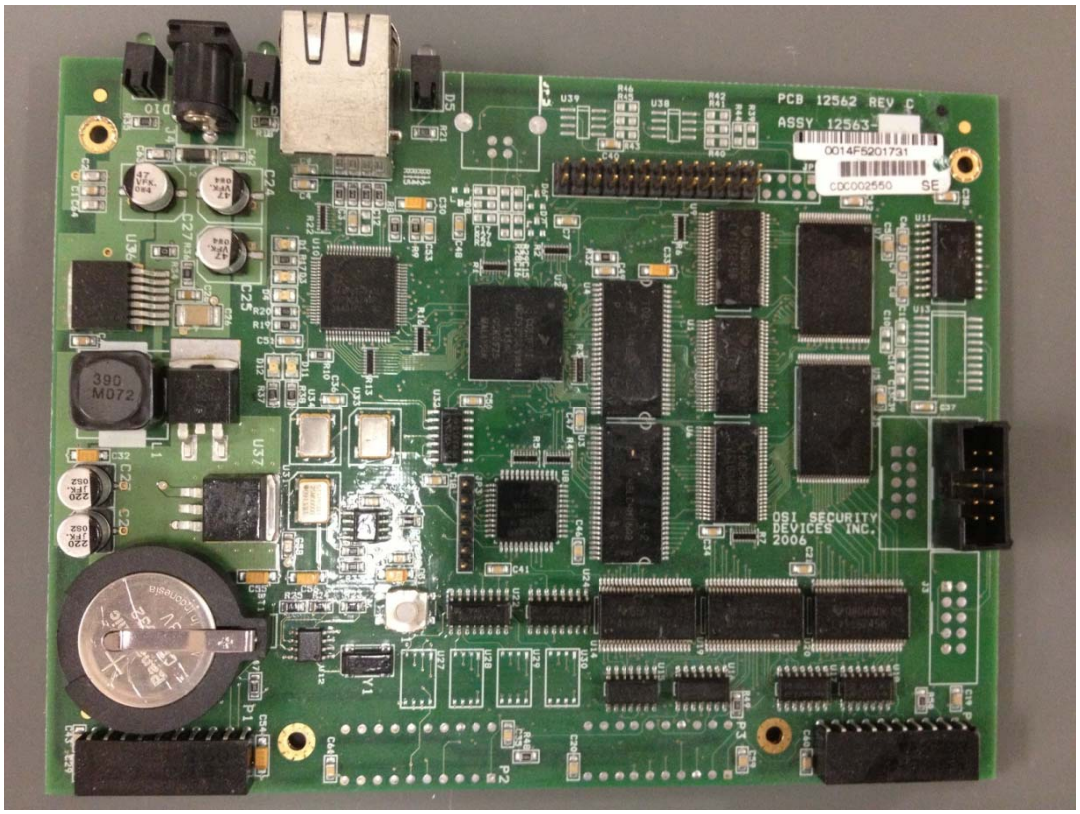

Figure 2. Cryptographic Physical Boundary

3 Cryptographic Module Ports and Interfaces

The PG provides the following ports and interfaces:

Portal Gateway Module		
PG Ports and Interfaces		
Interface	**Logical**	**Physical**
Data Input	Data received via Secure TCP from an external communication service (via Secure TCP/IP)	Ethernet Port
	Data received via Secure AES encrypted from external controller	RF Antenna Port (P1, P4)
Data Output	Data sent via Secure TCP to an external communication service (via Secure TCP/IP)	Ethernet Port
	Data transmitted to external controller via secure wireless protocol QSPI communication to MC1392	RF Antenna Port (P1, P4)
Control Input	Data received via Secure TCP from an external communication service (via Secure TCP/IP)	Ethernet Port
	Reset Signal	On Board Reset Switch
Status Output		
	Status data written to HTTP Status Page	Ethernet Port
	Data sent via secure TCP to external Communication Service	Ethernet Port
	Data sent via secure TCP to external Communication Service	Network LED Lights (D1,D2,D3,D4,D5)
	Power Applied Indicator	Power Indicator Light (D10)
	Proper operation indicator	Heartbeat LEDs (D11,D12)
Power Input	NA	Power Supply

Table 2. Ports and Interfaces

4 Roles and Services

The module runs in FIPS Mode only. Switching to a Non-Approved mode is not supported by the module.

4.1 Roles

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

Assumption of roles is accomplished by selection of services. Roles are implicitly assumed by the selection of the services. The PG communication process only allows one client PC connection at a time.

4.2 Services

- Cryptographic key management - Encryption and decryption and distribution of critical security parameters
- Firmware Management – Firmware SHA-256 validation and programming process.
- Secure data transmission – SSL and AES encryption and decryption and transmission of data
- Show status – PG webpage showing the current status of the PG and connected controllers and LED status output.
- Self-tests - KATs for AES, SHA-1, -224, -256, -384, -512, Triple-DES, and RSA, firmware integrity tests, and Pairwise Consistency Tests.
- Zeroize - Clearing copies of critical security parameters

4.3 Service Inputs and Outputs

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

Service	user	CO	data input	data output	status output
Cryptographic Key Management - SSL certificate management		x	AES encrypted	none	pass/fail
Cryptographic Key Management - segment key management		x	SSL encrypted	none	pass/fail
Firmware Management		x	AES encrypted	none	pass/fail
show status	x		none	none	module status
self-tests	x		none	none	pass/fail
zeroize	x		none	none	plaintext
PG Communication Process					
wired secure data transmission encryption/decryption	x		SSL encrypted	SSL encrypted	pass/fail
PG Radio Process					
wireless secure data transmission encryption/decryption	x		AES encrypted	AES encrypted	pass/fail

Table 3. Service Inputs and Outputs

5 Cryptographic Keys and Critical Security Parameters

The PG communication process is the only process that can access the CSPs, during run time. The PG provides secure management of the following CSPs:

- AES Key (Hard coded AES key used for storage and importing certificate), 128 bit AES key
- Segment Keypad Key (Session key used for wireless secure communication with controllers), 128 bit AES key
- Segment Credential Key (Session key used for wireless secure communication with controllers), 128 bit AES key
- SSL Certificate (AES Encrypted SSL information), 2048 bit public RSA key
- RSA Private Key (AES Encrypted keypair associated with SSL Certificate), 2048 bit private RSA key
- Triple-DES Session Key (Session key used by the PC connection for symmetric encryption), 168 bit Triple-DES key
- SHA256 Firmware Hash (Embedded Hash within Firmware Files), SHA-256 hash of firmware binary file

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
SSL Certificate	read, write, zeroize	read, zeroize
RSA Private Key	read, write, zeroize	read, zeroize
Triple-DES Session Key	read, write, zeroize	read, zeroize
SHA256 Firmware Hash	read, write	read only

Table 4. Access Rights

5.1 AES Keypad & Credential Key

The segment keypad key and segment credential key are sent to the portal gateway by the client PC via the established connection and are manually entered at the lock controller. Once these keys have been established in the portal gateway and controller, AES encrypted secure wireless communication can begin.

5.2 SSL Certificates

The certificates are generated outside of the module using OpenSSL Library version 1.2.3 implemented on a general purpose PC. The certificates are then transferred to the PG from the client PC encrypted with the AES hardcoded key. The PG module then AES decrypts, stores the certificate, and uses it for all SSL communication with the external client PC.

6 Physical Security

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

7 Self – Tests

7.1 Power-Up Tests

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

- AES encryption KAT and decryption KAT
- SHA-1, -224, -256, -384, -512 KATs
- Triple-DES encryption KAT and decryption KAT
- RSA encryption KAT and decryption KAT
- Firmware Integrity Test

Upon successful completion of the power-up self-tests the PG status webpage indicates firmware version 3.017.156.

If power-up self-tests do not complete successfully, the module will flash the power LED in a pattern indicating "S-O-S" in morse code ("…- - - … - - -") and all further cryptographic functions will halt.

7.2 Conditional Tests

The following conditional self-tests are conducted:

- RSA Pairwise Consistency Test

7.3 Firmware Files

Firmware loading to a firmware other than version 3.017.156 invalidates the cryptographic module.

7.4 Critical Functions Tests

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

7.5 Key Zeroization

Segment Sign-On keys in the module are held in RAM and may be zeroized by a forced reset of the module. This may also be done by disconnecting and connecting power. The PG will again retrieve Segment Sign-On keys upon successful power-up tests. The PG can also be returned to the factory default, therefore erasing SSL Certificates using the PortalConfig application.

8 Mitigation of Other Attacks

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