HP Inc.

Tera2 PCoIP Zero Client Processors

Hardware Models: TERA2140, TERA2321
Firmware Version: 21.01.5-fips

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.12

Prepared for:

HP Inc.
1501 Page Mill Road
Palo Alto, CA 94304
United States of America

Phone: +1 650-857-1501
www.hp.com

Prepared by:

Corsec Security, Inc.
12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a Cryptographic Module Security Policy for the Tera2 PCoIP Zero Client Processors from HP Inc. (HP). This Security Policy describes how the Tera2 PCoIP Zero Client Processors meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

This document also describes how to run the Tera2 PCoIP Zero Client Processors in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation. The Tera2 PCoIP Zero Client Processors are referred to in this document as the Tera2 Processors or, collectively, 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 HP website (www.hp.com) contains information on the full line of products from HP Inc.
- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

1.3 Document Organization

The Security Policy document is organized into two (2) primary sections. Section 2 provides an overview of the validated module. This includes a general description of the module's capabilities and their use of cryptography as well as a presentation of the validation level achieved in each applicable functional area of the FIPS standard. It also provides high-level descriptions of how the module meets FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions, management methods, and applicable usage policies.

2. Tera2 PCoIP Zero Client Processors

2.1 Overview

PC-over-IP (PCoIP) technology delivers a secure, high-definition and highly responsive computing experience. It uses advanced display compression to provide end-users with on-premises or cloud-based virtual machines as a convenient alternative to local computers. This virtual workspace architecture compresses, encrypts, and transmits only pixels to a broad range of software clients, mobile clients, thin clients, and stateless PCoIP Zero Clients, providing a highly secure enterprise environment (see Figure 1 below). Because the PCoIP protocol transfers only display information in the form of pixels, no business information ever leaves your cloud or data center.

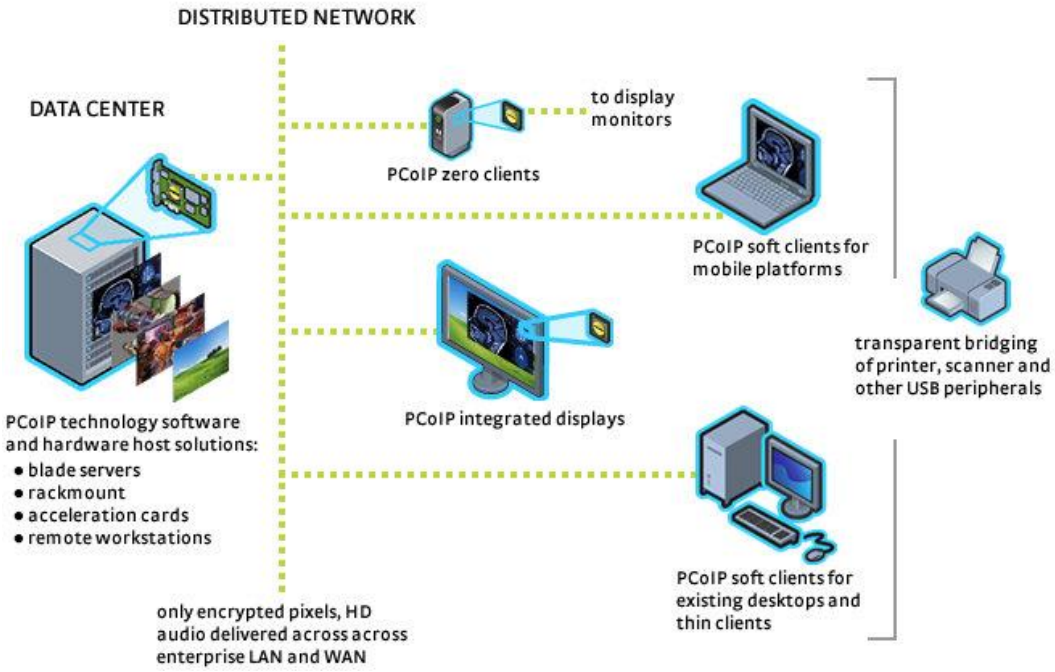


Figure 1 – Typical Network of PCoIP Clients

Tera2 PCoIP Zero Clients are hardware- and firmware-based endpoints that enable users to connect remotely to the following PCoIP host endpoints:

- PCoIP Remote Workstation Cards[1]
- HP Anyware
- Amazon WorkSpaces desktops
- VMware Horizon desktops

[1] **PCoIP Remote Workstation Cards** are small add-in cards that can be integrated into tower PCs, rack mount PCs, PC blades, and server blades. The card's TERA-series processor performs advanced display compression algorithms to encode a user's full desktop environment. This information is communicated in real-time over an IP network to the user's Tera2 PCoIP Zero Client.

Because they do not have general purpose CPUs[2], local data storage, or application operating systems, Tera2 PCoIP Zero Clients are very secure and easy to manage. Tera2 PCoIP Zero Clients contain upgradable firmware that enables client to be customized with various features.

Zero Clients come in many forms, such as small stand-alone devices, PCoIP-integrated displays, and touch-screen monitors. They support multiple wide-screen formats, HD[3] audio, and local USB[4] peripherals, and are IPv6[5]-ready. They also have extensive USB security and authentication features, including multiple-factor authentication for use with proximity cards, smart cards, and One-Time-Passwords.

For Tera2 PCoIP Zero Client systems, HP's family of PCoIP processors enables the creation of a perception-free remote Graphical User Interface (GUI) by bridging user interface connections for a personal computer (PC) across an IP[6] network. The system (see Figure 2 below) includes a PCoIP host processor at the host PC that encodes the display, USB, and audio signals before transmitting them over the network. A second PCoIP processor at the remote Zero Client site receives and decodes these signals.

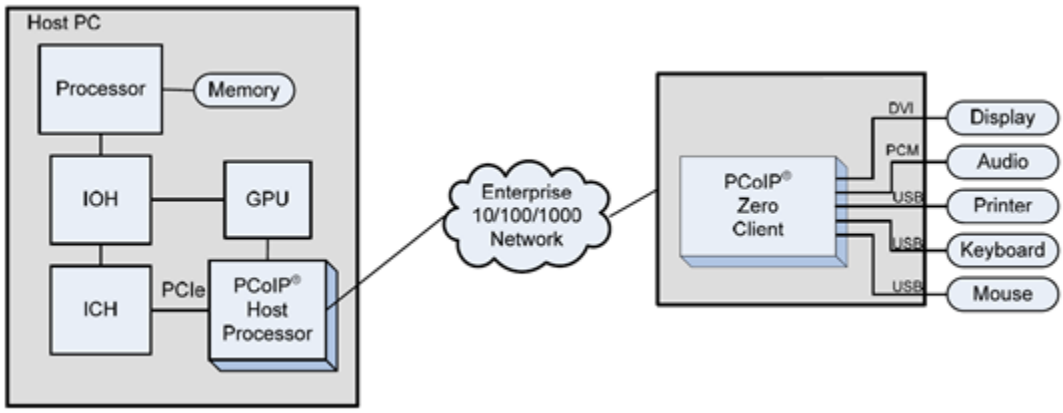


Figure 2 – Typical Single-User PCoIP Deployment in a Zero Client System

HP's Tera2 PCoIP Zero Client Processors (highly-integrated, purpose-built ASICs[7], see Figure 3 and Figure 4 below) perform the image decompression and decoding functions at the Zero Client site, creating standard PC interfaces for the display, USB peripherals, and PC audio. The system supports a reverse communication path for items like USB keyboards, mice, microphone audio, and other peripherals. PCoIP session negotiation and key establishment occur over TLS[8], while PCoIP sessions occur over UDP[9] (using the UDP-encapsulated ESP[10] packet format per *RFC*[11] *3948*) and are protected using 256-bit AES[12]-GCM[13] encryption.

[2] CPU – Central Processing Unit
[3] HD – High-Definition
[4] USB – Universal Serial Bus
[5] IPv6 – Internet Protocol version 6
[6] IP – Internet Protocol
[7] ASIC – Application-Specific Integrated Circuit
[8] TLS – Transport Layer Security
[9] UDP – User Datagram Protocol
[10] ESP – Encapsulating Security Payload
[11] RFC – Request For Comments
[12] AES – Advanced Encryption Standard
[13] GCM – Galois-Counter Mode

Figure 3 – TERA2140 Zero Client Processor

Figure 4 – TERA2321 Zero Client Processor

Each of the Tera2 Processors uses an external flash device for storing non-volatile program data, including the boot code for the onboard MIPS32® M4K® processor cores and the compressed firmware images. The TERA2140 processor uses an external parallel I/O flash device while the TERA2321 processor uses an external multi-bit serial I/O flash device. Each of the Tera2 Processors employs a MIPS32® 24kc® processor core running the ThreadX 4.0c operating system to execute the module firmware.

Management of the Tera2 PCoIP Zero Client Processors can be accomplished via the following method(s):

- PCoIP On-Screen Display (OSD) – a pre-session GUI embedded within the client for configuring the device's firmware. Used for local administration, the OSD appears on a direct-connected display when the Zero Client is powered on, but only when no PCoIP sessions are in progress.

- PCoIP Administrative Web Interface (AWI) – a web-based user interface for configuring a single PCoIP Zero Client's firmware remotely. It is accessible after typing the target client's IP address or FQDN[14] into the browser's address bar.

- PCoIP Management Console (MC) – a web-based user interface on a remote workstation for discovering, configuring, and managing multiple PCoIP Zero Client endpoints. It can be deployed as an Open Virtual Appliance (OVA) file for installation on a VMware Horizon ESXi host or as an Amazon Machine Image (AMI) for services delivered using Amazon Elastic Compute Cloud (EC2).

[14] FQDN – Fully Qualified Domain Name

These management interfaces provide authorized operators access to the module for configuration and management of all facets of the module's operation. Using these tools, IT[15] administrators can quickly provision new devices, review metrics, configure settings, update firmware, and view event logs.

The Tera2 PCoIP Zero Client Processors are validated at the FIPS 140-2 section levels indicated in Table 1 below.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC[16]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Tera2 PCoIP Zero Client Processors represent a hardware cryptographic module with a multiple-chip embedded embodiment. The cryptographic module has two instances; each instance consists of a Tera2 Processor, DDR3 SDRAM, and NOR Flash. Table 2 lists the components to be used for each module instance during validation testing.

Table 2 – Cryptographic Module Instance Components

Tera2 Processor	DDR3 RAM	NOR Flash
TERA2140	4x 1Gb Samsung DDR3 RAM (P/N: K4B1G1646G-BCH9)	Macronix NOR Flash (P/N: MX29GL256ELT2I-90Q)
TERA2321	2x 2Gb Samsung DDR3 RAM (P/N: K4B2G1646B-HCH9)	Macronix NOR Flash (P/N: MX25L25635EMI-12G)

In each case, the module's cryptographic boundary surrounds all module components.

[15] IT – Information Technology
[16] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

Figure 5, Figure 6, and Figure 7 below provide images of the module instances as each would appear on a reference PCB[17]. Note that the reference board and remaining components shown in the figures are not within the defined cryptographic boundary and are not part of the validated module.

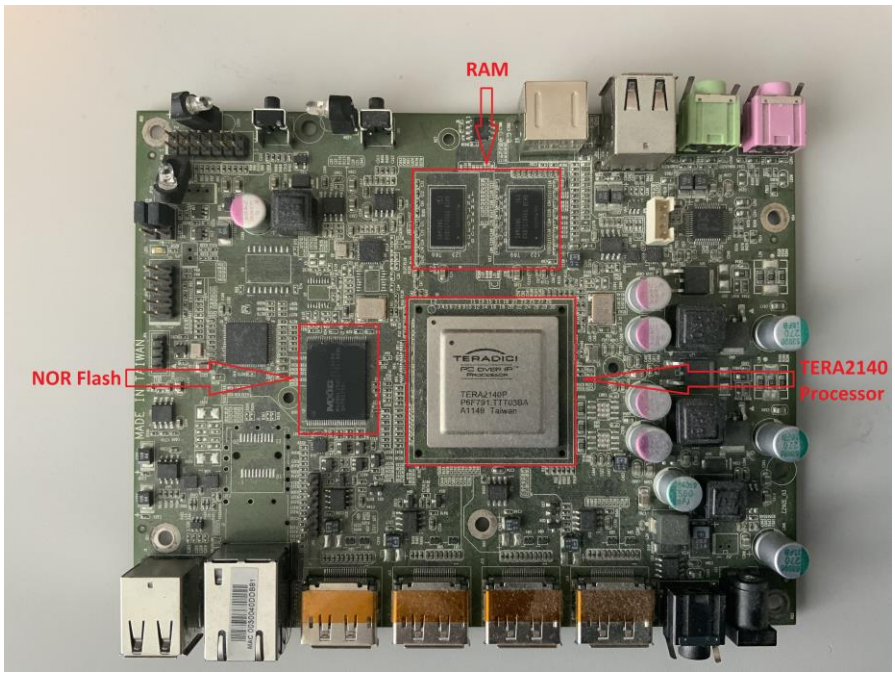
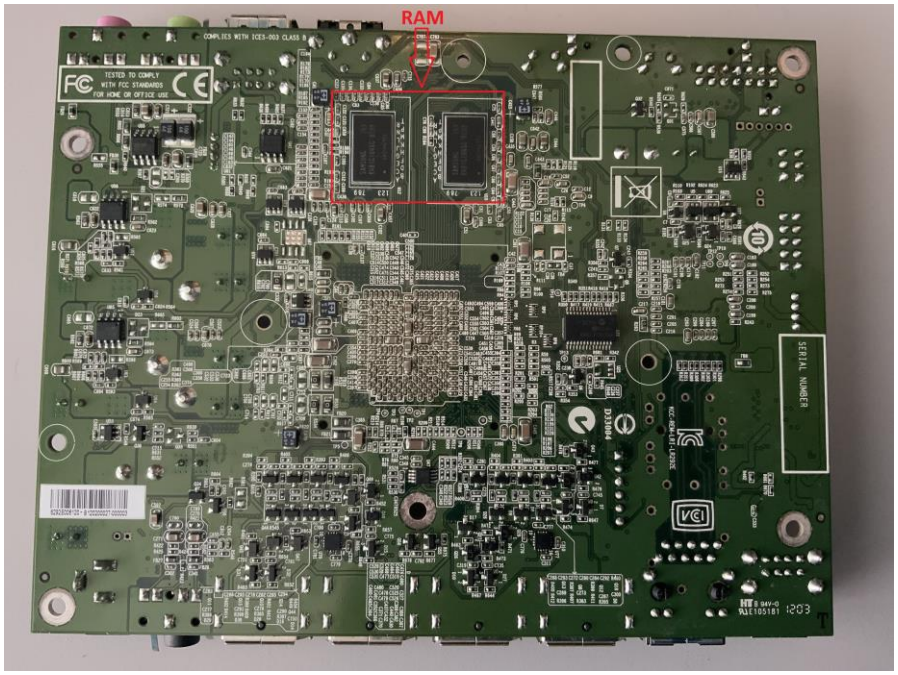


Figure 5 – Module Components on Reference PCB (TERA2140, Top View of PCB)



[17] PCB – Printed Circuit Board

Figure 6 – Module Components on Reference PCB (TERA2140, Bottom View of PCB)

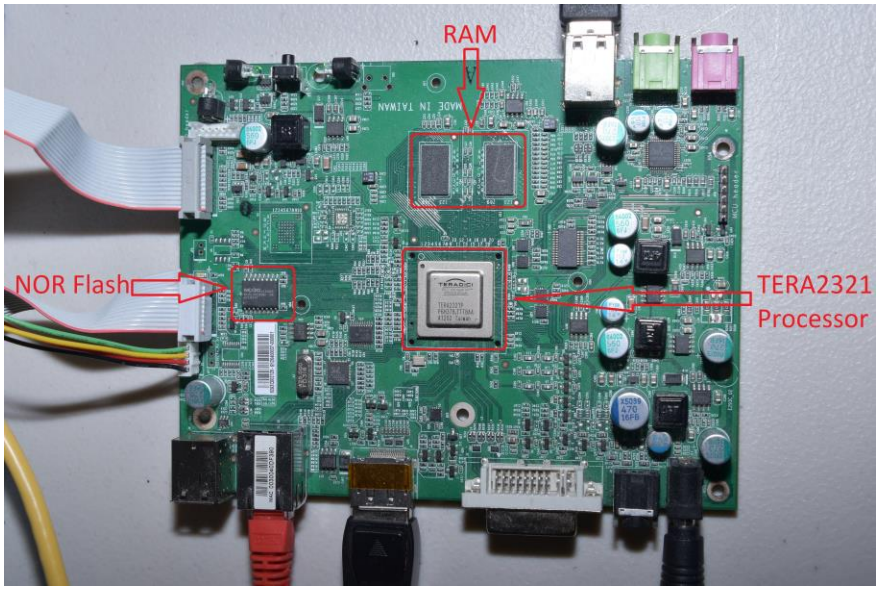


Figure 7 – Module Components on PCB (TERA2321, Top View of PCB)

While the reference instances of the module are as stated above, the Tera2 processors are provided to OEMs for installation onto PCBs that may employ various other DDR3 RAM and NOR Flash components. However, based on CMVP hardware equivalency guidance in *FIPS 140-2 IG G.19*, replacing either of these memory components with other memory components of the same type/technology is not considered security relevant.

The module firmware includes two components: a full-featured Mode 1 main image and a limited-function Mode 2 recovery image. While each component has its own version and build ID (see section 3.2.1 for guidance on how to view this information), the collection of firmware components is versioned **21.01.5-fips**. As such, both components were found compliant during module testing.

The overall security level of the module is 1.

2.2.1 Approved and Non-Approved Algorithms

The module includes the cryptographic algorithm providers listed in Table 3 below.

Table 3 – Cryptographic Algorithm Providers

Certificate Number	Implementation Name	Version	Use
A1111	HP Tera2 Cryptographic Library	1.0	Firmware-based cryptographic primitives
A1112	HP Tera2 SNMP KDF	1.0	Firmware-based SNMP key derivation function
A1113	HP Tera2 HW AES-GCM	1.0	Hardware-based AES-GCM implementation
A2048	HP Tera2 SHA3	1.0	Firmware-based SHA3 implementation

The cryptographic module implements the FIPS-Approved algorithms listed in Table 4.

Table 4 – FIPS-Approved Algorithms

Certificate Number		Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
HW	FW					
A1113	-	AES[18]	*FIPS PUB 197*	ECB[19]	256	Encryption/decryption *AES-ECB is not used operationally; the forward cipher was tested as a prerequisite for GCM testing.*
			NIST SP 800-38D	GCM	256	Encryption/decryption
-	A1111	AES	*FIPS PUB 197*	CBC[20], CFB128[21], CTR[22], ECB, OFB[23]	128, 256	Encryption/decryption
			NIST SP 800-38D	GCM	256	Encryption/decryption
-	Vendor Affirmed	CKG[24]	*NIST SP 800-133rev2*	-	-	Symmetric key generation
-	A1111	CVL[25]	*FIPS PUB 186-4*	RSA PKCS1-v1.5[26] digital signature generation primitive	2048	Digital signature generation
			NIST SP 800-135rev1	TLS 1.0/1.1 and 1.2	-	Application-specific Key derivation
-	A1112	CVL	*NIST SP 800-135rev1*	SNMPv3[27]	-	Application-specific Key derivation

[18] AES – Advance Encryption Standard
[19] ECB – Electronic Codebook
[20] CBC – Cipher-Block Chaining
[21] CFB – Cipher Feedback
[22] CTR – Counter
[23] OFB – Output Feedback
[24] CKG – Cryptographic Key Generation
[25] CVL – Component Validation List
[26] PKCS1-v1.5 – Public Key Cryptography Standard #1 version 1.5
[27] SNMPv3 – Simple Network Management Protocol version 3

Certificate Number		Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
HW	FW					
-	A1111	DRBG[28]	*NIST SP 800-90Arev1*	CTR-based	256-bit AES	Deterministic random bit generation
-	A1111	ECDSA	*FIPS PUB 186-4*	-	P-224, P-256, P-384, P-521	Public key validation *Operationally, ECDSA public key validation is only used to support ECDH.*
				-	P-224, P-256, P-384, P-521	Key pair generation *Operationally, ECDSA key pair generation is only used to support ECDH.*
				SHA2-224, SHA2-256	P-224, P-256, P-384, P-521	Digital signature generation
				SHA2-224, SHA2-256	P-224, P-256, P-384, P-521	Digital signature verification
-	N/A	ENT (NP)[29]	*NIST SP 800-90B*	-	-	Non-deterministic random bit generation
-	A1111	HMAC[30]	*FIPS PUB 198-1*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	KS<BS, KS=BS, KS>BS	Message authentication
-	A1111	KAS-SSC[31]	*NIST SP 800-56Arev3*	ECC CDH[32]	P-224, P-256, P-384, P-521	Shared secret computation
				FFC DH[33]	MODP-2048, MODP-3072	Shared secret computation *Not used operationally*
-	A1111	KTS[34]	*NIST SP 800-38D*	AES-GCM	256	Key wrapping[35] (in TLS)
			FIPS PUB 197 *FIPS PUB 198-1*	AES with HMAC	-	Key wrapping[36] (in TLS)
A1113	-	KTS	*NIST SP 800-38D*	AES-GCM	256	Key wrapping[37] (in PCoIP)
-	A1111	PBKDF[38]	*NIST SP 800-132*	PBKDF2 Option 1a with HMAC SHA	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	Key derivation
-	A1111		*FIPS PUB 186-4*	-	2048	Key pair generation

[28] DBRG – Deterministic Random Bit Generator
[29] ENT (NP) – Entropy (Non-Physical)
[30] HMAC – Keyed-Hash Message Authentication Code
[31] KAS-SSC – Key Agreement Scheme - Shared Secret Computation
[32] ECC – Elliptic Curve Cryptography Cofactor Diffie-Hellman
[33] FFC DH – Finite Field Cryptography Diffie-Hellman
[34] KTS – Key Transport Scheme
[35] Per FIPS 140-2 IG D.9, AES-GCM is an Approved key wrapping technique.
[36] Per FIPS 140-2 IG D.9, AES with HMAC is an Approved key wrapping technique.
[37] Per FIPS 140-2 IG D.9, AES-GCM is an Approved key wrapping technique.
[38] PBKDF – Password-Based Key Derivation

Certificate Number		Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
HW	FW					
		RSA[39]		SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	2048, 3072, 4096	Digital signature verification
-	A1111	Safe Primes	-	-	MODP-2048, MODP-3072	Key generation *Not used operationally*
				-	MODP-2048, MODP-3072	Key verification *Not used operationally*
-	A2048	SHA-3[40]	*FIPS PUB 202*	SHA3-256	-	Message digest
-	A1111	SHS[41]	*FIPS PUB 180-4*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	-	Message digest

***NOTE**: No parts of the SNMP and TLS protocols, other than the KDFs[42], have been tested by the CAVP[43] or CMVP.*

The vendor affirms the following cryptographic security method(s):

- Cryptographic key generation – Per *NIST SP 800-133rev2*, the module uses the FIPS-Approved counter-based DRBG specified in *NIST SP 800-90Arev1* to generate cryptographic keys. The resulting symmetric key or generated seed is an unmodified output from the DRBG. The module's DRBG is seeded via a CPU jitter-based entropy source (jent 3.3) internal to the module.

The module implements the non-Approved but allowed algorithms shown in Table 5.

[39] RSA – Rivest Shamir Adleman
[40] SHA – Secure Hash Algorithm
[41] SHS – Secure Hash Standard
[42] KDF – Key Derivation Function
[43] CAVP – Cryptographic Algorithm Validation Program

Table 5 – Allowed Algorithms

Algorithm	Caveat	Use
MD5[44]	No security is claimed on this function	Used during TLS 1.1 protocol handshake (is redundant to an approved cryptographic algorithm) *Allowed per FIPS140-2 IG 1.23*
2048-bit RSA encrypt/decrypt (non-compliant)	No security is claimed on this function	Used only to obfuscate/un-obfuscate data and public keys for export/import in support of SCEP[45] *Allowed per FIPS140-2 IG 1.23*

2.2.2 Modes of Operation

The module supports two (2) Approved modes of operation:

- Mode 1 – This is the module's normal mode of operation and includes all of the module's documented services. This mode is implemented in the module's main firmware image. This image includes all requisite power-up and conditional self-tests.

- Mode 2 – This is the module's recovery mode of operation and includes a subset of the module's documented services. This mode is implemented in a special recovery firmware image. As is the case with the primary image, the recovery image includes all requisite power-up and conditional self-tests.

The module operator does not select which Approved mode to execute. Rather, selection of the Approved mode is based on the module's operational status. Upon initial power-up, the module will boot into Mode 1 by default. If the module encounters a power-up self-test failure, it will automatically attempt to reboot back into Mode 1. If a power-up self-test failure occurs on four (4) consecutive attempts, the module will then automatically boot into Mode 2. At each respective bootup, all required power-up self-tests for the active image are executed.

A switch to Mode 2 is a likely indication that the main firmware image is corrupted and will no longer operate. Here, the only way to again operate in Mode 1 is to upload a new main firmware image to the module (using the AWI or MC) and reboot from that image. Note that, in order to maintain this validation, only FIPS-validated firmware can be loaded.

See section 2.4.2 for a list of services available in each Approved mode of operation. When following all installation, configuration, and initialization guidance provided in this Security Policy, the module does not support a non-Approved mode of operation.

[44] MD5 – Message Digest 5
[45] SCEP – Simple Certificate Enrollment Protocol

2.3 Module Interfaces

While the module consists of a Tera2 ASIC and its connected NOR flash and DDR3 SDRAM memory devices, the module's external interfaces are provided only by the Tera2 ASIC. Each ASIC is packaged in a flip chip ball grid array (FCBGA) package. Each FCBGA package has one face covered with solder balls in a grid pattern which, in operation, conduct electrical signals between the integrated circuit and the printed circuit board (PCB) on which it is mounted. The TERA2140 (Figure 8) is packaged in an 896-ball FCBGA package, while the TERA2321 (Figure 9) is packaged in a 396-ball FCBGA package.

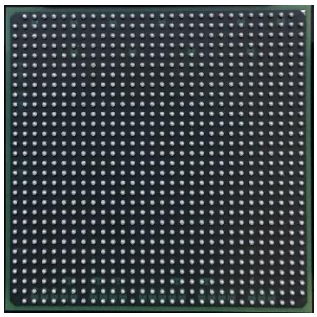


Figure 8 – TERA2140 896-Ball FCBGA

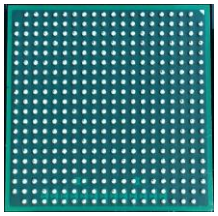


Figure 9 – TERA2321 396-Ball FCBGA

The module's design separates the physical interfaces into four logically distinct and isolated categories. The categories are:

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

The solder balls provide the contact points between the chip package and the printed circuit board (PCB). Each solder ball is responsible for carrying a specific signal, and defined groups of solder balls work together to create each of the module's distinct physical interfaces. Table 6 provides the mapping from those physical interfaces to the logical interfaces as defined by FIPS 140-2.

Table 6 – Physical-to-Logical Interface Mappings

Physical Interface	Quantity		FIPS 140-2 Logical Interface
	TERA2140	TERA2321	
Clock Controller	1	1	• Control In • Status Out
DDR3[46] Memory Controller + PHY	1	1	• N/A (internal interface to DDR3 memory device)
Ethernet System	1	1	• Data Input • Data Output • Control Input • Status Output
Low Speed Peripheral Controller	1	1	• N/A (internal interface to NOR flash device)
High-Definition Audio Controller	1	1	• Data Input • Data Output • Control Input • Status Output
USB 2.0 4-Port PHY	1	1	• Data Input • Data Output • Control Input • Status Output
Dual Display Port/DVI PHY	2	1	• Data Input • Data Output • Control Input • Status Output
Video Digital-to-Analog Converter	-	1	• Data Input • Data Output • Control Input • Status Output
Power/Ground	1	1	• Power Input

***NOTE**: The TERA2140 and TERA2321 also includes a JTAG[47] interface. However, this interface is only available when the module is executing with a development build; it is disabled in release firmware builds during normal operation. The TERA2321 also includes a Test & Control interface. However, this interface is used for manufacturing test purposes; it is not used in a client/server solution or production environment.*

2.4 Roles, Services, and Authentication

The sections below describe the module's roles and services.

2.4.1 Authorized Roles

As required by FIPS 140-2, the module supports two authorized roles that operators may assume: Crypto Officer (CO) and User. The module supports multiple concurrent operators with the following limitations:

[46] DDR – Double Data Rate
[47] JTAG – Joint Test Action Group

- Only one operator at a time can access the module using the OSD.
- Only one operator session at a time is supported on the AWI. If a second operator logs in from another browser, the first operator's session is terminated.
- Multiple operators can access the module concurrently using a single MC instance.

Any authorized operator that accesses the module via one of its operator interfaces assumes the set of roles consisting of the CO role and the User role, and thus has access to all available CO and User services.

2.4.2 Module Services

Descriptions of the services available to authorized operators in Mode 1 and Mode 2 are provided in Table 7. The type of access required for the keys and CSPs listed in these tables is indicated 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.

Table 7 – Authorized Operator Services

Service	Mode		Description	Input	Output	CSP and Type of Access
	1	2				
Initiate PCoIP session	✓		(OSD, AWI) Create a PCoIP session between the client and a remote resource	Command	None	PCoIP Encrypt Key – W/X PCoIP Decrypt Key – W/X ZC Public Key – R/X ZC Private Key – R/X P2P Client Suite B Public Key– R/X P2P Client Suite B Private Key – R/X P2P CA Public Key – X P2P CA Private Key – X AES-GCM IV – R/W/X ECDH Public Key – W/X ECDH Private Key – W/X TLS Server Public Key – R/X TLS Pre-Master Secret – W/X TLS Master Secret – W/X TLS Session Key – R/W/X TLS Authentication Key – W/X

Service	Mode		Description	Input	Output	CSP and Type of Access
	1	2				
Initiate TLS session	✓	✓	(OSD, AWI, MC) Initiate a TLS session (non-PCoIP sessions)	Command	None	AES-GCM IV – R/W/X ECDH Public Key – R/X ECDH Private Key – X TLS Server Public Key – R/X TLS Pre-Master Secret – W/X TLS Master Secret – W/X TLS Session Key – R/W/X TLS Authentication Key – W/X
Configure initial settings	✓		(AWI) Configure the client's initial audio, network, and session information	Command and parameters	None	None
Configure network settings	✓	✓	(OSD, AWI, MC) Change IPv4 network settings for the device	Command and parameters	None	None
Configure IPv6 settings	✓	✓	(OSD, AWI) Change IPv6 network settings for the device	Command and parameters	None	None
Clear management settings	✓	✓	(OSD, AWI) View or clear the zero client's management settings	Command and parameters	Command response	None
Manage management settings	✓		(AWI) View, configure, or clear the zero client's management settings	Command and parameters	Command response	None
Configure SCEP[48] settings	✓		(OSD, AWI, MC) Configure SCEP settings	Command and parameters	None	None
Request certificate	✓		(OSD, AWI) Request endpoint certificate from SCEP server	Command and parameters	None	802.1x Client Public Key – W/X 802.1x Client Private Key – W/X SCEP "Verify" Public Key – R/X SCEP "Obfuscate" Public Key – R/X
Configure device label	✓		(OSD, AWI) Manage the device identification information	Command and parameters	None	None
Manage discovery settings	✓		(OSD) Enable/disable device discovery (AWI, MC) Enable/disable device discovery; manage settings for device discovery	Command and parameters	None	None

[48] SCEP – Simple Certificate Enrollment Protocol

Service	Mode		Description	Input	Output	CSP and Type of Access
	1	2				
Configure session settings	✓		(OSD, AWI, MC) Configure settings for PCoIP connections to a peer device	Command and parameters	None	None
Configure power settings	✓		(OSD, AWI, MC) Set/change timeout and power settings for the client	Command and parameters	None	None
Configure display settings	✓		(OSD – TERA2140) Configure display resolution for attached monitors (OSD – TERA2321) Configure display resolution and display cloning for attached monitors	Command and parameters	None	None
Configure access settings	✓		(OSD, AWI, MC) Configure the administrative access settings	Command and parameters	None	None
Configure audio settings	✓		(OSD, AWI, MC) Select audio input and output devices	Command and parameters	None	None
Reset	✓	✓	(OSD, AWI, MC) Reset all configuration and permissions settings stored on the devices; zeroize CSPs stored in flash	Command	None	802.1x Client Public Key – W 802.1x Client Private Key – W 802.1x Peer Public Key – W ZC Public Key – W Root CA Public Key – W P2P Client Suite B Public Key– W P2P Client Suite B Private Key – W SCEP “Verify” Public Key – W SCEP “Obfuscate” Public Key – W Admin Password – W
Configure USB settings and permissions	✓		(AWI, MC) Configure USB settings and permissions	Command and parameters	None	None
Configure SNMP settings	✓		(AWI, MC) Enable or disable the device’s SNMP agent	Command and parameters	None	None
Configure session bandwidth	✓		(AWI, MC) Configure the client bandwidth limit, target, and floor used during a PCoIP session	Command and parameters	None	None
Configure time settings	✓		(AWI, MC) Set the time zone; configure Network Time Protocol parameters; enable Daylight Savings Time	Command and parameters	None	None

Service	Mode		Description	Input	Output	CSP and Type of Access
	1	2				
Enable/disable event log	✓	✓	(AWI, MC) Enable or disable the event log	Command and parameters	None	None
View event log	✓	✓	(OSD, AWI) View, refresh, or clear event log messages	Command and parameters	Command response	None
Enable/disable syslog	✓		(AWI, MC) Enable or disable syslog	Command and parameters	None	None
View session statistics	✓		(OSD) View session statistics from the previous session (AWI) View session statistics from the previous session; view/reset session statistics from a live session	Command	Command response	None
View processor statistics	✓		(OSD) View PCoIP processor statistics (AWI) View PCoIP processor statistics; reset PCoIP processor	Command	Command response	None
View boot time	✓	✓	(OSD, AWI in Mode 1; AWI in Mode 2) View the processor uptime since boot	Command	Command response	None
Ping host	✓		(OSD) Ping a host across the IP network	Command	Command response	None
Display client information	✓	✓	(OSD, AWI, MC) View the device hardware/firmware version information and IP address	Command	Command response	None
Configure certificate checking mode	✓		(OSD, AWI, MC) Configure the client's certificate checking mode	Command and parameters	None	None
Adjust mouse speed	✓		(OSD) Adjust the mouse cursor speed	Command and parameters	None	None
Adjust keyboard settings	✓		(OSD) Adjust the keyboard character repeat and delay settings	Command and parameters	None	None
Adjust image quality	✓		(OSD, AWI, MC) Adjust the image quality	Command and parameters	None	None

Service	Mode		Description	Input	Output	CSP and Type of Access
	1	2				
Configure display topology	✓		(OSD, MC) Set the layout and alignment of the displays; configure the position, rotation, and resolution for each display	Command and parameters	None	None
Configure touch screen settings	✓		(OSD) Configure the touch screen settings for attached touch-enabled displays	Command and parameters	None	None
Configure tablet/display mapping	✓		(OSD) Configure the mapping between displays and attached tablets	Command and parameters	None	None
Configure region settings	✓		(OSD) Configure time zone, keyboard, and language for the client (AWI, MC) Configure keyboard and language for the client	Command and parameters	None	None
Configure the OSD interface settings	✓		(OSD, MC) Enable/disable the OSD's low light color palette	Command and parameters	None	None
Change password	✓	✓	(OSD, AWI, MC) Update the local administrative password for the client	Command and parameters	None	Admin Password – W
Reset password	✓	✓	(OSD, MC) Reset the client administrative password	Command	None	Admin Password – W
Load firmware	✓	✓	(AWI, MC) Load new firmware to the client	Command and parameters	None	Firmware Load Key – R/X
Load /display OSD logo	✓		(AWI, MC) Load an image to display on the OSD "Connect" page; set image for display on OSD login screens	Command and parameters	None	None
Load certificate	✓	✓	(AWI, MC) Load and manage root CA[49] and client certificates	Command and parameters	None	802.1x Client Public Key – R 802.1x Client Private Key – R P2P Client Suite B Public Key – R P2P Client Suite B Private Key – R TLS Server Public Key – R Root CA Public Key – R

[49] CA – Certificate Authority

Service	Mode		Description	Input	Output	CSP and Type of Access
	1	2				
Configure display override settings	✓		(OSD, MC) Configure display override settings	Command and parameters	None	None
Test audio	✓		(AWI) Generate an audio test tone from the client	Command and parameters	Command response	None
Test attached displays	✓		(AWI) Initiate and view a visual test pattern on the client's attached displays	Command and parameters	Command response	None
Capture packets	✓		(AWI) Capture non-PCoIP network traffic packets on the client	Command and parameters	Command response	None
Manage password protection	✓	✓	(MC) Enable/disable password protection on the client (Mode 2 allows the current setting to only be viewed)	Command and parameters	Command response	None
View attached devices	✓		(AWI) View information for presently connected monitors and USB devices	Command	None	None
View open source licenses	✓		(AWI) View licenses for client's open source components	Command	None	None

Note that the MC offers several services for modifying the configuration of the module. These services are available via the MC when the module is operating in either Mode 1 or Mode 2. However, settings that are modified via the MC while the module is operating in Mode 2 are not pushed to the module for application until the module successfully reboots into Mode 1.

The module offers operators additional services that do not require assumption of an authorized role. These additional services, described in Table 8 below, do not modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the security of the module.

Table 8 – Additional Services

Service	Mode		Description	Input	Output	CSP and Type of Access
	1	2				
Authenticate[50]	✓	✓	Log in to the module	Command	Module access	Admin Password – R/X Smart Card Authentication Signing Key – R/X
Perform self-tests	✓	✓	Perform power-up self-tests on demand	Power cycle the client	Status output	None
Zeroize	✓	✓	Zeroize keys and CSPs	Power cycle the client	Status output	Keys/CSPs in volatile memory – W

2.4.3 Authentication

The Tera2 PCoIP Zero Client Processors are sold to third-party OEMs[51] for installation into their own Zero Client endpoint devices. While the module supports role-based authentication, the OEMs have the option of disabling password protection prior to delivery of the endpoint device to the end-user. Thus, while some deployment of the module will have authentication enabled, no security claims are being made regarding the module's authentication mechanisms (as allowed at level 1), and all requirements regarding authentication are thus out of scope.

In all cases, module operators accessing the module via any one of its operator interfaces implicitly and automatically assume the set of roles consisting of the CO role and the User role.

2.5 Physical Security

The cryptographic module is a multiple-chip embedded cryptographic module consisting of production-grade components and standard IC packaging material.

2.6 Operational Environment

The operational environment of the module does not provide the module operator with access to a general-purpose operating system (OS). The module employs a non-modifiable operating environment. The firmware integrity test protects against unauthorized modification of the module.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 9.

[50] The "Authenticate" service is only applicable to modules deployed with authentication enabled.
[51] OEM – Original Equipment Manufacturer

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

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization[52]	Use
ECDH Public Key	ECDH public key (P-224, P-256, P-384, P-521 curves)	[for the module] Generated internally via FIPS-Approved DRBG [for a peer] Generated externally, entered into the module during TLS handshake in plaintext form	[for the module] Exits the module during TLS handshake in plaintext form [for a peer] Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Generation of shared secret for TLS sessions in ECDH-based cipher suites
ECDH Private Key	ECDH private key (P-224, P-256, P-384, P-521 curves)	Generated internally via FIPS-Approved DRBG	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Generation of shared secret for TLS sessions in ECDH-based cipher suites
802.1x Client Public Key	2048/3072-bit RSA public key	Generated internally via FIPS-Approved DRBG	Exits the module via digital certificate in plaintext form	Stored in flash memory in plaintext form	"Reset" service	Certificate-based authentication of client for 802.1x communications
802.1x Client Private Key	2048/3072-bit RSA private key	Generated internally via FIPS-Approved DRBG	Never exits the module	Resides in flash memory in plaintext form	"Reset" service	Certificate-based authentication of client for 802.1x communications; un-obfuscation of SCEP messages
802.1x Peer Public Key	2048/3072/4096-bit RSA public key	Generated externally, imported in a certificate in plaintext form	Never exits the module	Stored in flash memory in plaintext form	"Reset" service	Certificate-based authentication of peer for 802.1x communications
SNMP Session Key	128-bit AES-CFB key	Derived internally via SNMP KDF using operator-entered passphrase	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Encryption of SNMP data packets
SNMP Authentication Key	160-bit HMAC key	Derived internally via SNMP KDF using operator-entered passphrase	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Authentication of SNMP data packets

[52] All CSPs with "N/A" in the **Zeroization** column are either public keys in plaintext form or secret/private keys in encrypted form.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization[52]	Use
ZC Public Key	3072-bit RSA public key	Generated externally, hardcoded in the module firmware in encrypted form	Exits the module in plaintext form	Stored in flash memory in encrypted form (256-bit AES-CBC)	"Reset" service	Verification of signatures for certificate-based authentication when the module acts as the server (for AWI connections; for MC Endpoint Discovery; and for direct-to-host PCoIP sessions over TLS)
ZC Private Key	3072-bit RSA private key	Generated externally, hardcoded in the module firmware in encrypted form	Never exits the module	Stored in flash memory in encrypted form (256-bit AES-CBC)	N/A	Generation of signatures for certificate -based authentication when the module acts as the server (for AWI connections; for MC Endpoint Discovery; and for direct-to-host PCoIP sessions over TLS)
Root CA Public Key	2048/3072-bit RSA public key P-384 curve ECDSA public key	Generated externally, imported in a certificate in plaintext form	Never exits the module	Resides in flash memory in plaintext form	"Reset" service	Certificate-based authentication for TLS connections
TLS Server Public Key	2048-bit (minimum) RSA public key	Generated externally, imported in a certificate in plaintext form	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Certificate-based authentication for TLS connections
TLS Pre-Master Secret	ECDH shared secret	Derived internally via ECDH shared secret computation	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Derivation of the TLS Master Secret
TLS Master Secret	384-bit shared secret	Derived internally using the TLS Pre-Master Secret via TLS KDF	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Derivation of the TLS Session Key and TLS Authentication Key
TLS Session Key	128/256-bit AES-CBC key 128/256-bit AES-GCM key	Derived internally via TLS KDF	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Encryption of TLS data packets
TLS Authentication Key	256-bit HMAC key	Derived internally via TLS KDF	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Authentication of TLS data packets

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization[52]	Use
PCoIP Encrypt Key	256-bit AES-GCM key	Generated internally via FIPS-Approved DRBG	Exits the module in ciphertext during PCoIP session negotiation over TLS	Resides in volatile memory in plaintext form	Cycle power	Encryption of transmitted PCoIP session data packets
PCoIP Decrypt Key	256-bit AES-GCM key	Generated externally, imported in ciphertext during PCoIP session negotiation over TLS	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Decryption of received PCoIP session data packets
P2P Client Suite B Public Key	P-384 ECDSA public key	[for default certificate] Generated externally, hardcoded in the module firmware in encrypted form [for custom certificates] Generated externally, imported in encrypted form over TLS	Exits the module in plaintext form during TLS negotiation	[for default certificate] Stored in flash memory in encrypted form (256-bit AES-CBC) [for custom certificate] Stored in flash memory in plaintext form	[for default certificate] N/A [for custom certificate] "Reset" service	Verification of signatures for certificate-based authentication in direct-to-host PCoIP sessions over TLS for Suite B compliant PCoIP connections
P2P Client Suite B Private Key	P-384 ECDSA private key	[for default certificate] Generated externally, hardcoded in the module firmware in encrypted form [for custom certificates] Generated externally, imported in encrypted form over TLS	Never exits the module	[for default certificate] Stored in flash memory in encrypted form (256-bit AES-CBC) [for custom certificate] Stored in flash memory in plaintext form	[for default certificate] N/A [for custom certificate] "Reset" service	Generation of signatures for certificate-based authentication in direct-to-host PCoIP sessions over TLS for Suite B compliant PCoIP connections
P2P CA Public Key	[for normal PCoIP connections] 2048-bit RSA key [for Suite B compliant PCoIP connections] P-384 ECDSA key	Generated externally, hardcoded in the module firmware in encrypted form	Never exits the module	Stored in flash memory in plaintext form	N/A	Verification of signatures for authentication in direct-to-host PCoIP sessions over TLS

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization[52]	Use
P2P CA Private Key	[for normal PCoIP connections] 2048-bit RSA key [for Suite B compliant PCoIP connections] P-384 ECDSA key	Generated externally, hardcoded in the module firmware in encrypted form	Never exits the module	Stored in flash memory in encrypted form (256-bit AES-CBC)	N/A	Generation of signatures for authentication in direct-to-host PCoIP sessions over TLS
P2P Key Protection Key	256-bit AES-CBC key	Derived internally using FIPS-Approved PBKDF	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Decryption of: • ZC Public Key • ZC Private Key • P2P Client Suite B Public Key • P2P Client Suite B Private Key • P2P CA Private Key • Smart Card Authentication Signing Key
SCEP "Verify" Public Key	2048-bit (minimum) RSA key	Generated externally, imported in plaintext form over HTTP	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Verification of signatures on SCEP messages
SCEP "Obfuscate" Public Key	2048-bit (minimum) RSA key	Generated externally, imported in plaintext form over HTTP	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Obfuscation of SCEP messages
Smart Card Authentication Signing Key[53]	P-256 ECDSA private key	Generated externally, imported in encrypted form over TLS	Never exits the module	Stored in flash memory in encrypted form (256-bit AES-CBC)	N/A	Authentication of MD 830 smart cards
Admin Password[54]	Password (14-byte minimum)	Entered in plaintext form	Never exits the module	Resides in flash memory in hashed form (SHA2-256)	"Reset" service; "Reset password" service	Enables the CO or User role
DRBG Entropy[55]	Random data – 256 bits	Generated internally	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Entropy material for CTR_DRBG

[53] The Smart Card Authentication Signing Key is only applicable to modules deployed with authentication enabled.
[54] The Admin Password is only applicable to modules deployed with authentication enabled.
[55] The module generates a minimum of 384 bits of entropy per each 384-bit request for use in key generation.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization[52]	Use
DRBG Seed	Random data – 384 bits	Generated internally	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Seeding material for CTR_DRBG
DRBG 'V' Value	Internal state value	Generated internally	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Internal state value for CTR_DRBG
DRBG 'Key' Value	Internal state value	Generated internally	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	Internal state value for CTR_DRBG
AES GCM IV[56]	96-bit IV	Generated internally deterministically	Never exits the module	Resides in volatile memory in plaintext form	Cycle power	IV for AES-GCM
Firmware Load Key	P-384 ECDSA public key	Generated externally, hardcoded in the module firmware in plaintext form	Never exits the module	Stored in flash memory in plaintext form	N/A	Verification of loaded firmware images

[56] IV – Initialization Vector

The AES-GCM IV[57] is constructed by the module using the following methods:

- When used with the TLS protocol – The AES-GCM IV is generated deterministically (external to the AES-GCM implementation but internal to the module boundary) in compliance with TLS v1.2 GCM cipher suites as specified in *RFC 5288* and section 8.2.1 *of NIST SP 800-38D*. When the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, the module stops encrypting data and the TLS session is terminated.

- When used with PCoIP protocol – The AES-GCM IV is constructed at its entirety deterministically (external to the AES-GCM implementation but internal to the module boundary) in accordance with section 8.2.1 of *NIST SP 800-38D*. The IV length is 96 bits, including a 32-bit name field (in the form of a salt value) and a 64-bit non-repetitive counter field (implemented using a linear feedback shift register). Four bits of the 64-bit counter field are set to '0', while the remaining 60 bits are incremented. When the 60-bit counter exhausts the maximum number of possible values for a given session key, the module will terminate the PCoIP session. The module operator will then need to trigger a new session negotiation, thus establishing a new encryption key.

2.8 EMI / EMC

According to 47 Code of Federal Regulations (CFR), Part 15, Subpart B, Unintentional Radiators, the module is not subject to EMI/EMC regulations because it is considered a subassembly. Per CFR 47:

> "*Subassemblies to digital devices are not subject to the technical standards in this part unless they are marketed as part of a system in which case the resulting system must comply with the applicable regulations.*"

The module is sold directly to equipment manufacturers to be embedded within that manufacturers' systems. The equipment manufacturers for the resulting systems are responsible for obtaining the necessary authorization for the equipment with the module embedded prior to further marketing to a vendor or to a user.

2.9 Self-Tests

Cryptographic self-tests are performed by the module when the module is first powered up and when operational parameters dictate. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

2.9.1 Power-Up Self-Tests

The module performs the following self-tests at power-up to verify the integrity of the firmware image and the correct operation of the FIPS-Approved algorithm implementations:

- Firmware integrity check using an Error Detection Code (a 32-bit FNV-1a[58] hash)
- Algorithm tests

[57] IV – Initialization Vector
[58] FNV – Fowler-Noll-Vo

- Hardware
  - 256-bit AES (GCM) encrypt and decrypt KATs[59]
- Firmware
  - 256-bit AES (CBC, CTR, ECB, OFB, GCM) encrypt and decrypt KATs
  - 128-bit AES (CFB128) encrypt and decrypt KATs
  - SHA KATs (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)
  - HMAC KATs (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)
  - P-224 curve ECDSA sign/verify PCT[60]
  - 2048-bit RSA sign/verify KAT
  - 256-bit AES-CTR DRBG KAT
  - ECC CDH Primitive "Z" computation test
  - PBKDF KAT

The module's SHA3-256 implementation is used solely in a conditioning component of an entropy generation process. Thus, per FIPS 140-2 IG 7.18, a SHA3-256 power-up KAT is not mandatory.

2.9.2 Conditional Self-Tests

The module performs the following conditional self-tests:

- Stuck Test on entropy source
- Repetition Count Test on entropy source
- Adaptive Proportion Test on entropy source
- RSA sign/verify PCT
- ECDSA PCT
- Firmware load test (ECDSA digital signature with curve P-384 and SHA-384)

The RCT and APT are also performed on 1024 consecutive noise source samples at module power-up.

2.9.3 Critical Functions Tests

The module performs health checks for the DRBG's Generate, Instantiate, and Reseed functions as specified in section 11.3 of *NIST SP 800-90Arev1*. These health tests are performed at module power-up.

The module performs all applicable assurances for its key agreement schemes as specified in section 9 of *NIST SP 800-56Arev3*. The module also performs a developer-defined Lag Prediction Test on its entropy source as described in *NIST SP 800-90B*. These tests are performed conditionally.

2.9.4 Self-Test Failures

Upon failure of a power-up, conditional, or critical functions test, the module will enter an error state as follows:

[59] KAT – Known Answer Test
[60] PCT – Pairwise Consistency Test

- As a result of a failed conditional firmware load test in Mode 1 or Mode 2, the module will enter a soft error state. In this state, the module first logs the error to a log file that is accessible to the Zero Client device operator. Once the error is logged, the module will abort the load process, clear the error condition, and continue executing using the already-loaded firmware image.

- As a result of any other self-test error while running in Mode 1, the module will enter a critical error state. In this state, the module first logs the error to a log file that is accessible to the Zero Client device operator. Once the error is logged, the module will automatically attempt a reboot back into Mode 1, clearing the error condition.

  For each failure experienced during Mode 1 bootup, the module will increment a counter that tallies the boot failures; a successful boot will reset the counter to 0. If four (4) boot failures are tallied without a counter reset, the module will then attempt to boot into Mode 2 using the recovery image.

- As a result of any other self-test error while running in Mode 2, the module enters a critical error state. In this state, the module will first log the error to a log file that is accessible to the Zero Client device operator. Once the error is logged, the module will automatically attempt a reboot back into Mode 2, clearing the error condition.

  A non-recoverable failure experienced during bootup in Mode 2 will cause the module will repeatedly attempt to reboot into Mode 2, effectively rendering the module non-operational. The CO will need to contact HP customer support for assistance.

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3. Secure Operation

The Tera2 PCoIP Zero Client Processors meet Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in the FIPS-Approved mode of operation. **Any operation of the module without following the guidance provided below will result in non-compliant use and is outside the scope of this Security Policy.**

3.1 Initial Setup

The module is pre-installed in PCoIP Zero Client devices in an unconfigured state prior to delivery to end-users. Before using the Zero Client, the CO must perform general initial setup and configuration steps to set the audio, network, and session parameters. These steps may be performed using the AWI or MC interfaces. Additionally, the CO can define which of the module interfaces (OSD, AWI, and MC) is allowed administrative access to the module. Note that at least one of the PCoIP ZC administrative configuration interfaces must remain enabled at all times.

The module requires no additional setup steps for FIPS operation (for modules that deploy with authentication mechanisms enabled, it is recommended that module operators change the default password at first boot). Once setup is complete, the module will be in FIPS-Approved mode.

Guidance on setting administrative access and configuring general settings can be found in HP's *PCoIP® Zero Client Firmware Administrators' Guide*.

3.2 Operator Guidance

This section provides guidance for Crypto Officers and Users for the management of the cryptographic module.

3.2.1 Monitoring Status

As stated in section 2.2.2, the module supports two Approved modes of operation. Further, when following all installation, configuration, and initialization guidance provided in this Security Policy, the module does not support a non-Approved mode of operation. Thus, the module is always running in an Approved mode.

To verify that the FIPS-validated version of the module is being used, module operators can use the following methods:

- While operating in Mode 1 – Confirm that the module version shown using the "Display Client Information" service (available via the OSD, AWI, or MC interface) is **21.01.5-fips**. The firmware build ID will begin with **client-21.01**.

- While operating in Mode 2 – Confirm that the module version shown using the "Display Client Information" service (available via the OSD, AWI, or MC interface) is **1.67.0** (executing this service in Mode 2 will display the version for the module's recovery firmware image only, which is a component of the overall module package identified by **21.01.5-fips**.) The firmware build ID will begin with **release/fips-21.01**.

Additionally, module operators shall monitor the module's status by regularly checking the event log. If the operator notices any irregular activity or module errors, then HP customer support should be contacted.

3.2.2 Loading Firmware

Module operators can load new firmware to a single instance of the module installed on an endpoint using AWI, or to multiple instances installed on across multiple endpoints using the MC interface. In order to maintain compliance, only FIPS-validated firmware shall be loaded onto the module hardware.

- To load a firmware image onto an individual endpoint using the AWI:

    1. Enter the endpoint's IP address in your browser's address bar and then log in to its AWI.
    2. Select the **Upload > Firmware** menu.
    3. From the "Firmware Upload" page, browse to the folder containing the firmware file. This file will have a `.all` extension.
    4. Double-click the "*.all" firmware file and then click **Upload**.
    5. Click **OK** to confirm that you want to proceed with the load.
    6. Click **Reset**.
    7. Click **OK**.

    This information is also available in the *HP PCoIP Zero Client Firmware Administrator's Guide*.

- To load a new firmware image onto multiple endpoints using MC:

    1. Ensure that the endpoints you wish to update are placed in their own group.
    2. From the MC home page, click **Update Firmware**.
    3. Click the **Import Firmware** link to transfer the firmware file from your host machine to the MC virtual machine.
    4. Click **Browse**, locate the combined firmware file, and then click **Open**. This file will have a `.pcoip` extension.
    5. Click **Import Now** to transfer the firmware file from your host machine to the MC virtual machine.
    6. Click the **Update Devices** link.
    7. Click **View Devices to Update**.
    8. Select the endpoints you wish to update, choose the desired endpoint restart and schedule options, and then click **Schedule Update**.
    9. If desired, click **View Status** to watch the update status of the endpoints.

    This information is also available in the *HP PCoIP Management Console Administrator's Guide*.

The newly loaded firmware will become the active firmware at the module's next reboot.

3.2.3 Resetting Parameters

From the OSD and AWI, module operators can reset parameters to the factory default values stored in flash memory. To reset parameters, follow these steps:

1. Open the Reset page.
   - From the OSD, navigate to **Options > Configuration > Reset**.
   - From the AWI, navigate to **Configuration > Reset**.
2. Click **Reset** and confirm when prompted.

3.3 Additional Guidance and Usage Policies

The following is a list of policies that must be followed by module operators as well as additional guidance for general module operation.

- All keys and CSPs residing in volatile memory can be zeroized on demand by cycling power to the module. Keys and CSPs residing in flash memory are zeroized via the “Reset” service.

- The module’s power-up self-tests can be initiated on demand by removing and re-applying power to the module.

- In the event that the module’s power is lost and then restored, a new key for use with the AES-GCM encryption shall be established.

4. Acronyms and Abbreviations

Table 10 below provides definitions for the acronyms and abbreviations used in this document.

Table 10 – Acronyms

Term	Definition
AES	Advanced Encryption Standard
AMI	Amazon Machine Image
ASCII	American Standard Code for Information Interchange
ASIC	Application-Specific Integrated Circuit
AWI	Administrative Web Interface
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CFB	Cipher Feedback
CFR	Code of Federal Regulations
CKG	Cryptographic Key Generation
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DDR	Double Data Rate
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DVI	Digital Visual Interface
EC2	Elastic Compute Cloud
ECB	Electronic Codebook
ECDH	Elliptic Curve Diffie Hellman
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie Hellman
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ENT (NP)	Entropy (Non-Physical)
ESP	Encapsulating Security Payload
FCBGA	Flip Chip Ball Grid Array

FFC DH	Finite Field Cryptography Diffie-Hellman
FIPS	Federal Information Processing Standard
FNV	Fowler-Noll-Vo
GCM	Galois Counter Mode
GUI	Graphical User Interface
HMAC	(keyed-) Hash-based Message Authentication Code
IP	Internet Protocol
IT	Information Technology
IV	Initialization Vector
JTAG	Joint Test Action Group
KAS-SSC	Key Agreement Scheme - Shared Secret Computation
KAT	Known Answer Test
KDF	Key Derivation Function
KTS	Key Transport Scheme
LDAP	Lightweight Directory Access Protocol
MC	Management Console
MD5	Message Digest 5
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OS	Operating System
OSD	On-Screen Display
OVA	Open Virtual Appliance
PBKDF	Password-Based Key Derivation Function
PC	Personal Computer
PCB	Printed Circuit Board
PCT	Pairwise Consistency Test
PCoIP	Personal Computer over Internet Protocol
PKCS	Public Key Cryptography Standard
RFC	Request for Comments
RSA	Rivest Shamir Adleman
RSA-OAEP	RSA with Optimal Asymmetric Encryption Padding
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SNMPv3	Simple Network Management Protocol version 3
SP	Special Publication
SSH	Secure Shell

TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
ZC	Zero Client

Prepared by:

Corsec Security, Inc.

12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

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