Curtiss-Wright

CCA-685 Secure Router

Hardware Version: CCA-685-C2820; Firmware Version: 2.1

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document number: 832404
Document Version: 1.1

Prepared for:

Curtiss-Wright
333 Palladium Drive
Kanata, Ontario
Canada K2V 1A6

Phone: +1 (613) 599-9191
http://www.cwcdefense.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the CCA-685 Secure Router from Curtiss-Wright. This Security Policy describes how the CCA-685 Secure Router meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic module. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The CCA-685 Secure Router is referred to in this document as the CCA-685 module, the cryptographic module or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Curtiss-Wright website (http://www.cwcdefense.com/) contains information on the full line of products from Curtiss-Wright.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Curtiss-Wright. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Curtiss-Wright and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Curtiss-Wright.

2 CCA-685 Secure Routers

2.1 Overview

Curtiss-Wright is a leading provider of state-of-the-art embedded computing solutions that offer high-density data processing under rugged operating conditions. Their product and service offerings include cutting-edge radar and graphics solutions, high-speed communication, custom software design and hardware engineering, and manufacturing services. By providing flexible design options and complete product integration services, Curtiss-Wright has earned itself a significant customer base in the aerospace, defense, and commercial markets.

2.1.1 CCA-685 Secure Router

The CCA-685 Secure Router is a high-performance custom conduction-cooled, network security appliance delivering converged firewall, intrusion detection or prevention system, switching, routing and Virtual Private Networking (VPN) services. Designed for secure rugged military or aerospace networks (Ethernet-based networks in air, land, and sea vehicles), the CCA-685 prevents unauthorized access to critical information. It can be used to secure a data storage network or to protect mission-critical applications from hostile attacks.

Figure 1 below shows a picture of the CCA-685 Secure Router with clamshell metal case installed.

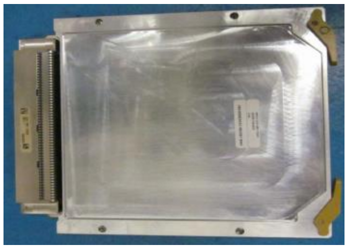


Figure 1 – CCA-685-C2820

The CCA-685 can be used as an intelligent Layer 2-managed switch or an advanced Layer 3-managed switch or router. It incorporates security software and a high-performance hardware-based security engine. Using the CCA-685, systems integrators can make high performance chassis-to-chassis, board-to-board or CPU[1]-to-CPU connections over Gigabit Ethernet. Advanced security and network features provided by the module include:

- Support for VLANs[2] and VPNs (IPsec[3]) to protect dedicated networks
- Spanning Tree Algorithms (STP[4], RSTP[5], MSTP[6]), IP multicasting, intelligent routing (RIP[7], OSPF[8]), Quality of Service (QoS), priority scheduling, network management, and remote monitoring
- Network Address Translation (NAT) routing for IPv4 masquerading
- Port- and protocol-based Access Control Lists to prevent unauthorized access
- IPv6 with IPsec tunneling for secure communications channels

[1] CPU – Central Processing Unit
[2] VLAN – Virtual Local Area Network
[3] IPsec – Internet Protocol Security
[4] STP – Spanning Tree Protocol
[5] RSTP – Rapid Spanning Tree Protocol
[6] MSTP – Multiple Spanning Tree Protocol
[7] RIP – Routing Information Protocol
[8] OSPF – Open Shortest Path First

- Advanced standards-based cryptographic functions (encryption, decryption, and authentication)

The CCA-685 module implements Non-Volatile Memory Read Only (NVMRO) protection. NVMRO is a hardware implementation that physically prevents writing to any non-volatile memory device on the module. The NVMRO signal must be asserted when entering FIPS-Approved mode.

2.1.1.1 CCA-685 System

The validated CCA-685 Secure Router supports twelve 10/100/1000 Base-T Ethernet ports. Embedded backplane routing is supported with standard Base-T GbE interfaces.

The CCA-685 Secure Router is comprised of a motherboard enclosed in a secure tamper-evident production-grade opaque clamshell-style metal case. The two primary devices on the board are the encryption-enabled general-purpose processor and the switch fabric. The processor includes CAVP-validated hardware implementations of cryptographic algorithms, referenced in Table 7. The switch fabric is used to support network routing and switching. The CCA-685 firmware architecture provides support for Ethernet switching, routing and cryptographic functionality implemented in the firmware.

Management of the CCA-685 Secure Router is possible via CLI[9] or WebNM[10]. The system provides secure management interfaces through secure HTTP[11] (HTTPS[12]) and Secure Shell (SSH). Figure 2**Error! Reference source not found.** below illustrates a typical deployment scenario of the CCA-685 Secure Router. The cryptographic boundary is shown by the red-colored dotted line and includes the entire metal case of the CCA-685 Secure Router.

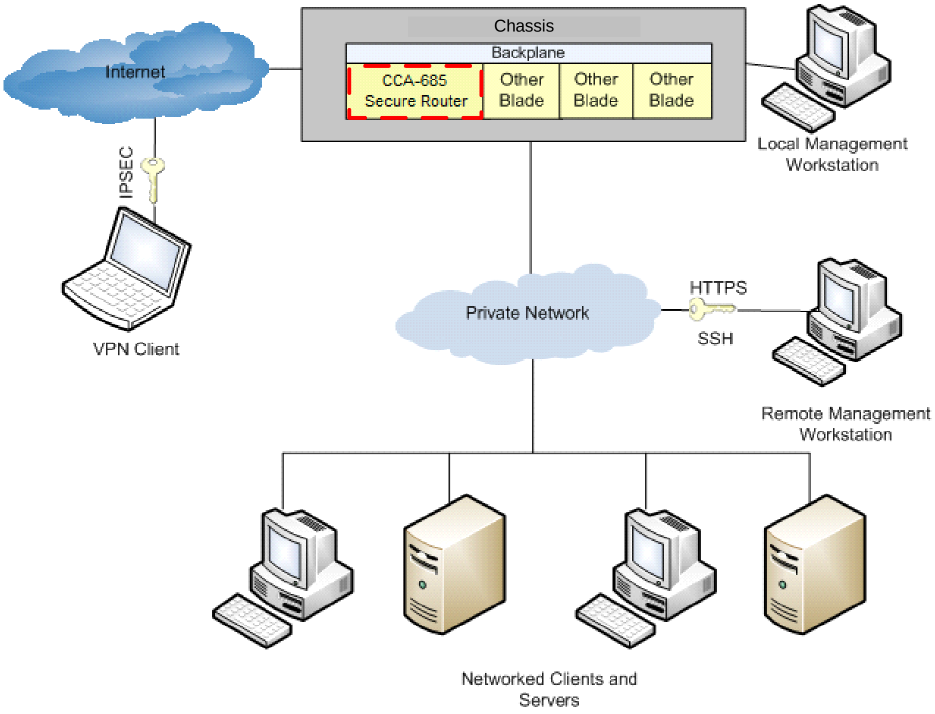


Figure 2 – Typical Deployment

[9] CLI – Command Line Interface
[10] WebNM – Web-based Network Management
[11] HTTP – Hyper Text Transfer Protocol
[12] HTTPS – HTTP over SSL

.

2.1.2 CCA-685 FIPS 140-2 Validation

The CCA-685 Secure Router is validated at the FIPS 140-2 Section levels as shown in Table 1 below:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A[13]
7	Cryptographic Key Management	2
8	EMI/EMC[14]	2
9	Self-tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The CCA-685 Secure Router is a multi-chip embedded cryptographic module including firmware and hardware. The main hardware components consist of a main processor, memory, and switch fabric with a backplane interface providing 10/100/1000 Base-T interfaces. The entire CCA-685 board (including the enclosure) is defined as the cryptographic boundary of the module. Figure 3 shows a block diagram for the module and the red-colored dotted line indicates the cryptographic boundary.

[13] N/A – Not applicable

[14] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

.

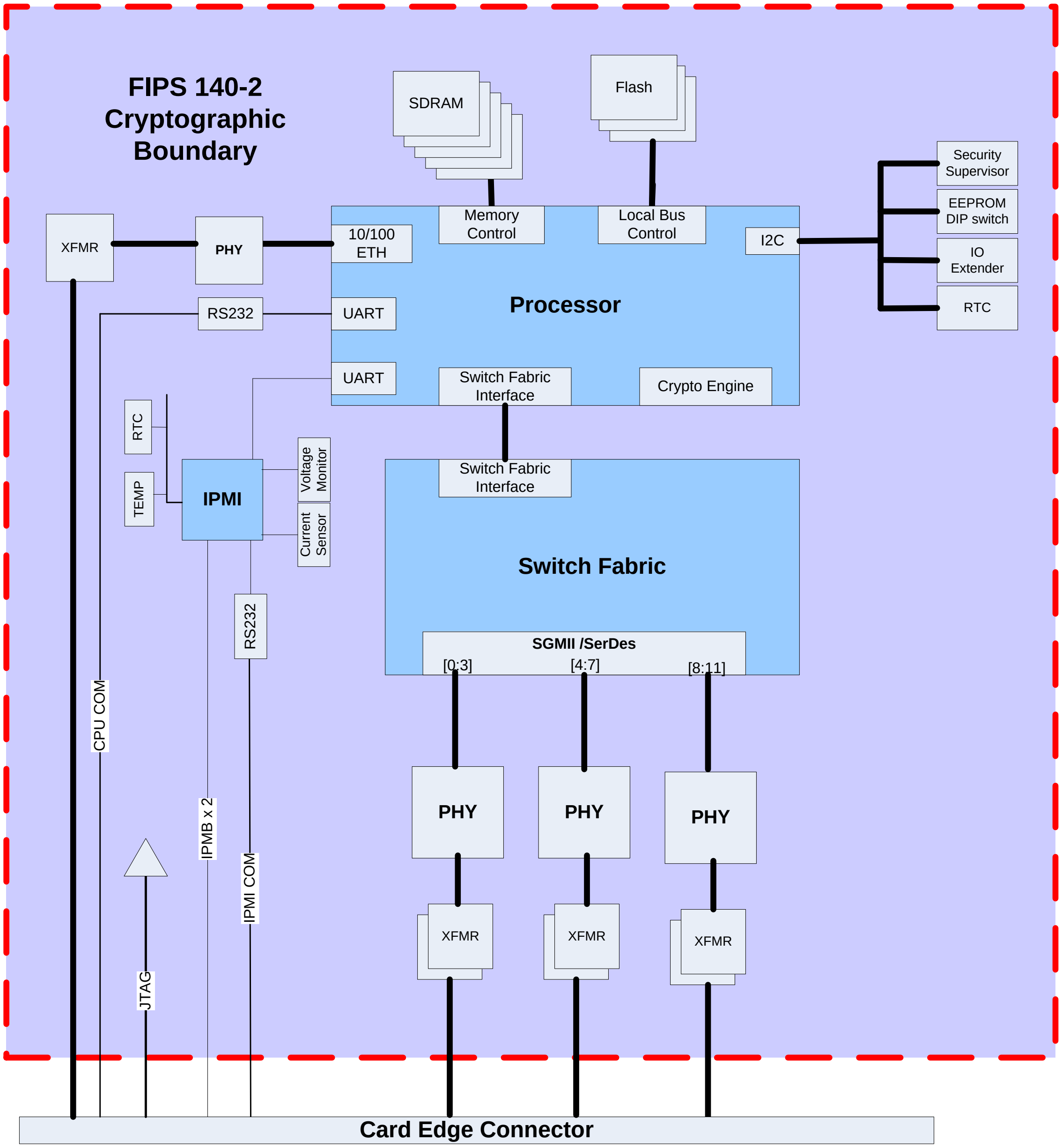


Figure 3 – Block Diagram with Cryptographic Boundary

2.3 Module Interfaces

The CCA-685 Secure Router offers two management interfaces:

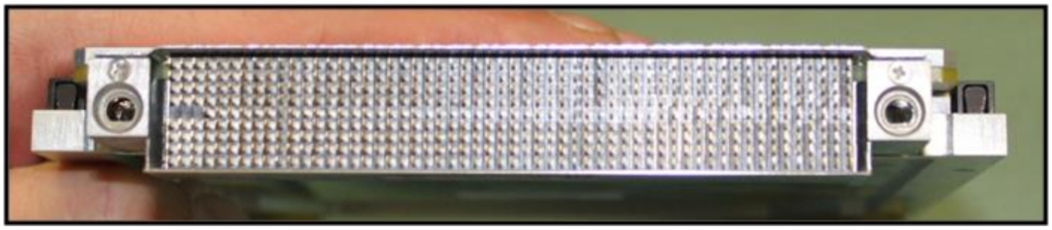
- CLI – accessible via an SSH session
- Web Interface

The design of the CCA-685 Secure Router separates the physical ports into four logically distinct and isolated categories. They are:

- Data Input
- Data Output
- Control Input
- Status Output

All ports and interfaces of the CCA-685-C2820 are accessible from the backplane connector, shown in the photo below.

Figure 4 – CCA-685 Connectors



The CCA-685 module has the ports/interfaces listed in Table 2 below.

Table 2 – CCA-685 Ports/Interfaces

Port/Interface	Description
TP01 – TP12	12 x 10/100/1000Base-T Ethernet ports
*OOB	Out Of Band (OOB) download port, 10/100 Base-T Ethernet Interface
*RS232	Serial console interface
*IPMB	Intelligent Platform Management Bus
*ALT_BOOT	Alternative Boot selection interface
NVMRO	Non-Volatile Memory Read-only control interface
Reset	Reset interface (SYS_RST or Mskble RST)
GA	Geographical Address interface
Key Zero	Discrete key zero control
Power	Power interface (12V)

To prevent tampering of programmable parts, JTAG access is physically disabled at the factory. The module also disables the IPMI COM, RS-232 and Out-Of-Band Ethernet interfaces when FIPS-Approved mode is set. The Field Replaceable Unit (FRU) is a mass memory device attached to the IPMI controller. It is factory programmable and write-protected through a controlled process when it leaves the factory.

.

The ports and interfaces marked with an asterisk (*) in Table 2 are physically disabled in the FIPS-Approved mode of operation. Table 3 lists the physical ports/interfaces available in the CCA-685 module, and also provides the mapping from the physical ports/interfaces to logical interfaces as defined by FIPS 140-2.

Table 3 – Logical Interface Mapping

FIPS 140-2 Logical Interface	Physical Port/Interface
Data Input Interface	Gigabit Ethernet ports, Geographical Address interface
Data Output Interface	Gigabit Ethernet ports
Control Input Interface	Gigabit Ethernet ports, NVMRO, Reset, Key Zero
Status Output Interface	Gigabit Ethernet ports
Power Input	Power interface

2.4 Roles and Services

As required by FIPS 140-2, the module supports two roles that operators may assume: a Crypto Officer (CO) role and a User role. Multiple concurrent operators are able to access the module at the same time. The CCA-685 Secure Router offers privilege levels 1-15 that provide operators with different levels of access to the module as defined by the CO who performs initial configuration. The keys and Critical Security Parameters (CSPs) listed in the

Table 4 indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

2.4.1 Crypto Officer Role

The CO is the administrator of the module. Only a Crypto Officer can create other COs (privilege level 1-15) and Users (privilege levels 1-4) and provision the CCA-685 to operate in FIPS-Approved mode. The Crypto Officers have access to the module's services and one or more CSPs. CO services are provided via the supported secure protocols, including Transport Layer Security (TLS), SSH, and IPsec[15] or IKE[16] for VPN[17] connections. Descriptions of the services available to the Crypto Officer are provided in Table 4.

2.4.2 User Role

The User (privilege levels 1-4) is limited to information and status activities and cannot configure the devices. Table 4 below lists the services available to the User.

[15] IPsec – Internet Protocol Security
[16] IKE – Internet Key Exchange
[17] VPN – Virtual Private Network

.

Table 4 – Mapping of Operator Services to Inputs, Outputs, CSPs, and Type of Access

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Authenticate	✓	✓	Used to log into the module	Command	Status output	Password – X
Configure the CCA-685 system	✓		Define network interfaces, settings, set the protocols to be used, load authentication information, define policies	Command and parameter	Command response	Password – X
Configure routing services	✓		Configure IP stack and firewall related features	Command and parameters	Command response	Password – X
Add/Delete/ Modify users	✓		Creating, editing and deleting users; Define user accounts and assign permissions.	Command and parameters	Command response	Password – R/W/X
Change passwords	✓		Modify existing login passwords	Command and parameters	Command response	Password – R/W
Load certificate	✓		Loads new certificates	Command	Command response	CA[18] Public Keys – R/W
Run script	✓		Run a script file. The script file is a text file containing a list of CLI commands.	Command	Command response	Password – X
Enter FIPS-Approved Mode	✓		Switch to FIPS-Approved mode	Command	Status output	None
Exit FIPS-Approved Mode	✓		Exit the FIPS-Approved mode	Command	Status output	All CSPs – W
Perform Self Tests	✓		Perform initiated self-tests (IBIT)	Command	Status output	Password – X
Network Diagnostics (e.g. ping)	✓	✓	Monitor connections	Command	Command response	Password – X
Show Status	✓	✓	Show the system status, Ethernet status, FIPS-Approved mode, system identification and configuration settings of the module	Command	Status output	Password – R/X

[18] CA – Certificate Authority

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
System Log	✓	✓	View system status messages	Command	Status output	Password – X
Zeroize	✓		Zeroize all keys and CSPs.	Command	Command response	All CSPs – W
Reset	✓		Reset the module	Command	Status output	CSPs stored in RAM – W
RADIUS or TACACS service	✓	✓	RADIUS or TACACS server logs in and performs authentication.	Command	Command response	RADIUS or TACACS Shared Secret Key – X
TLS	✓	✓	Login to the module via Web interface and perform any of the services listed above	Command	Command response/ Status output	Password – X TLS Public key – R/X TLS Private key – X TLS Session key – R/W/X TLS Authentication Key – R/W/X
SSH	✓	✓	Login to the module remotely using SSH protocol and perform any of the services listed above	Command	Command response/ Status output	Password – R SSH Authentication Key – R/W/X SSH Encryption Key – R/W/X
IPsec/IKE	✓	✓	Login to the module over VPN and perform any of the services listed above	Command	Command response/ Status output	Password – R IKE pre-shared Key – R/W/X IKE Private Key – R/W/X IKE DH key-pairs – R/W/X IPsec Message Authentication Key – R/W/X IPsec Message Encryption Key – R/W/X IPsec ESP[29] Key – R/W/X

2.4.3 Authentication Mechanism

All services provided by the module require the operator to assume a role and a specific identity. The module provide services only to authenticated operators. The module perform identity-based authentication.

All users authenticate to the module using a username and password or by the use of public key certificates. All users are required to follow the complex password restrictions. Table 5 lists the authentication mechanisms used by the module.

Table 5 – Authentication Mechanism Used by the Module

Authentication Type	Strength
Username/Password	The minimum length of the password is eight characters, with 95 different case-sensitive alphanumeric characters and symbols possible for usage. The “!” is only supported as the last character of the password. The chance of a random attempt falsely succeeding is 1: (94^7 x 95), or 1: 6,160,537,144,830,080. The fastest network connection supported by the module is 1 Gbps. Hence at most (10^9 × 60 = 6 × 10^{10} =) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is 1 : [(94^7 x 95) possible passwords / ((6 ×10^{10} bits per minute) / 64 bits per password)] 1: (94^7 x 95) possible passwords / 937,500,000 passwords per minute) 1: 6,571,239; which is less than 1:100,000 as required by FIPS 140-2.
Public Key Certificates	The module support RSA[19] digital certificate authentication of users during IPsec/IKE. Using conservative estimates and equating a 2048-bit RSA key to a 112 bit symmetric key, the probability for a random attempt to succeed is 1:2^{112} or 1: 5.19 x 10^{33}. The fastest network connection supported by the module is 1 Gbps. Hence at most (10^9 × 60 = 6 × 10^{10} =) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is 1: (2^{112} possible keys / ((6 × 10^{10} bits per minute) / 112 bits per key)) 1: (2^{112} possible keys / 53,571,428 keys per minute) 1: 96.92 × 10^{23}; which is less than 100,000 as required by FIPS 140-2.

2.5 Physical Security

All CSPs are stored and protected within the production-grade enclosures of the CCA-685 Secure Router. The removable enclosure is opaque within the visible spectrum and is protected by a tamper-evident seal. The structure of the enclosures is such that the top half is screwed in from the PWB[20] side and the bottom half screws go through the PWB and screw into the top half of the enclosures. The tamper evident seal is placed over one screw on the bottom half. The metal is such that any attempts to access without removing the covered screw would result in evidence in the metal cover itself. While the module is running in the FIPS-Approved mode, the tamper protection controller within the module monitors the power signal and zeroizes all keys and CSPs on detection of a tamper event[21]. All of the components within the module are production grade. The placement of tamper-evident seals can be found in Section 3.1 of this document.

[19] RSA – Rivest, Shamir, Adleman

[20] PWB – Printed Wiring Board

[21] A tamper event is defined as removing the module from a supported chassis which results in the loss of power

2.6 Operational Environment

The operational environment requirements do not apply to the CCA-685 Secure Router, because the module does not provide a general-purpose operating system (OS) to the user. The operating system is not modifiable by the operator and only the module's signed image can be executed.

2.7 Cryptographic Key Management

The CCA-685 module uses the FIPS-validated algorithm implementations in Hardware as listed in Table 6 below.

Table 6 – FIPS-Approved Algorithm Implementations in Hardware

Algorithm	Certificate Number
Advanced Encryption Standard (AES) in CBC[22], ECB[23], CFB128[24], CTR[25] and CMAC[26] modes (128-bit and 256-bit keys)	963
Triple Data Encryption Standard (Triple-DES) – CBC, ECB, OFB ; 3-key	758
Secure Hash Algorithm (SHA)-1, SHA-224, SHA-256, SHA-384, and SHA-512	934
Keyed-Hash Message Authentication Code (HMAC) using SHA-1*, SHA-224, SHA-256, SHA-384, and SHA-512	538

*Note: The use of SHA-1 for the purpose of Digital Signature Generation is non-compliant. The use of SHA-1 for the purpose of Digital Signature Verification is allowed for legacy-use. Any other use of SHA-1 for non-digital signature generation applications is acceptable and approved.

Additionally, the CCA-685 module supports FIPS-Approved algorithms implemented in firmware as listed in Table 7.

[22] CBC – Cipher Block Chaining
[23] ECB – Electronic Codebook
[24] CFB128 – Cipher Feedback (128-bit)
[25] CTR – Counter Mode
[26] CMAC – CBC Message Authentication Code

.

Table 7 – FIPS-Approved Algorithm Implementations in Firmware

Algorithm	Certificate Number
RSA PKCS#1 v1.5 Signature Verification – Mod (2048 and 3072)	1135
RSA PKCS#1 v1.5 Signature Verification – Mod (4096)**	1135
DSA Signature Verification with 1024-bit keys	713
DSA PQG Verification	713
SHA-1 (Uboot Firmware)	1907
ANSI[27] X9.31 PRNG[28]	1111
CVL – NIST SP 800-135 (IKE, SSH and TLS KDF)	405

The CCA-685 module supports non-approved and non-compliant algorithms implemented in both hardware and firmware as listed in Table 8 below.

Table 8 – Non-Approved and Non-Compliant Algorithm Implementations

Algorithm	Certificate Number
DSA Key-Pair Generation with 1024-bit keys (non-compliant)	713
DSA Signature Generation with 1024-bit keys(non-compliant)	713
RSA Key-Pair Generation Mod (4096)**	1135
RSA Key-Pair Generation Mod (2048 and 3072)	1135
RSA PKCS#1 v1.5 Signature Generation – Mod (2048 and 3072)	1135
RSA PKCS#1 v1.5 Signature Generation – Mod (4096)**	1135
DSA PQG Generation (non-compliant)	713
SHA-1 (non-compliant only when used for Digital Signature Generation)	538
DES (non-approved)	N/A
MD5 (non-approved)	N/A

**Note: The equivalent key-strength for RSA Mod (4096) is limited to 128-bits [i.e. equivalent of RSA Mod (3072)] instead of 150-bits because the maximum strength of the internally generated keys by the underlying ANSI X9.31 PRNG is limited to 128-bits.

The module implements the following key establishment schemes, which are allowed for use in a FIPS-approved mode of operation:

[27] ANSI – American National Standards Institute

[28] PRNG – Pseudo Random Number Generator

.

- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 128 bits of encryption strength)

Additional information concerning DSA, SHA-1, Diffie-Hellman key establishment, ANSI X9.31 PRNG, and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A. The module supports the CSPs described in Table 9.

Table 9 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Effective Strength	Generation/Input	Output	Storage	Zeroization	Use
IKE pre-shared key	Alpha-numeric string (Shared Secret)	Min 53-bits Max 203-bits	Electronically entered by the Crypto Officer	Never exits the module	SECRAM[29] (plain text)	Exit FIPS-Approved mode or zeroize command	Used for authentication during IKE when the authentication method is selected as “preshared”
IKE Private Key	RSA 2048-bit Private key	112-bits	Generated externally; Input encrypted via SFTP	Never exits the module	SECRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	Used for authentication during IKE when the authentication method is selected as “cert”
IKE Public Key	RSA 2048-bit Public key	112-bits	Generated Internally via ANSI X9.31 PRNG	Exits the module in plaintext in the form of a certificate	SECRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	Used for peer authentication to module during IKE when the authentication method is selected as “cert”
IKE DH Symmetric Key	2048-bit DH session key	112-bits	Generated internally during IKE negotiation via ANSI X9.31 PRNG	Never exits the module	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	Exchanging shared secret to derive encryption keys during IKE
IPsec Message Authentication Key	HMAC SHA-1 for IPsec data integrity	160-bits	Electronically entered in the case of manual VPN policy	Never exits the module	SECRAM (plain text)	Exit FIPS-Approved mode or zeroize command	Used for peer authentication before encrypting IPsec packets
		128-bits	Generated internally via ANSI X9.31 PRNG) as a result of IKE protocol exchanges	Never exits the module	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	

[29] SECRAM - SecureRAM

.

CSP	CSP Type	Effective Strength	Generation/Input	Output	Storage	Zeroization	Use
IPsec Message Encryption Key	Triple-DES AES key	112-bits 128 or 256 bits	Electronically entered in the case of manual VPN policy	Never exits the module	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	Used to encrypt peer-to-peer IPsec messages
		112-bits 128-bits	Generated internally (via ANSI X9.31 PRNG) as a result of IKE protocol exchanges	Never exits the module	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	
IPsec ESP[30] Key	Triple-DES AES key	112-bits 128 or 256 bits	Electronically entered in the case of manual VPN policy	Never exits the module	SECRAM (plain text)	Exit FIPS-Approved mode or zeroize command	Used to encrypt IPsec session data
		112-bits 128-bits	Generated internally (via ANSI X9.31 PRNG) as a result of IKE protocol exchanges	Never exits the module	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	
SSH Authentication Key	HMAC SHA-1	128-bits	Generated internally via ANSI X9.31 PRNG	Never exits the module	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	It is used for data integrity and authentication during SSH sessions
SSH Encryption Key	Triple-DES keys	112-bits	Generated internally via ANSI X9.31 PRNG	Never exits the module	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	It is used for encrypting or decrypting the data traffic during the SSH session
TLS Session Key	Triple-DES AES	112-bits 128-bits	Generated internally via ANSI X9.31 PRNG	Never exits the module	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	It is used for encrypting or decrypting the data traffic during the TLS session
TLS Authentication Key	HMAC SHA-1	128-bits	Generated internally via ANSI X9.31 PRNG	Never exits the module	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	It is used for data integrity and authentication during TLS sessions

[30] ESP – Encapsulating Security Payload

.

CSP	CSP Type	Effective Strength	Generation/Input	Output	Storage	Zeroization	Use
TLS Private Key	RSA 2048-bit Private Key	112-bits	Generated internally via ANSI X9.31 PRNG	Never exits the module	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	It is used for authenticating a peer attempting to establish a secure HTTPS connection
TLS Public Key	RSA 2048-bit Public Key	112-bits	Generated internally via ANSI X9.31 PRNG	Exits the module in plaintext in the form of a certificate	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	It is used by a peer attempting to establish a secure HTTPS connection with the module
RADIUS Shared Secret Key	Alpha-numeric string (Shared Secret)	Min 53-bits Max 315-bits	Electronically entered by Crypto Officer	Never exits the module	SECRAM (plain text)	Exit FIPS-Approved mode or zeroize command	Used for authenticating the RADIUS server to the CCA-685
Password	Crypto Officer and User passwords	53-bits	Electronically entered by Crypto Officer	Never exits the module	SECRAM (plain text)	Exit FIPS-Approved mode or zeroize command	Used for authenticating the Crypto Officer or User
ANSI X9.31 PRNG Seed	Seed	128-bits	Generated internally	Never exits the module	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	Used to generate FIPS approved random number
ANSI X9.31 PRNG Seed Key	Seed Key	128-bits	Generated internally	Never exits the module	SDRAM (plain text)	Power cycle, exit FIPS-Approved mode or zeroize command	Used to generate FIPS approved random number

Caveat: The module generates cryptographic keys whose strengths are modified by available entropy, and thus the maximum encryption strength of the internally generated module keys is 128 bits.

.

2.8 EMI/EMC

The module was tested and found to be conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2.9 Self-Tests

The CCA-685 Secure Router provides cryptographic support in the form of hardware and firmware cryptographic algorithm implementations. As such, cryptographic self-tests are required to be performed on these implementation in order to operate in a FIPS-Approved mode of operation.

2.9.1 Power–Up Self–Tests

The CCA-685 Secure Router implements the following Power-Up Self-Tests, also referred as Power-up Built-In-Tests (PBIT):

- Boot ROM[31] firmware integrity self-test via 160-bit EDC
- Power-up Self-Tests
  - AES KAT[32] (encrypt/decrypt tested)
  - Triple-DES KAT (encrypt/decrypt tested)
  - SHA-1 KAT
  - SHA-2[33] KAT
  - HMAC SHA-1 KAT
  - HMAC SHA-2 KAT
  - RSA KAT
  - DSA PCT[34]
  - ANSI X9.31 PRNG KAT

Upon failing a PBIT KAT, the module will transition to a temporary error state. In the error state, the module will notify the operator of a failed PBIT, clear the error conditions, and then exit the FIPS_Approved mode of operation. and the module will not be operating in the FIPS-Approved mode. To attempt the PBIT again and run the module in a FIPS-Approved mode of operation, the operator will be required to restart the module. The self-tests listed above will generate a hard error if a failure occurs, and will require the module to be returned to Curtiss-Wright for service.

2.9.2 Conditional Self–Tests

The CCA-685 module implements the following Conditional Built-In-Tests (CBIT) on the software cryptographic algorithm implementations. CBITs are not required for the hardware algorithm implementations.

- Continuous Random Number Generator Test for the ANSI X9.31 PRNG
- RSA PCT
- DSA PCT

Upon failing a CBIT, and the module will transition to a temporary error state and display an error message to the operator when the syslog is configured[35]. The error state will then be cleared by the CCA-685 and the module will restart outside the FIPS-Approved mode of operation.

[31] ROM – Read Only Memory
[32] KAT – Known Answer Test
[33] The SHA-2 hash family includes SHA-224, SHA-256, SHA-384, and SHA-512
[34] PCT – Pairwise Consistency Test

.

2.9.3 User-Initiated Built-In-Tests

The CCA-685 module implements the following Initiated Built-In-Tests (IBIT) that can be initiated by an authorized operator. The operator will invoke the IBIT test through a single command via the CLI. IBITs will only be performed on the firmware cryptographic algorithms:

- SHA-1 KAT
- SHA-256 KAT
- SHA-512 KAT
- HMAC SHA-1 KAT
- HMAC SHA-2 KAT
- Triple-DES KAT
- AES KAT
- RSA KAT
- DSA PCT
- ANSI X9.31 PRNG KAT

Upon failing an IBIT, the test will immediately stop, and the module will transition to a temporary error state. All data output from the module is suppressed. The error state will be cleared by the CCA-685 while all cryptographic operations are suspended. The CO at this point may choose to retry the test or restart the module. The self-tests listed above will generate a hard error if a failure occurs, and will require the module to be returned to Curtiss-Wright for service.

To perform on-demand self-tests on the hardware cryptographic algorithms, the module must be restarted.

2.10 Mitigation of Other Attacks

This section is not applicable. The module do not claim to mitigate any attacks beyond the FIPS 140-2 requirements for this validation.

[35] Please refer to "CCA-685 Command Line Interface (CLI) Software Reference Manual"

3 Secure Operation

The CCA-685 Secure Router meets overall Level 2 requirements for FIPS 140-2. The sections below describe how to ensure that the module is running securely.

3.1 Initial Setup

The following sections provide the necessary step-by-step instructions for the secure installation of the CCA-685, as well as the steps necessary to configure the module for a FIPS Approved mode of operation.

3.1.1 CCA-685 Installation

In order to setup a CCA-685 module, the following steps shall be performed by an authorized CO:

1. Unpack the Circuit Card Assembly from the shipping carton in a suitable work area. If the shipping carton appears to be damaged, request that an agent of the shipper or carrier be present during unpacking and inspection.
2. Find the packing list. Make sure all the items on the list are present.
3. Place the CCA-685 in the selected slot of the backplane. Refer to the CCA-685 User's Manual for a complete set of instructions on installing the module.
4. After successful installation, the module can be configured per the initial configuration instructions in the CCA-685 User's Manual. This includes the creation of the CO and User accounts.
5. Once the network settings are correctly configured for the module, return to Section 3.1.3 in this document to configure CCA-685 module for FIPS-Approved mode.

3.1.2 CCA-685 Tamper-Evident Seal Inspection

The CCA-685 module will be shipped from the factory with the tamper-evident seal already installed. Prior to use, the Crypto Officer shall inspect the tamper-evident seal and if tampering is witnessed, the Crypto Officer shall return the module back to Curtiss-Wright. The tamper seal shall also be inspected periodically, on a schedule established by the Crypto-Officer, and the module returned to Curtiss-Wright if tampering is witnessed. The removable enclosure is opaque within the visible spectrum and is protected by one tamper evident seal placed on the bottom of the enclosure over a single screw. Figure 5 shows the placement of the tamper evident seal on the CCA-685 Secure Router.

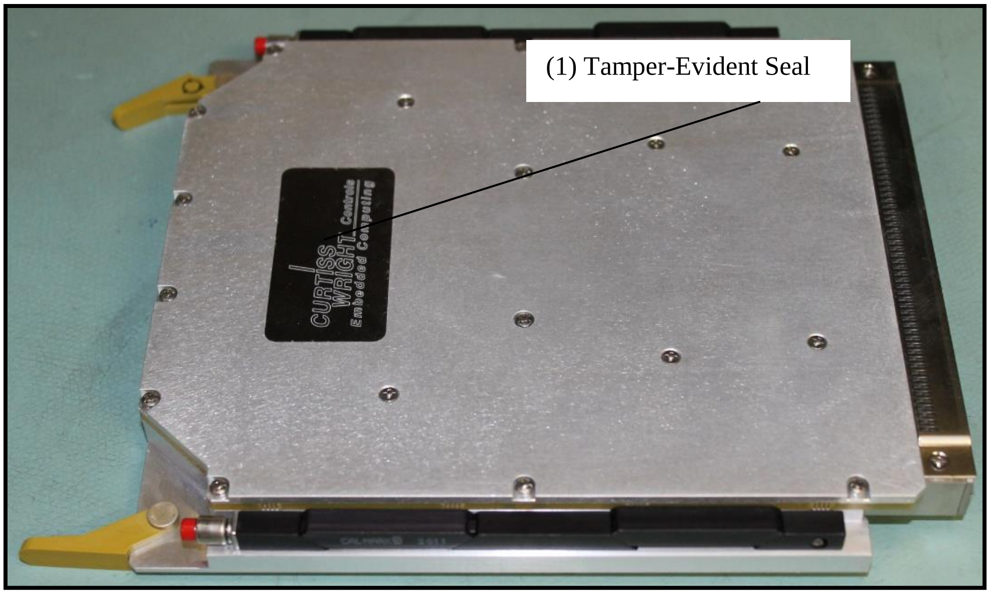


Figure 5 – CCA-685 Tamper Evident Seal Placement

3.1.3 CCA-685 FIPS-Approved mode Configuration

Once all necessary initialization procedures have been performed as described in the preceding sections, the module needs to be configured to comply with FIPS 140-2 requirements. By default, the module is not configured to operate in the FIPS-Approved mode on the first power-up. In order to place a module in FIPS-Approved mode, the following steps are to be followed:

1. Enter command "crypto zeroize keys" to zeroize CSPs
2. Confirm configuration as mentioned in Section 3.1.1 above
3. The command "fips mode enable" is used to enter FIPS-Approved mode. One of the conditions of entering and staying in FIPS-Approved mode is that NVMRO remains asserted which prevents write access to SECRAM memory protecting the firmware and configuration.
4. The command which may be entered into the CLI, includes a system status indicating if the CCA-685 is in FIPS-Approved mode.
5. Configure operator accounts and authorizations.
6. In FIPS-Approved mode, the operator is prevented from setting a VPN configuration with strength stronger than the security provided by the management interface.

3.1.4 CCA-685 Non-Approved mode Configuration

The CCA-685 contains a non-Approved mode of operation. The same services listed in Table 4 are also available in the non-Approved mode, however there are no restrictions on their execution, and thus no assurances can be made that they are used in a compliant manner. Additionally, DES and MD5 algorithms are available in the non-Approved mode. (The module enforces the non-use of DES and MD5 in the Approved mode of operation.) The module can be configured for non-Approved mode as follows:

1. Install jumper on PCB for r/w mode;
2. Reboot the module;
3. Verify that the module is in the non-Approved mode by entering the command "show fips status".
4. Configure accounts and authorizations.

In addition to DES and MD5 being exclusive to the non-Approved mode of operation, SSHv1 and SSL3.0 are also only allowed in the non-Approved mode.

.

3.2 Crypto Officer Guidance

The Crypto Officer shall receive the module from Curtiss-Wright via trusted couriers (e.g. United Parcel Service, Federal Express, and Roadway). On receipt, the Crypto Officer shall check the package for any irregular tears or openings. Prior to use, the Crypto Officer shall inspect the tamper-evident seal and if tamper is suspected, the Crypto Officer shall contact Curtiss-Wright for further guidance. The Crypto Officer shall create a schedule to periodically re-inspect these seals for tampering.

The CCA-685 module supports multiple Crypto Officers. This role is assigned when the first CO logs into the system using the default username and password. The Crypto Officer shall change the default password after initial login. Only the Crypto Officer can create other operators and bring the CCA-685 module to a FIPS-Approved mode. It is only possible to enter FIPS-Approved mode with NVMRO asserted. The following functions shall be performed by the Crypto Officer to enter and remain in a FIPS approved mode:

- Enter command “crypto zeroize keys” to zeroize CSPs
- Enter command “fips mode enable” to enter FIPS-Approved mode
- Confirm configuration as mentioned in Section 3.1.1 above
- Verify that the module is in FIPS-Approved mode by entering the command “show fips status”.

3.2.1 Management

The Crypto Officer is responsible for maintaining and monitoring the status of the module to ensure that it is running in its FIPS-Approved mode. Please refer to Section 3.1.3 and Section 3.2 above for guidance that the Crypto Officer must follow for the module to be considered in a FIPS-Approved mode of operation. For details regarding the management of the module, please refer to the CCA-685 Manuals.

3.2.2 Zeroization

There are many critical security parameters (CSP) within the cryptographic boundary of the module, including private keys, certificate secret credentials, and logon passwords. All ephemeral keys used by the module are zeroized on reboot or session termination. Keys and CSPs reside in plaintext in multiple storage media including the SDRAM and SECRAM. Keys residing in volatile memory are zeroized when the module are rebooted. Other keys and CSPs, such as public and private keys, that are in a file stored on SDRAM can be zeroized by the CO by issuing the “crypto zeroize keys” command. Additionally, all keys and CSPs are also zeroized when the module loses power, or the Key Zeroize backplane signal is asserted. Zeroization will also occur whenever the module transitions to the FIPS-Approved or exits the FIPS-Approved mode of operation. Please refer to Table 9 for the specific zeroization methods of each key and CSP.

3.3 User Guidance

The User does not have the ability to configure sensitive information on the module, with the exception of their password. The User must be diligent to pick strong passwords, and must not reveal their password to anyone. Additionally, the User should be careful to protect any secret or private keys in their possession.

4 Acronyms

Table 10 describes the acronyms used in this Security Policy.

Table 10 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AUX	Auxiliary
BIT	Built In Test
CA	Certificate Authority
CBC	Cipher Block Chaining
CBIT	Continuous Built-In Test
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CLI	Command Line Interface
CMAC	CBC Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSE	Communications Security Establishment Canada
CSP	Critical Security Parameter
CTR	Counter
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EDC	Error Detection Code
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
FRU	Field Replaceable Unit

.

Acronym	Definition
FTP	File Transfer Protocol
GA	Geographical Address
GbE	Gigabit Ethernet
HMAC	(Keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL
IBIT	Initial Built-In Test
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
IPsec	Internet Protocol Security
JTAG	Joint Test Action Group
KAT	Known Answer Test
L2TP	Layer 2 Tunneling Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
MD	Message Digest
MSTP	Multiple Spanning Tree Protocol
N/A	Not Applicable
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NVMRO	Non-Volatile Memory Read Only
NVRAM	Non-Volatile Random Access Memory
OFB	Output Feedback
OOB	Out Of Band
OS	Operating System
OSPF	Open Shortest Path First
PBIT	Power-up Built-in Test
PCI	Peripheral Component Interface
PCT	Pairwise Consistency Test
PHY	Physical Layer

.

Acronym	Definition
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunneling Protocol
PRNG	Pseudo Random Number Generator
PWB	Printed Wiring Board
PWR	Power
RADIUS	Remote Authentication Dial-In Service
RAM	Random Access Memory
RIP	Routing Information Protocol
RNG	Random Number Generator
ROM	Read Only Memory
RS	Recommended Standard
RSA	Rivest, Shamir, and Adleman
RST	Reset
RSTP	Rapid Spanning Tree Protocol
RTM	Rear Transition Module
SDRAM	Synchronous Dynamic Random Access Memory
SerDes	Serializer/Deserializer
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
STAT	Status
STP	Spanning Tree Protocol
Triple-DES	Triple Data Encryption Standard
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WebNM	Web based Network Management

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com