CR2700 and A271 Firmware Security FIPS 140-2 Integration Guide

Corporate Office
434 West Ascension Way Suite 300
Salt Lake City, UT 84123, USA
Phone: 801-495-2200 Fax: 801-495-2202
Salt Lake City | Boston | Amsterdam

Associated NIST Certifications:

- Validation Certificate:
https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3389
- Security Policies:
https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3389.pdf
- Algorithm Certificate:
https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13382

FIPS Interactions:

CR2700 and A271 FIPS devices are password-protected. They always transfer encrypted and protected data transparent to the user experience. Due to the rules governing FIPS 140-2 certification, these devices require a security role other than the normal day-to-day users to make changes relating to the security of these devices.

These devices operate in the same way as non-FIPS versions for normal usage out of the box. The added security is transparent to the user role for normal operations such as barcode scanning and device configurations. An officer role is required for any changes to the configuration of the system security provided by the FIPS 140-2 implementation.

FIPS Indications:

Several operations for making changes to the system security provided by FIPS 140-2 require a cryptographic officer, and some for users, to be logged into the devices. If an officer or user is not logged in for a service that is supported for their role, then these services that require login will not be available and issuing the commands will result in a FIPS error indication, which is independent of the error indication during normal scanning operations.

FIPS error indications consist of beeps, LED changes, and log entries. The FIPS error beep is one longer and higher pitched beep followed by three lower and shorter beeps

similar to normal error beeps on CR2700. Errors on the A271 are indicated by a series of fast blinks on the LED. Some errors will cause CR2700's red LED to light up and some will cause an entry to be put into its error log, or messages sent to host from A271.

FIPS Services and Commands:

FIPS commands allow the utilization of FIPS services for both cryptographic officers and system/device users. The main aspect of these commands are to give officer(s) and user(s) the ability to log into the FIPS interface and be able to run services that are otherwise unavailable or prohibited. For officers, these services include upgrading the firmware, resetting the officer password, renewing cryptographic keys, and running cipher tests. For users, the only service currently available is resetting password.

<table>
<tr><th>Services</th><th>Role</th><th>CR2700</th><th>A271</th><th>Examples</th></tr>
<tr><td rowspan="2">FIPS Device Interface Status</td><td>None</td><td>FWSEGFS</td><td>BTSEGFS</td><td>FWSEGFS
BTSEGFS</td></tr>
<tr><td colspan="4">Description: Returns the current status code for the firmware's FIPS interface module, showing if the device is properly initialized and started or it if has thrown errors on initialization. Each return value is for a different initialization or execution error as noted below:
FIPS Device is Connected = 3
FIPS Interface is Started = 2
FIPS Interface is Initialized = 1
FIPS Interface is Uninitialized = 0
Entropy Initialization Failed = -1
FIPS Core Health Test Failed = -2
Firmware Integrity Test Failed = -3
Crypto RNG Initialization Failed = -4
Crypto Key Initialization Failed = -5
The codes are consecutive and the processes run in order. For example, it is implied that the FIPS interface module is also properly initialized if the status report shows that it is started with the return the value 2.</td></tr>
<tr><td rowspan="2">FIPS Certification Library Version</td><td>None</td><td>FWSEGFV</td><td>BTSEGFV</td><td>FWSEGFV
BTSEGFV</td></tr>
<tr><td colspan="4">Description: Returns the current version of the cryptographic library WolfSSL's FIPS core version used for NIST CMVP level 1 certification. This value remains v4.5.2 until the next certification.</td></tr>
</table>

Officer Login	Officer	FWSEPON	BTSEPON	FWSEPONfipsOLpass BTSEPONfipsOLpass
	Description: Allows officers to login with the default or generated password. It takes a 10-character string of only letter and digits. The default password is "fipsOLpass" and it can be used for all officer services, but if the password is reset, then the new password must be read from CT2 and saved somewhere.			

Officer Logout	Officer	FWSEXOT	BTSEXOT	FWSEXOT BTSEXOT
	Description: Allows officers to logout. After logging out, none of the officer services will be available. If an officer is not logged in, this command has no effect.			
Officer Logging Status	None	FWSEGOL	BTSEGOL	FWSEGOL BTSEGOL
	Description: Reports if the officer role is logged in or not.			
Officer Password Renewal	Officer	FWSEPOR	BTSEPOR	FWSEPOR1234OLtest BTSEPOR1234OLtest FWSEPOR0 BTSEPOR0
	Attention: This command requires officer login. It allows officers to renew the service password. **Description:** There are two ways to renew this password: • Officers may enter their own new password. This requires appending the command with a 10-character alpha-numeric string to be set as the officer password. • The interface can generate passwords. This requires appending the command with a zero 0. The new password can be read from CT2 and should be recorded in a safe place as there is no way to retrieve it after CT2 is closed.			
User Login	User	FWSEPUN	BTSEPUN	FWSEPUNfipsULpass BTSEPUNfipsULpass
	Description: Allows users to log in with the default or generated password. It takes a 10-character string of only letters and digits. The default password is "fipsULpass" and it can be used for all user services, but if the password is reset, then the new password must be read from CT2 and saved somewhere. User login currently has no effect as no useful services are supported until further notice.			

User Logout	User	FWSEXUT	BTSEXUT	FWSEXUT BTSEXUT
	Description: Allows users to log out. After logging out, none of the user services will be available. If a user is not logged in, this command has no effect.			
User Logging Status	None	FWSEGUL	BTSEGUL	FWSEGUL BTSEGUL
	Description: Reports if the user role is logged in or not.			

User Password Renewal	User	FWSEXUR	BTSEXUR	FWSEXUR1234ULtest BTSEXUR1234ULtest FWSEXUR0 BTSEXUR0
	Attention: This command requires user login. It allows users to renew the service password. **Description:** There are two ways to renew this password: • Users may enter their own new password. This requires appending the command with a 10-character alpha-numeric string to be set as the user password. • The interface can generate passwords. This requires appending the command with a zero 0. The new password can be read from CT2 and should be recorded in a safe place as there is no way to retrieve it after CT2 is closed.			
Cryptographic Keys Renewal	Officer	FWSEXRK	BTSEXRK	FWSEXRK BTSEXRK
	Attention: This command requires officer login. It allows officers to renew all cryptographic keys on demand. **Description:** CR2700 generates and stores a 2048-bit RSA key pair for connection exchange and A271 generates and stores a 16-bit AES key and IV set for data encryption and decryption. When this command is issued on the CR2700, the RSA key pair is erased and then regenerated, and the current Bluetooth connection is maintained. If this command is issued on A271, then any active Bluetooth connection is dropped since the current session data key and IV are no longer valid as they are erased, and new ones are regenerated. **Interaction:** The large LED turns to amber during the key generation and storage, and a single beep indicates success.			

<table>
<tr><td rowspan="2">Cryptographic Library FIPS Core Power-up Self-test On-demand Run</td><td>Officer</td><td>FWSEXWF</td><td>BTSEXWF</td><td>FWSEXWF
BTSEXWF</td></tr>
<tr><td colspan="4">Attention: This command requires officer login. It allows officers to run health tests for WolfSSL library FIPS core on demand.

Description: This test may take several seconds. On CR2700 the large LED will turn amber, and in case of errors, the FIPS error beeps will be heard and an error message will be sent to the error log during this test. On A271 there are no indications, and in case of errors, messages will be sent to host.

Interaction: The large LED turns to amber during the key generation and storage, and a single beep indicates success.</td></tr>
</table>

<table>
<tr><td rowspan="2">Cryptographic Library Cipher Health Test Run</td><td>Officer</td><td>FWSEXWH</td><td>BTSEXWH</td><td>FWSEXWH
BTSEXWH</td></tr>
<tr><td colspan="4">Attention: This command requires officer login. It allows officers to run health tests for WolfSSL library ciphers on demand.

Description: This test may take several minutes. On CR2700 the large LED will turn amber, and in case of errors, the FIPS error beeps will be heard and an error message will be sent to the error log during this test. On A271 there are no indications, and in case of errors, messages will be sent to host.

Interaction: The large LED turns to amber during the key generation and storage, and a single beep indicates success.</td></tr>
<tr><td rowspan="2">Firmware Upgrade</td><td>Officer</td><td></td><td>None</td><td></td></tr>
<tr><td colspan="4">Attention: This command requires officer login. Please use CortexTools2 to upgrade both devices.

A271 Steps:
1. Open CortexTools2
2. Make sure it is not connected to a CR2700
3. Log into A271’s officer services (See the command in this table)
4. Download the new CRBFW file to A271

CR2700 Steps:
1. Open CortexTools2
2. Log into CR2700’s officer services (See the command in this table)
3. Connect to an A271

Download the new CRVFW file to CR2700</td></tr>
</table>