Caymas Systems, Inc.

Caymas 318 and Caymas 525 Identity-Driven Access Gateways

(Firmware version: R2.6.0, Hardware Version: 318 Rev 100-000001, 525 Rev 100-000002)

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation
Version 0.43

August 2005

Table of Contents

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Caymas 318 and 525 Identity-Driven Access Gateways from Caymas Systems, Inc. This Security Policy describes how the Caymas 318 and 525 Identity-Driven Access Gateways meet the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. 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) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/cryptval/.

The Caymas 318 and 525 Identity-Driven Access Gateways are referred to in this document as the 318 and 525, the gateways, or the modules.

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 Caymas Systems, Inc. website (http://www.caymas.com/) contains information on the full line of products from Caymas Systems, Inc..

- The CMVP website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

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 Machine
  - Other supporting documentation as additional references

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

CAYMAS SYSTEMS 318 AND 525 IDENTITY-DRIVEN ACCESS GATEWAYS

Overview

Caymas Systems enables, controls, and secures the extended enterprise with the world's first Identity-Driven Access Gateways. Caymas solutions allow enterprises, government agencies, and institutions to securely extend their information assets to remote employees, customers, partners and suppliers. Caymas solutions integrate third generation remote access, secure extranets and wire speed internal access control, allowing businesses to identify, authorize, protect and audit users and resources.

Caymas gateways are targeted at enterprises that have a business imperative to provide controlled access to their information resources, including Microsoft Windows® and Unix® file systems, web-enabled applications, web services applications, Intranet Mail systems, and client-server applications.

The Caymas 318 and 525 Identity-Driven Access Gateways provide identity-driven access to company resources while blocking unwanted and unauthorized activity at the application level. The devices can be configured to implement:

- *3rd Generation Remote Access* for businesses that must provide anywhere, anytime access for remote and mobile employees without the burden of a network-based VPN solution.

- *Secure Extranets* for enterprises that need to provide quick and secure access for their suppliers, business partners and customers without the expense of cumbersome access management software or software-intensive extranet solutions.

- *Wire Speed Internal Access Control* for enterprises that need to protect their Intranet and LAN-based resources from internal and external attack without continuous re-patching of the servers or the deployment of expensive application firewalls.

Module Specification

The Caymas Systems 318 and 525 are multi-chip standalone modules that meet all level 2 FIPS 140-2 requirements. The 318 is a 1U rack-mountable server, and the 525 is a 2U rack-mountable service. Both devices are completely enclosed in a hard, opaque metal case with tamper-evident labels, and this case is defined as the cryptographic boundary of the modules.

Section	Section Title	Level
1	Cryptographic Module Specification	2
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
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Table 1 – Security Level Per FIPS 140-2 Section

Module Interfaces

Caymas Systems 525 and 318 provide specific physical ports that cross the cryptographic boundary of the devices, and these ports provide the only access to the module's services.

The 525 provides the following physical ports:

- Management port (10/100 Ethernet port - RJ45 connector) dedicated to management
    - The link LED (lower left corner of the (RJ45) Ethernet connectors) for each of the ports is only lit when the Ethernet port has an active link, and the act LED (lower left corner of the (RJ45) Ethernet connectors) blinks when traffic is flowing over the port.
- 4 LAN ports (Gigabit Ethernet ports - RJ45 connectors) for data path (redundant pairs) and optionally management

    - The link LED (lower left corner of the (RJ45) Ethernet connectors) for each of the ports is only lit when the Ethernet port has an active link, and the act LED (upper left corner of the (RJ45) Ethernet connectors) blinks when traffic is flowing over the port.

- 1 Serial port (RJ45 connector) for management
- 1 CDM (LCD display, status LEDs, buttons) panel for limited management
- 1 power button
- 2 power connectors
- 2 USB ports for high availability (HA) – management

The following is a list of the physical ports for the 318:

- 2 LAN ports (Gigabit Ethernet ports – RJ45 connectors) for data path and management
- The link LED (lower left corner of the (RJ45) Ethernet connectors) for each of the ports is only lit when the Ethernet port has an active link, and the act LED (upper left corner of the (RJ45) Ethernet connectors) blinks when traffic is flowing over the port.
- 1 Serial port for management
- 1 CDM (LCD display, status LEDs, buttons) panel for limited management
- 1 power button
- 1 power switch
- 1 power connector
- 2 USB ports for HA – management

The physical ports of the 318 and 525 are depicted in the following figures.

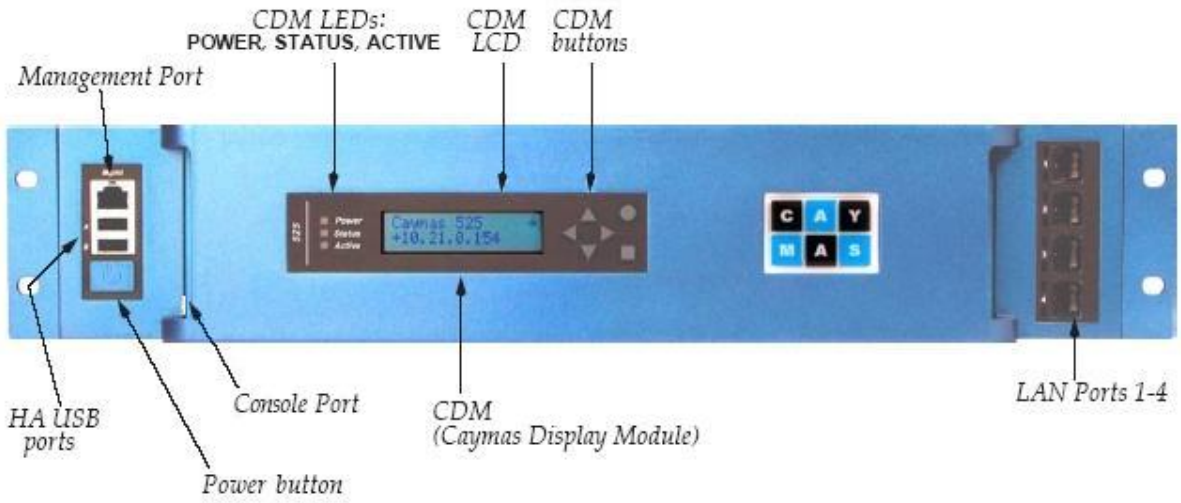

Figure 1 – 525 Front Physical Ports

Figure 2 – 525 Rear Physical Ports

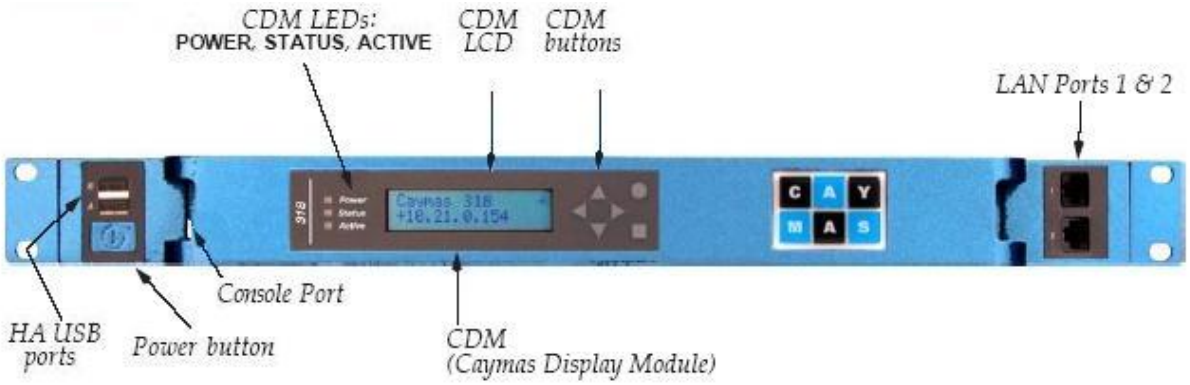

Figure 3 – 318 Front Physical Ports

Figure 4 – 318 Rear Physical Ports

The LEDs of the CDM indicate the following status.

LED Name	Color	Description
SYSTEM	Green	All diagnostics have passed and the system is operational.
	Orange (Amber)	Flashing: The system is booting and/or running diagnostics (normal initialization sequence).
	Red	The system is not operational because a fault has occurred during the initialization sequence.
	Off	No Power
STATUS	Green	No alarms.
	Orange (Amber)	Minor Alarm(s) are present on the system. Minor alarms need to be defined, but may include various chassis environmental, power supplies, and fan monitors.
	Red	Major or critical alarm(s) are present on the system.
	Off	No Power
ACTIVE	Green	The system is in Active mode.
	Orange (Amber)	The system is in Standby mode.
	Red	Active/Standby Failure, or Not Ready
	Off	Inactive

Table 2 – CDM Status Indicator LEDs

The physical ports of the 318 and 525 map to the logical interfaces of FIPS 140-2, as described in the following table.

525 Physical Port	318 Physical Port	FIPS 140-2 Logical Interface
Power connectors	Power connector	Power interface
10/100 BaseT Ethernet port (dedicated management)		Data input, data output, control input, status output
10/100/1000 BaseT Ethernet ports (LAN, WAN, management)	10/100/1000 BaseT Ethernet ports (LAN, WAN, management)	Data input, data output, Control input, status output
RJ45 serial port (CLI)	RJ45 serial port (CLI)	Control input, status output
USB ports	USB ports	Data input, data output
LEDs	LEDs	Status output
LCD	LCD	Status Output
LCD Buttons	LCD Buttons	Control input
Power Button	Power Button	Control input
	Hard power switch	Control input

Table 3 – Physical Ports and Logical Interfaces

Roles and Services

Caymas Systems 318 and 525 support three roles: a Crypto-Officer, a User, and a Network User. The module supports identity-based authentication.

Crypto Officer Role

The Crypto-Officer can manage the Caymas module over a TLSv1 session using CMS API calls through a software Graphical User Interface (GUI) application provided by Caymas called the Caymas Management System (CMS). Through this interface, the Crypto-Officer is able to configure Users of the device, load/generate key pairs, configure IPSec settings, and perform virtually all of the management of the module.

Additionally, Crypto-Officers can manage the box using a CLI over the locally connected serial port or remotely via SSHv2. The CLI contains a subset of the remote management functionality provided through the CMS API and some additional commands, most notably software upgrading.

Crypto-Officers can be defined with different subsets of functionality (user, system, superuser, monitor, security, user-defined), and these subsets are/can be configured with varying degrees of hide/read/write permissions for administrative functionality. Only the “admin” superuser is able to access the CLI.

Crypto-Officer service descriptions are provided in the table below.

Service	Description	Input	Output	CSP and Type of Access
Login	Authenticate the Crypto-Officer role, which can be on top of	Login information	Result of login attempt	Crypto-Officer password - Read

	authentication mechanism employed by cryptographic protocols.			
Logout	Log out the Crypto-Officer.	Logout call	Call response	
administer	Access administer level sub-commands.	Command	Status	
clear-known-hosts	Clear the database of known host keys.	Administer sub-command and parameters	Status	
dumpstate	Dump state information to log.	Administer sub-command and parameters	Status and state information	
file	File operation utilities.	Administer sub-command and parameters	Status information and file data	
ha	High Availability information and administration.	Administer sub-command, HA sub-commnds, if necessary, and parameters, including HA shared secret, if configuring	Status information	HA shared secret – Write
log	Log utility.	Administer sub-command and parameters	Status information	
reboot	Reboot the system.	Administer sub-command	Status	
release	Firmware upgrade.	Administer sub-command and parameters, including firmware release if uploading to box	Status information	Firmware upgrade public key – Read/Write
secpassword	Set boot password.	Administer sub-command and parameters, including a password (not a critical security parameter), if configuring	Status information	
show	Display administrator settings.	Administer sub-command	Status information	
shutdown	Power down of system.	Administer sub-command	Status	
sysfailaction	Set system failure action.	Administer sub-	Status	

		command and parameters		
timeout	Set the CLI idle timeout period.	Administer sub-command and parameters	Status	
userid	User configuration.	Administer sub-command, userid sub-command, if necessary, and parameters	Status information	
arp	Address resolution display and control	Sub-command and applicable parameters	Status information	
configure	General system configuration commands.	Command and parameters	Status information	
diagnostics	General system diagnostics.	Command and parameters	Status information	
exit	Exit from CLI interface.	Command	Status	
help	Display context sensitive help text.	Command and parameters	Status information	
ping	Send ICMP ECHO_REQUEST packets to network hosts.	Command and parameters	Status information	
quit	Exit from CLI interface.	Command	Status	
saveconfig	Save the current configuration database.	Command	Status	
show	Show system information.	Command and parameters	Status information	
top	Move to top-most level of command hierarchy.	Command	Status	
traceroute	Print the route packets take to a network host.	Command and parameters	Status information	
up	Move one level up the command hierarchy.	Command	Status	
Open CLI	Establish an SSH session and authenticate an operator with digital certificates, if configured.	SSH handshake parameters, SSH inputs	SSH outputs	SSH session keys - Read/Write DSA/RSA private keys - Read DSA/RSA public keys - Read/Write
Policy	Configure access control policies for Users, Web/File Resources, Applications, Machines, and Networks.	CMS API calls and configuration information, including User passwords, if configuring	Status information, including configured policies	User passwords – Read/Write
App Protection	Configure IDS rules for monitoring traffic	CMS API calls and configuration information	Status information, including configured policies	
Authentication	Configuration authentication	CMS API calls and	Status information,	

	policies, including password length and complexity restrictions	configuration information	including configured policies	
Configure Secure Connect	Configure Secure Connect functionality	CMS API calls and configuration information	Status information, including configured policies	
IPSec	Configure the IPSec services, including setting up whether to use IKE, what algorithms to support, what keys and certificates to use, etc.	CMS API calls and configuration information, including pre-shared keys and manually configured IPSec session keys, depending on configuration	Status information, including configured policies	Pre-shared keys – Write IPSec session keys - Write
Configure system settings	Configure the system settings, including generation of key pairs, configuring certificates, setting up SSL servers	CMS API calls and configuration information, including public keys, depending on configuration	Status information, including configured policies	RSA/DSA public keys – Read/Write RSA/DSA private keys – Read/Write
Administration	Configure administrators, including Crypto-Officer passwords, and monitor the devices	CMS API calls and configuration information, including Crypto-Officer passwords, if configuring	Status information, including configured policies	Crypto-Officer passwords – Read/Write
Zeroization	Zeroize the module's CSPs	CMS API calls	Status information	ALL CSPs - Write
TLS	Establish a TLS session.	TLS handshake parameters, TLS inputs	TLS outputs	TLS session keys - Read/Write RSA private keys - Read RSA public keys - Read/Write

Table 4 – Crypto-Officer Services, Descriptions, and CSPs

User Role

Users (people) authenticate to the Caymas devices and are granted access to particular resources (networks, servers, files) based on the access control permission configured for that operator or resource. These access control permissions are configured by administrators, and this configuration is an extremely robust, policy based architecture.

The Users are able to access the module over a TLS session or through an IPSec tunnel. On top of these protocols, users authenticate using user IDs (UIDs) and passwords, and the authentication may be performed internally using a local database or via a 3rd party authentication mechanism, such as Radius.

User service descriptions and inputs/outputs are listed in the following table:

Service	Description	Input	Output	CSP and Type of Access
Login	Authenticate the User role, which can be on top of authentication mechanism employed by cryptographic protocols.	Login information	Result of login attempt	User password - Read
Logout	Log out the User.	Logout call	Call response	
Password change	Change the User's password	Password change information	Status	User password - Write
Resource, Application, and Network access	Users, Web/File Resources, Applications, Machines, and Networks.	Data inputs for particular resource, application, or network	Data outputs for particular resource, application, or network	
TLS	Establish a TLS session.	TLS handshake parameters, TLS inputs	TLS outputs	TLS session keys - Read/Write DSA/RSA private keys - Read DSA/RSA public keys - Read/Write
IPSec	Establish an IPSec session and authenticate an operator with digital certificates or pre-shared, if configured.	IPSec handshake parameters, IPSec inputs	IPSec outputs	IPSec session keys - Read/Write Pre-shared keys - Read DSA/RSA private keys - Read DSA/RSA public keys - Read/Write

Table 5 – User Services, Descriptions, Inputs and Outputs

Network User Role

Network users (networks, machines) authenticate to the Caymas devices and are granted access to particular resources (networks, servers, files) based on the access control permission configured for that network. These access control permissions are configured by administrators, and this configuration is an extremely robust, policy based architecture.

The Network Users are able to access the module through an IPSec tunnel, which authenticates Network Users via pre-shared keys or digital certificates.

Network User service descriptions and inputs/outputs are listed in the following table:

Service	Description	Input	Output	CSP and Type of Access
Resource, Application,	Users, Web/File Resources, Applications, Machines, and	Data inputs for particular resource,	Data outputs for particular resource,	

and Network access	Networks.	application, or network	application, or network	
IPSec	Establish an IPSec session and authenticate an operator with digital certificates or pre-shared, if configured.	IPSec handshake parameters, IPSec inputs	IPSec outputs	IPSec session keys - Read/Write Pre-shared keys - Read DSA/RSA private keys - Read DSA/RSA public keys - Read/Write

Table 6 – Network User Services, Descriptions, Inputs and Outputs

Authentication Mechanisms

The Crypto-Officers are able to access the module over a TLS or SSH session, or through a directly connected console port. On top of these protocols, Crypto-Officers authenticate using user IDs (UIDs) and passwords. The Users are able to access the module over a TLS session or through an IPSec tunnel. On top of these mechanisms, Users authenticate using user IDs (UIDs) and passwords, and the authentication may be performed internally using a local database or via a 3rd party authentication mechanism, such as Radius 3rd party. Network Users authenticate during IPSec via pre-shared keys or digital certificates.

Authentication Type	Strength
Passwords	Considering a case sensitive alphanumeric password with repetition, the total possible combinations for the password are 62^6. The probability for a random attempt to succeed is 1:62^6 or 1:56800235584, and, since this authentication attempt is additionally piped over an encrypted session, it is not possible to perform enough authentication attempts to reduce the 1:62^6 chance per attempt to 1:100,000 over a minute.
Pre-shared Keys	Considering a case sensitive alphanumeric pre-shared key with repetition, the total possible combinations for the pre-shared key are 62^16. The probability for a random attempt to succeed is 1:62^16 or 1: 47672401706823533450263330816, and it is not possible for an operator to perform enough authentication attempts to reduce the 1: 62^16 chance per attempt to 1:100,000 over a minute.
Public key certificates	Using conservative estimates equating a 1024 bit DSA/RSA key to an 80 bit symmetric key, the probability for a random attempt to succeed is 1:2^80 or 1:1208925819614629174706176, and it is not possible for an operator to perform enough authentication attempts to reduce the 1: 2^80 chance per attempt to 1:100,000 over a minute

Table 7 – Authentication Mechanisms

Unauthenticated Services

The module has a limited set of unauthenticated services, which are only available through local access to the module using the CDM. (Although a password can be configured for authentication through the CDM during boot, this is not required nor deemed security-relevant as the services provided by the CDM are meant to be unauthenticated and FIPS 140-2 does not require a password to be entered for booting a module.)

Service	Description	Input	Output	CSP and Type of Access
CDM status	Status information displayed on the CDM		Status	
Factory defaults (zeroization)	Zeroize all CSPs and return to factory default state	CDM button input	Command status	All CSPs - Write
Management network interface configuration	Set the network settings for the management port	CDM button input	Command status	
Savecore	Saves the system core	CDM button input	Command status	
Restart	Reboots the system	CDM button input	Command confirmation and status	
Viewing alarms	View system alarms	CDM button input	Command status	
Shutdown	Shuts down the system	CDM button input	Command confirmation and status	

Table 8 – Unauthenticated Services, Descriptions, Inputs and Outputs

Physical Security

Caymas Systems 318 and 525 are enclosed in a hard, opaque metal case that completely encloses all of the internal components of the modules. There are only a limited set of vent holes provided in the case, and these are all obscured to prevent viewing of the internal components of the module. Tamper-evident labels are applied to the case of the 525 and 318 to provide physical evidence of attempts to remove the case or hard drives of the modules. All of the modules' components are production grade.

The 525 and 318 were tested and found 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).

Operational Environment

The operational environment requirements do not apply to the 525 and 318. The modules do not provide a general purpose operating system and only allow firmware updating using digital signed Caymas Systems firmware updates. Additionally, only upgrades validated to FIPS 140-2 may be activated, as described in the Crypto-Officer Management guidance below.

Cryptographic Key Management

Caymas Systems 525 and 318 implement FIPS-approved algorithms in both hardware and software. The following is a list of the FIPS-approved algorithms supported by the modules.

Digital signatures

- DSA - FIPS 186-2 (certificate #129, 130, 131)
- RSA - PKCS#1 (certificate #55, 56)

DSA key generation

- DSA - FIPS 186-2 (certificate #131)

RSA key generation

- RSA key generation – Appendix B.4 of ANSI X9.31 (certificate #55, 56)

Symmetric encryption

- DES (CBC mode – for legacy use only – transitional phase only – valid until May 19, 2007) – FIPS 46-3 (certificate #299, 300, 301, 302, 303, 304)
- TripleDES (ECB,CBC mode) – FIPS 46-3 (certificate #319, 320, 321, 322, 323, 325, 326)
- AES (ECB, CBC mode) – FIPS 917 (certificate #229, 230, 231, 232, 233, 234, 235)

Hashing

- SHA-1 – FIPS 180-2 (certificate #308, 309, 310, 311, 312, 313, 314)

MAC'ing

- HMAC with SHA-1 – FIPS 198 (certificate #41, 42¸ 43, 44, 45; SHA- certificate #308, 309, 310, 311, 314 respectively)

Random number generation

- X9.31 PRNG – Appendix A.2.4 of ANSI X9.31 (certificate #69, 70, 71, 72, 73, 74)

Additionally, the module implements the following non-FIPS-approved algorithms for use in a FIPS mode of operation.

- Diffie-Hellman key agreement
- RSA key transport (encrypt/decrypt)
- Hardware RNG

The module also implements the following non-FIPS-approved algorithms, which are not used in a FIPS mode of operation.

- MD5
- MD5 HMAC
- RC4

The modules support the following critical security parameters:

Key	Key Type	Generation	Storage	Zeroization	Use
RSA Public Keys	RSA (1024-2048 bit)	RSA public key generated internally by the module using X9.31 key generation; or externally generated loaded onto the module in a certificate (during IKE, TLS, or SSH handshakes) and/or over a management TLS session	Stored on the hard drive in database in plaintext; or not stored - in volatile memory only	Zeroized by deleting the key through the CMS API. Zeroized during execution of the zeroization command.	Used during TLS, SSH, or IPSec session establishment. Used for certificate verification.
RSA Private Keys	RSA (1024-2048 bit)	RSA private key generated internally by the module using X9.31 key generation; or externally generated loaded onto the module over a management TLS session	Stored on the hard drive in database in plaintext	Zeroized by deleting the key through the CMS API. Zeroized during execution of the zeroization command.	Used during TLS, SSH, or IPSec session establishment.
DSA Public Keys	DSA (1024 bit)	DSA public key generated internally by the module; or externally generated loaded onto the module in a certificate (during IKE or SSH handshakes) and/or over a management TLS session	Stored on the hard drive in database in plaintext; or not stored - in volatile memory only	Zeroized by deleting the key through the CMS API. Zeroized during execution of the zeroization command.	Used during SSH or IPSec session establishment. Used for certificate verification.
DSA Private Keys	DSA (1024 bit)	DSA private key generated internally by the module; or	Stored on the hard drive in database in	Zeroized by deleting the key through the	Used during SSH or IPSec session

		externally generated loaded onto the module over a management TLS session	plaintext	CMS API. Zeroized during execution of the zeroization command.	establishment.
HA shared secret key	AES (128 bits)	Externally generated loaded onto the module over a management TLS session	Stored on the hard drive in database in plaintext	Zeroized by deleting the key through the CMS API. Zeroized during execution of the zeroization command.	Used during High Availability synchronization
TLS session keys	AES (128, 256 bits), Triple-DES (168 bits), DES (56 bits), SHA-1 HMAC (160 bits)	Negotiated during TLS session establishment.	Not stored - in volatile memory only in plaintext.	Zeroized when the module is powered down.	Used to encrypt/MAC the TLS session.
IPSec session keys	AES (128, 192, 256 bits), Triple-DES (168 bits), DES (56 bits), SHA-1 HMAC (160 bits)	Negotiated during IPSec session establishment; or externally generated loaded onto the module over a management TLS session	Stored on the hard drive in database in plaintext; or not stored - in volatile memory only	Zeroized when the module is powered down; or Zeroized by deleting the key through the CMS API. Zeroized during execution of the zeroization command.	Used to encrypt/MAC the IPSec session.
SSH session keys	AES (128, 256 bits), Triple-DES (168 bits), SHA-1 HMAC (160 bits)	Negotiated during SSH session establishment.	Not stored - in volatile memory only in plaintext.	Zeroized when the module is powered down.	Used to encrypt/MAC the SSH session.
Diffie-Hellman key pairs	Diffie-Hellman (768, 1024, or 1536 bit)	Generated for IKE/IPSec and SSH session establishment using an X9.31 PRNG.	Not stored - in volatile memory only in plaintext.	Zeroized when the module is powered down.	Used by the module in establishing a session key during IKE/IPSec and SSH negotiation.
Operator passwords	Passwords	Entered into module by remotely authenticating operator over an IPSec, TLS, or SSH session or locally over directly connected serial port, verified internally	Stored on the hard drive in database in plaintext; or not stored - in volatile memory only	Zeroized when the password is updated with a new one or the user is deleted. Zeroized during execution of the zeroization command.	Used for authentication of Crypto-Officer and User passwords.
X9.31 seeds	Seed	Generated internally by querying the Cavium hardware RNG, or generated using entropy gathering routines	Not stored - in volatile memory only in plaintext.	Zeroized when the module is powered down.	Used to seed the X9.31 PRNGs

Table 9 – Listing of Keys and Critical Security Parameters

Self-Tests

Caymas Systems 525 and 318 perform a series of self-tests to verify the correct operation of the modules. These tests are both perform at power-up and continuously during normal operations upon certain conditions. The following is a list of self-tests performed by the modules.

- Power-up Self-tests:
  - Software Integrity Test – The modules verify that their firmware has not been modified by verifying CRC-32 checksums over their firmware.
  - Cryptographic Algorithm Tests – The 525 and 318 perform cryptographic algorithm tests on all FIPS-approved algorithms at power-up to verify the correct operation of the algorithm implementations.
    - DES Known Answer Tests (KATs)
    - Triple-DES-ECB KATs
    - AES-CBC KATs
    - SHA-1 KATs
    - HMAC with SHA-1 KATs
    - DSA Pair-wise Consistency Tests (sign/verify)
    - RSA Pair-wise Consistency Tests (sign/verify)
    - RSA Pair-wise Consistency Tests (encrypt/decrypt)
    - X9.31 PRNG KATs
- Conditional Self-tests:
  - Continuous Random Number Generator Tests – This test is run upon generation of random data by the module's random number generators to detect failure to a constant value.
  - Software update test – This test is run upon updating of the module's firmware. A digital signature is verified over the firmware update to ensure the integrity of the firmware update.

- RSA Pair-wise Consistency Tests (sign/verify) – This test is run upon generation of a new RSA key pair to verify the correct operation of the newly generated key pair.

- RSA Pair-wise Consistency Tests (encrypt/decrypt) – This test is run upon generation of a new RSA key pair to verify the correct operation of the newly generated key pair.

- DSA Pair-wise Consistency Tests (sign/verify) – This test is run upon generation of a new DSA key pair to verify the correct operation of the newly generated key pair.

If any of the power-up self-tests fail, the modules enter an error state and output an error indicator. If any of the conditional self-tests fails, the service that caused the failure enters an error state, outputs an error indicator, and terminates.

Design Assurance

Caymas uses AccuRev/CM for its configuration management of source code and related documentation and Arena Solutions PLM for its configuration management of hardware components and related documentation. Both systems provide access control, versioning, and logging.

Additionally, Microsoft Visual Source Safe is used to provide configuration management for the 525 and 318's FIPS documentation. This software provides access control, versioning, and logging.

Mitigation of Other Attacks

This section is not applicable.

SECURE OPERATION

Caymas Systems 318 and 525 meet Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

Crypto-Officer Guidance

Initial Setup

The 318 and 525 are available from Caymas Systems through shipping using a bonded carrier or delivery directly by Caymas Systems, and by direct pickup from a Caymas Systems facility. The Crypto-Officer is responsible for inspecting the module and its packing upon receipt for signs of tamper.

The 318 or 525 is provided in a Caymas Systems box sealed with tape. Inside of this box, the 525 or 318 is sealed with tape in an anti-static bag. The Crypto-Officer must inspect the box, packing materials, and module for signs of tamper, including damage to the box, packing materials, or the module itself. If tamper-evidence is found, the Crypto-Officer should contact Caymas Systems immediately and not use the module.

If the 318 or 525 have been shipped without tamper-evident labels applied, then the Crypto-Officer must apply these labels.

The following steps detail application of the labels for the 318.

1. Ensure the system is unplugged.

2. Clean the areas to which the tamper-evident labels will be applied to remove any grease, dirt, etc. Rubbing alcohol can be used for this purpose.

3. Apply a tamper-evident label at the seam across the bottom center of the faceplate and bottom of the chassis of the front of the module.

Figure 5 – Apply label to bottom center of the faceplate of the 318

4. Apply a tamper-evident label at the seam across the top center of the faceplate and top of the chassis of the front of the module.

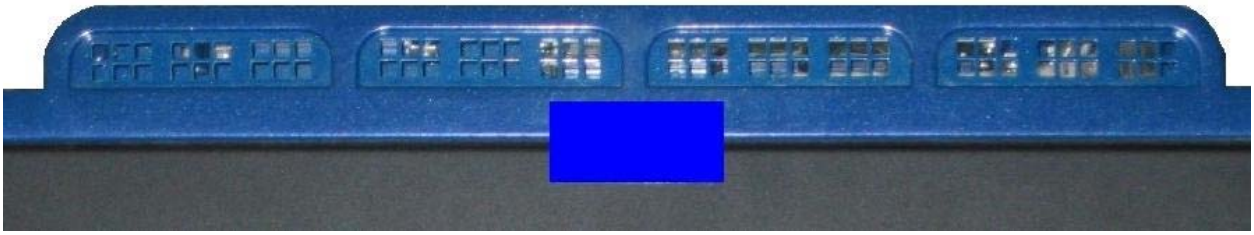

Figure 6 – Apply label to top center of the faceplate of the 318

5. Apply a tamper-evident label across the top of the chassis and the hard drive bay of the rear of the module.

Figure 7 – Apply label to upper hard drive bay of the rear of the 318

6. Log the serial numbers of the applied labels.
7. Allow a minimum of 24 hours for the labels to cure.

The following steps detail application of the labels for the 525.

1. Ensure the system is unplugged.
2. Clean the areas to which the tamper-evident labels will be applied to remove any grease, dirt, etc. Rubbing alcohol can be used for this purpose.
3. Apply a tamper-evident label at the seam across the bottom center of the faceplate and bottom of the chassis of the front of the module.

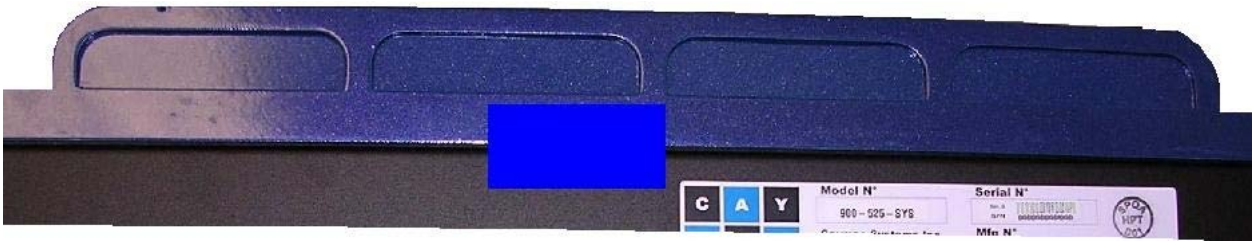

Figure 8 – Apply label to bottom center of the faceplate of the 525

4. Apply a tamper-evident label at the seam across the top center of the faceplate and top of the chassis of the front of the module.

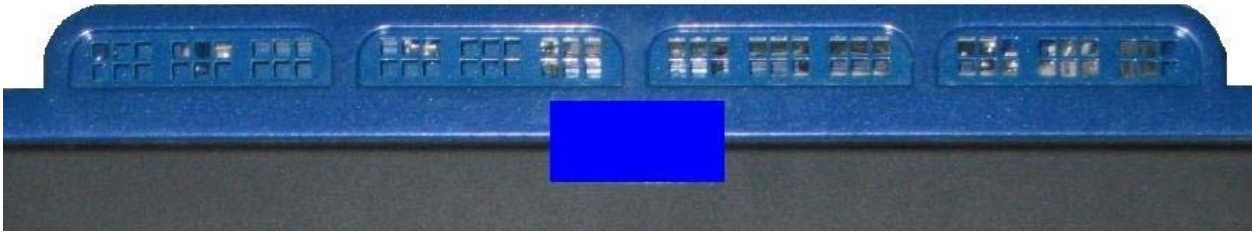

Figure 9 – Apply label to top center of faceplate of the 525

5. Apply a tamper-evident label across the top of the chassis and the upper hard drive bay of the rear of the module.

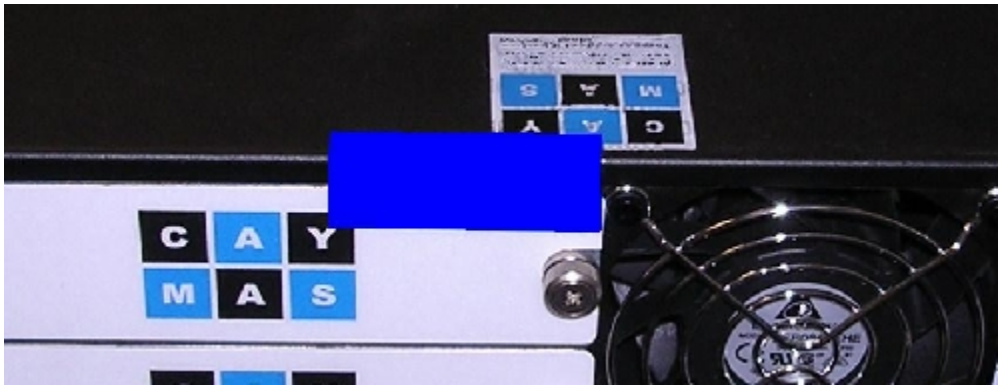

Figure 10 – Apply label to upper hard drive bay of the rear of the 525

6. Apply a tamper-evident label across the bottom of the chassis and the lower hard drive bay of the rear of the module.

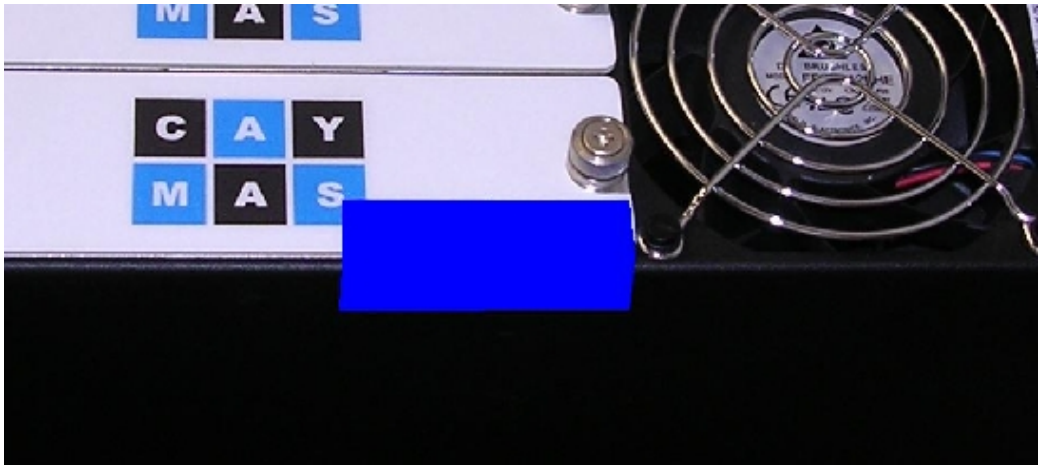

Figure 11 – Apply label to lower hard drive bay of the rear of the 525

7. Log the serial numbers of the applied labels.

8. Allow a minimum of 24 hours for the labels to cure.

Initialization

The module ships with a default Crypto-Officer account (“admin”) and a default password for this account (“caymas”). The Crypto-Officer must change this password and must use a password a minimum of 6 characters in length. This can be performed through the Administrators->Administrators screen in CMS GUI. Once completed, the Crypto-Officer must apply the changes.

Next, the Crypto-Officer must import or create a new key pair to replace the default Caymas key pair that is shipped with the module, and this key pair must be a minimum of 1024 bits for RSA. This can be done through the System->Certificates screen in CMS GUI. Once completed, the Crypto-Officer must apply the changes.

After creating a new key pair, the Crypto-Officer must configure a new SSL server to replace the default Caymas SSL server, and this server must be configured with a certificate other than the default Caymas certificate. Only FIPS-approved cipher suites may be configured for this SSL server, and these cipher suites are DES SHA-1 – for legacy use only, 3DES SHA-1, AES128 SHA-1, and AES256 SHA-1. This can be done through the System->SSL Servers screen in CMS. Once completed, the Crypto-Officer must apply the changes. (Note: While the term SSL is used here, once configuration for FIPS is completed, the actual protocol used will be TLSv1 and not SSL.)

Once these steps have been completed, the Crypto-Officer can proceed with removing the default SSL server and the default Caymas key pair. The Crypto-Officer must be careful to first remove the default SSL server,

and then to remove the default Caymas key pair. Removing the default SSL server can be accomplished through the CMS GUI on the System->SSL Servers screen by selecting the default SSL server and selecting to remove it. Removing the default Caymas key pair can be accomplished through the CMS GUI on the System->Certificates screen by selecting the default Caymas certificate and selecting to remove it. Once completed, the Crypto-Officer must apply the changes.

The Crypto-Officer must enable all of the FIPS flags in order to enable or disable certain functionality provided by the module for FIPS mode. The flags can be easily configured on the System->Settings->FIPS Settings screen in CMS. The following flags must be checked.

- Enable CMS Management over Secure Tunnel
- Restrict Front-End To TLS
- Restrict Back-End to TLS and FIPS Ciphers
- Verify Software Image Integrity on Startup
- Restrict CMS and CLI to One Administrator
- Disable Debug Shell Sessions
- Encrypt CSPs for High-Availability Communication
- Allow Only Encrypted Traffic
- Restrict CMS Management to Secure Tunnel
- Enable Cryptographic Module Self-Test
- Zeroize Upon Restore to Factory Defaults

These flags ensure that only TLS is used with FIPS-approved cipher suites, disable SSL, enable the FIPS self-tests, disable multiple administrators using the same management interfaces, disable shell access, ensure that all CSPs exiting the module are encrypted, disable any bypass capabilities, enable full zeroization when switching to a factory default state (i.e., out of the FIPS configuration), and enforce an encrypted management sessions. Once completed, the Crypto-Officer must apply the changes.

High availability, when configured, creates a channel that will encrypt CSPs exchange between the two modules established in the high availability configuration. An AES key must be entered into the module for

this purpose, and the Crypto-Officer is responsible for entering a 128 bit AES key when using high availability.

The Crypto-Officer must disable port 80 on the module. This flag can be configured on the System->Settings->Basic Settings screen in CMS. The “Disable Port 80” flag must be checked. This disables plaintext HTTP sessions through the module.

The Crypto-Officer must configure an Authentication Policy for passwords that requires password to be a minimum of 6 characters in length, and all pre-shared keys must be a minimum of 16 characters in length. By default, Crypto-Officer passwords must be a minimum of 6 characters in length. Additionally, the Crypto-Officer must take care to choose secure passwords containing upper case letters, lower case letters, numbers, and symbols.

At this point, the module must be rebooted to enable all of the changes. Upon reboot, initialization of the module for FIPS is complete and the module is now configured securely.

Note: While outside of the module’s boundary, the Crypto-Officer must configure their external software (e.g., a web browser) to use TLS when attempting to interface with the module using SSL/TLS.

Management

The Crypto-Officer must be sure to only configure cryptographic services for the module using the FIPS-approved algorithms, as listed Cryptographic Key Management section above. TLSv1 and IPSec must only be configured to use FIPS-approved cipher suites, and only digital certificates generated with FIPS-approved algorithms may be utilized. RSA key pairs must be a minimum of 1024 bits in length, and DSA key pairs must be equal to 1024 bits in length. DES must only be used for legacy purposes and is not to be used for management connections to the module.

The Crypto-Officer must configure all traffic flowing through the module to undergo cryptographic processing. All policies must require that services are accessed over encrypted session.

All IPSec Site to Site Policies must be configured prior to defining the network-based Resource Access Rules (RARs) that utilize the IPSec Site to Site Policies. When any IPSec Site to Site Policy is deleted, the module must be rebooted.

If used, third party authentication mechanism must be configured to follow the password guidelines set out in the previous paragraph. Active directory and LDAP authentication servers must be configured to use a

TLSv1 connection with the module. RADIUS servers must have a minimum of a 6 character shared secret/password in place with the module, and SecureID must be configured to use DES.

The Crypto-Officer must not configure FTP transfer of coredumps, as these may contain sensitive information. Additionally, FTP transfers of files are not permitted, and only SCP may be used, which pipes data over an SSH connection. The module is configured by default to only use FIPS-approved cipher suites with SSH and SCP, and this must not be modified.

The module permits upgrades through the CLI using the release upgrade command. When upgrading, the module verifies a DSA digital signature over the upgrade to ensure that it is an unmodified, Caymas firmware update. However, the Crypto-Officer must also ensure that the upgrade is validated to FIPS 140-2 by checking the version of the firmware and verifying this has been validated to FIPS 140-2 before activating the upgrade. Since upgrading the module with a release that has not been validated to FIPS 140-2 will take the module out of FIPS mode, the Crypto-Officer must either zeroize the module (see Zeroization below) before activating the upgrade or not proceed with activating the upgrade.

The Crypto-Officer should periodically backup the configuration of the module.

The Crypto-Officer must periodically check the module for signs of tamper-evidence, including unusual dents, scrapes, or damage to tamper-evident labels, and verify the tamper-evident labels still have the proper serial numbers. Additionally, the Crypto-Officer should monitor logs and alerts for the module for strange activity. If indications of suspicious activity are found, the Crypto-Officer should immediately take the module offline and investigate.

Zeroization

At the end of its life cycle or when taking the module out of FIPS mode, the module must be fully zeroized to protect CSPs. This can be accomplished through the CMS GUI on the System->Settings->FIPS Settings screen or by resetting to a factory default through the CDM. The Crypto-Officer must wait until the module has successfully rebooted in order to verify that zeroization has completed.

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 (8 characters or greater, a minimum of alphanumeric), and must not reveal their password to anyone.

Additionally, the User should be careful to protect any secret/private keys in their possession, such as IPSec session keys.

Note: While outside of the module's boundary, the User must be sure configure their external software (e.g., a web browser) to use TLS when attempting to interface with the module using SSL/TLS.

Network User Guidance

The Network User does not have the ability to configure sensitive information on the module.

ACRONYMS

ANSI	American National Standards Institute
API	Application Programming Interface
CDM	Caymas Display Module
CLI	Command Line Interface
CMS	Caymas Management System
CMVP	Cryptographic Module Validation Program
CRC	Cyclical Redundancy Check
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DSA	Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HA	High Availability
HMAC	(Keyed-) Hash MAC
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
RAM	Random Access Memory
RAR	Resource Access Rule
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SCP	Secure Copy Protocol
SHA	Secure Hash Algorithm
SSH	Secure SHell
SSL	Secure Socket Layer
TLS	Transport Layer Security

