Aastra USA Inc.

ViPr Cryptographic Module

FIPS 140-2
Non-Proprietary Security Policy

Level 1 Validation

Document Version 1.3

(084-0101-03)

Revision History

Version	Modification Date	Modified By	Description of Changes
1.0	15 April 2009	D. Green	Release version
1.1	4 November 2009	D. Green	Submitted version
1.2	10 November 2009	D. Green	Updated for ViPr firmware 3.0.4
1.3	11 November 2009	D. Green	Updated for patch release 3.0.5

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the ViPr Cryptographic Module from Aastra USA Inc. It provides detailed information relating to each of the FIPS 140-2 security requirements relevant to the ViPr Cryptographic Module along with instructions on how to run the module in a secure FIPS 140-2 Approved mode.

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:

[1] NIST Security Requirements For Cryptographic Modules, FIPS PUB 140-2, December 3, 2002.

[2] NIST Security Requirements For Cryptographic Modules, Annex A: Approved Security Functions for FIPS PUB 140-2, May 19, 2007.

[3] NIST Security Requirements For Cryptographic Modules, Annex B: Approved Protection Profiles for FIPS PUB 140-2, November 4, 2004.

[4] NIST Security Requirements For Cryptographic Modules, Annex C: Approved Random Number Generators for FIPS PUB 140-2, March 19, 2007.

[5] NIST Security Requirements For Cryptographic Modules, Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2, March 19, 2007.

[6] NIST Derived Test Requirements for FIPS 140-2, Draft, March 24, 2004.

[7] RFC 3261 – SIP (Session Initiation Protocol)

[8] RFC 2246 - TLS (Transport Layer Security)

[9] RFC 4474 - Authenticated Identity Management in SIP

[10] ViPr™ Media Center/Desktop Terminal User Guide

[11] ViPr™ System Administration Guide

[12] ViPr™ Application Server Quickstart Guide

[13] ViPr Cryptographic Module FIPS 140-2 Mode Configuration Guide

1.3 Product Overview

The ViPr Cryptographic Module is contained within an Aastra USA ViPr™ Media Center (VMC) Terminal network appliance. The VMC Terminals are part of a networked ViPr personal communications system as shown below.

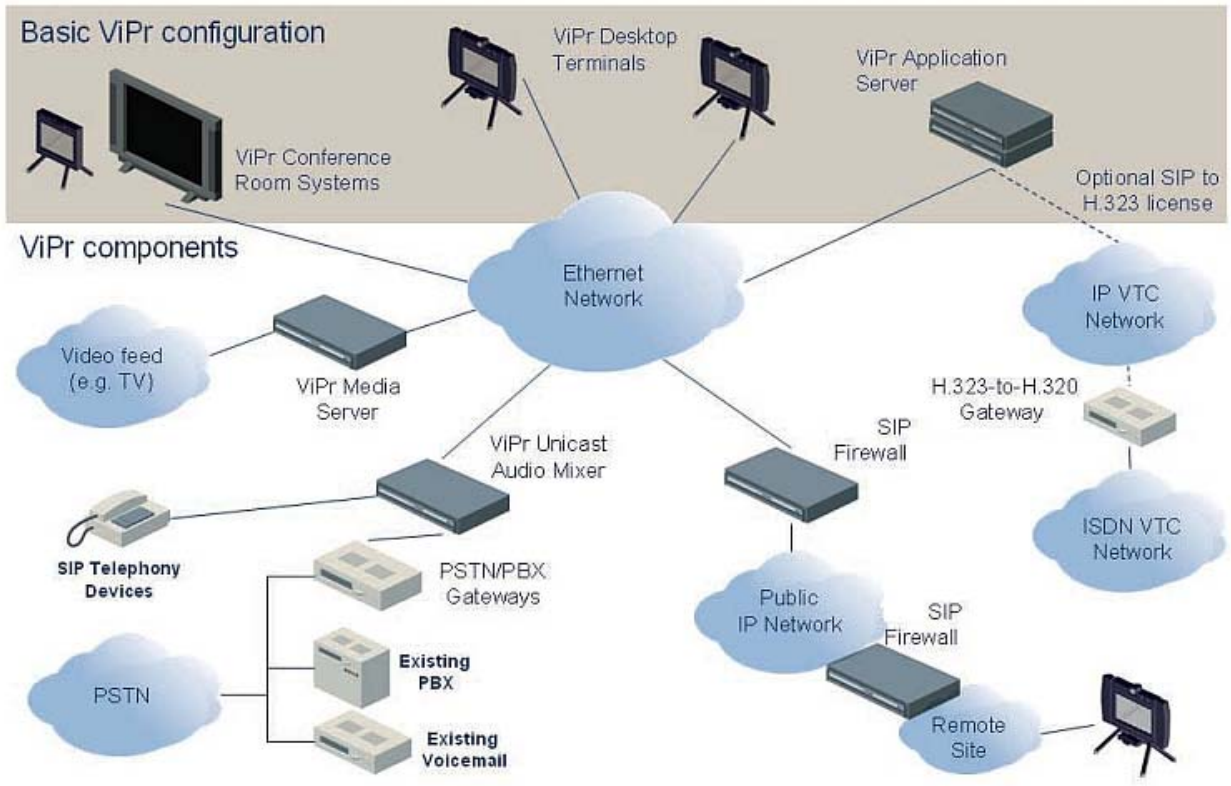

Figure 1: ViPr communications system network components

The Aastra USA VMC Terminal network appliances represent the next generation of personal communications. The VMC Terminal products have the ability to replace a telephone by combining the features of a modern telephone terminal with real-time, face-to-face video displayed on a high-resolution, flat-panel, color touch screen.

Figure 2: The Aastra USA ViPr™ Media Center/Desktop Terminal (containing the ViPr Cryptographic Module)

Up to 14 remote-party participants, each using their own VMC Terminal, can be visually conferenced together along with video feeds from TV or other video sources as shown below:

Figure 3: The VMC Terminal touchscreen with 14 concurrent remote participants

Each VMC Terminal is a single-user, networked device with its own internal ViPr Cryptographic Module which encrypts all outbound video and audio data streams originating on the terminal and decrypts all inbound data streams from other terminals for the Terminal user to view and/or hear. The built-in communications hardware features of the VMC Terminals are illustrated below:

Figure 4: VMC Terminal Hardware Input/Output Interfaces - front

The bottom of the VMC Terminals also provides a power input connector and a 10/100 Ethernet interface (RJ-45) that connects to the motherboard (not shown above).

VMC Terminals also incorporate a ViPr™ Collaboration Board that contains a Security Processor chip which provides a seed for the Random Number Generator, and also provides encryption and decryption using AES-128 for the voice and video produced by the VMC Terminal. This Security Processor chip and its associated PCI Bridge chip are included within the cryptographic boundary of the ViPr Cryptographic Module. All other components on the Collaboration Board are outside of the cryptographic boundary of the module.

Another important component of the ViPr personal communications system is the Aastra USA ViPr™ Application Server (VAS), a rack-mountable network server appliance that provides call control and central management functions to VMC Terminals. In this capacity, it functions as a "Crypto Officer" to the VMC Terminals under its control. The VAS also provides centralized storage of users' preferences and address books, enabling logged-in users to access their preferred environment from any VMC Terminal. A VAS device is shown below:

Figure 5: The ViPr Application Server (VAS)

The VAS normally is deployed as a High Availability (HA) pair. For small installations, the VAS may be operated as a Single Node server.

The ViPr Application Server and its associated VAS software provide Session Initiation Protocol (SIP) Services (acting as a "SIP proxy" per RFC3261) as well as an SQL Database for storage of configuration settings, user accounts, and each user's contacts (address book). The VAS can be managed (administered) using a web interface as well as via a local console interface. It is configured initially by attaching a monitor and keyboard to its console, powering up the system, logging in to the underlying Linux OS as the "root" userid, and running an Aastra USA-developed configuration application. Once the VAS is configured and attached to a working network, an administrative user may connect to it via a web browser, login with an "Administrator" userid and password, and manage the system via a browser-based GUI application. The VAS may also be configured by the Administrator to require any or all VMC Terminals under its control to run in FIPS Approved Mode. This configuration is then pushed out from the VAS to the VMC Terminals when they are powered off and back on again.

SIP Services provide signaling functions that facilitate creating and terminating calls between different terminals. They provide mechanisms and communication channels that enable locating users, negotiating audio and video properties, and setting up data streams to carry audio and video content. These mechanisms are used within one domain, between servers in different domains, or between a server and a SIP-enabled device that may provide a gateway service such as connecting to or from the PSTN.

The ViPr personal communications system is designed to be integrated into an existing enterprise or agency communications network. A number of other external input and output devices may be utilized as part of the ViPr communications system. The following graphic illustrates potential ViPr and 3rd party communications devices and the role of the VAS in communications management:

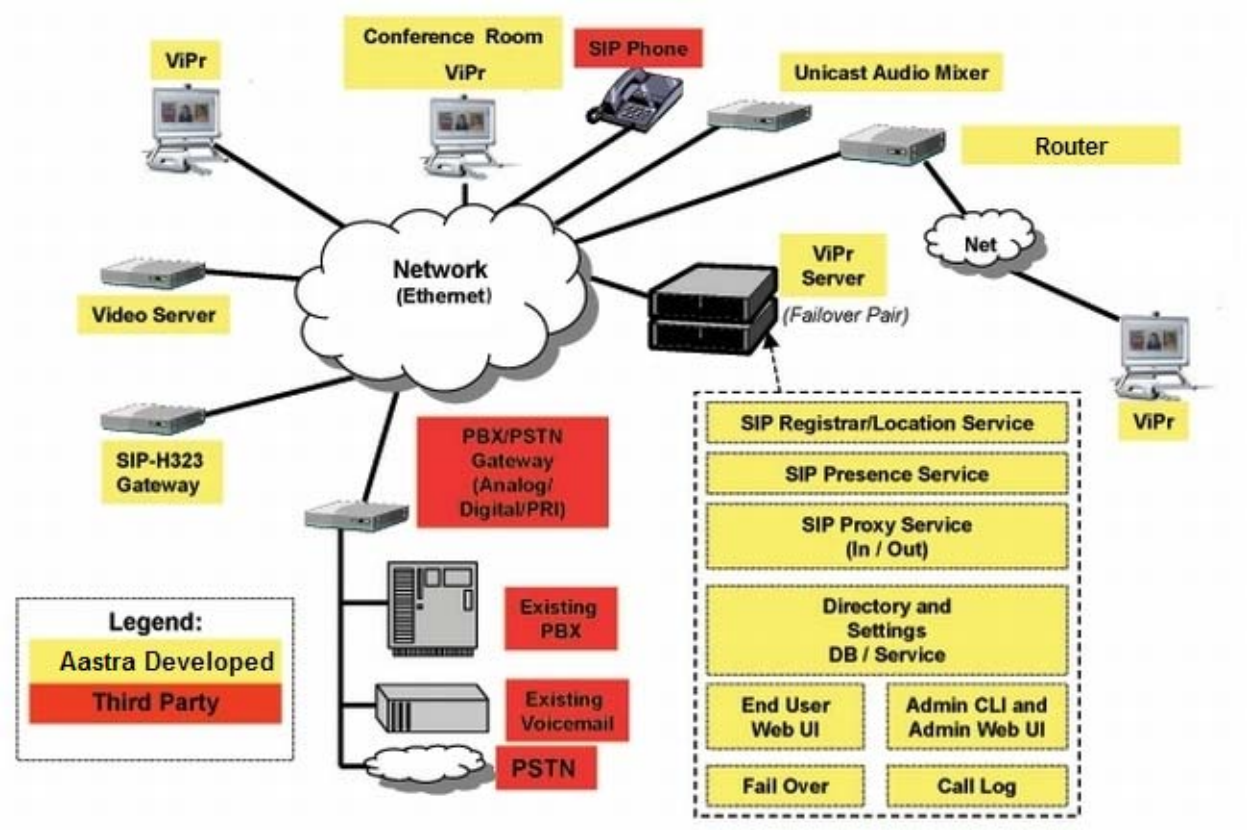

Figure 6: ViPr System Architecture and Optional Components

The ViPr Media Center Terminals are the primary focus of this document as they contain the ViPr Cryptographic Module that provides encrypted communications services. Note: The term "VMC Terminal" used throughout this document can include the following products: ViPr Media Center 4200 and 4400 Desktop Terminals, ViPr Media Center 5200 and 5400 Conference Room systems (rackmount), and ViPr Media Center 6200 and 6400 Conference Room systems (desktop systems that may be embedded into a conference-room table with a separate display screen for others to view). More information about the VMC Terminals and their associated systems can be found at the following web site: http://tolv.aastra.com/products/ViPr_Multimedia_Conferencing_pos.shtml

Each VMC Terminal device contains the ViPr Cryptographic Module, a hybrid module that provides the cryptographic functionality required for operation of the device in FIPS Approved mode. The ViPr Cryptographic Module, hereafter referred to as the "crypto module" or "module," provides the following cryptographic services:

- Data encryption and decryption
- Message digest testing of firmware integrity

The following assertions are intended to demonstrate that the ViPr Cryptographic Module can be validated to operate in a FIPS Approved mode when providing encrypted communications sessions per the FIPS 140-2 Publication.

1.4 Cryptographic Module Specification

The ViPr Cryptographic Module is a firmware-hybrid cryptographic module validated for use on an unmodified Redhat Linux 2.4.31 Operating System (OS) running on Aastra-designed hardware (a VMC Terminal). The module contains a BCM5812 hardware chip and ViPr Media Center application firmware v. 3.0.5. The module is entirely encapsulated by the logical cryptographic boundary as shown in Figure 7 below.

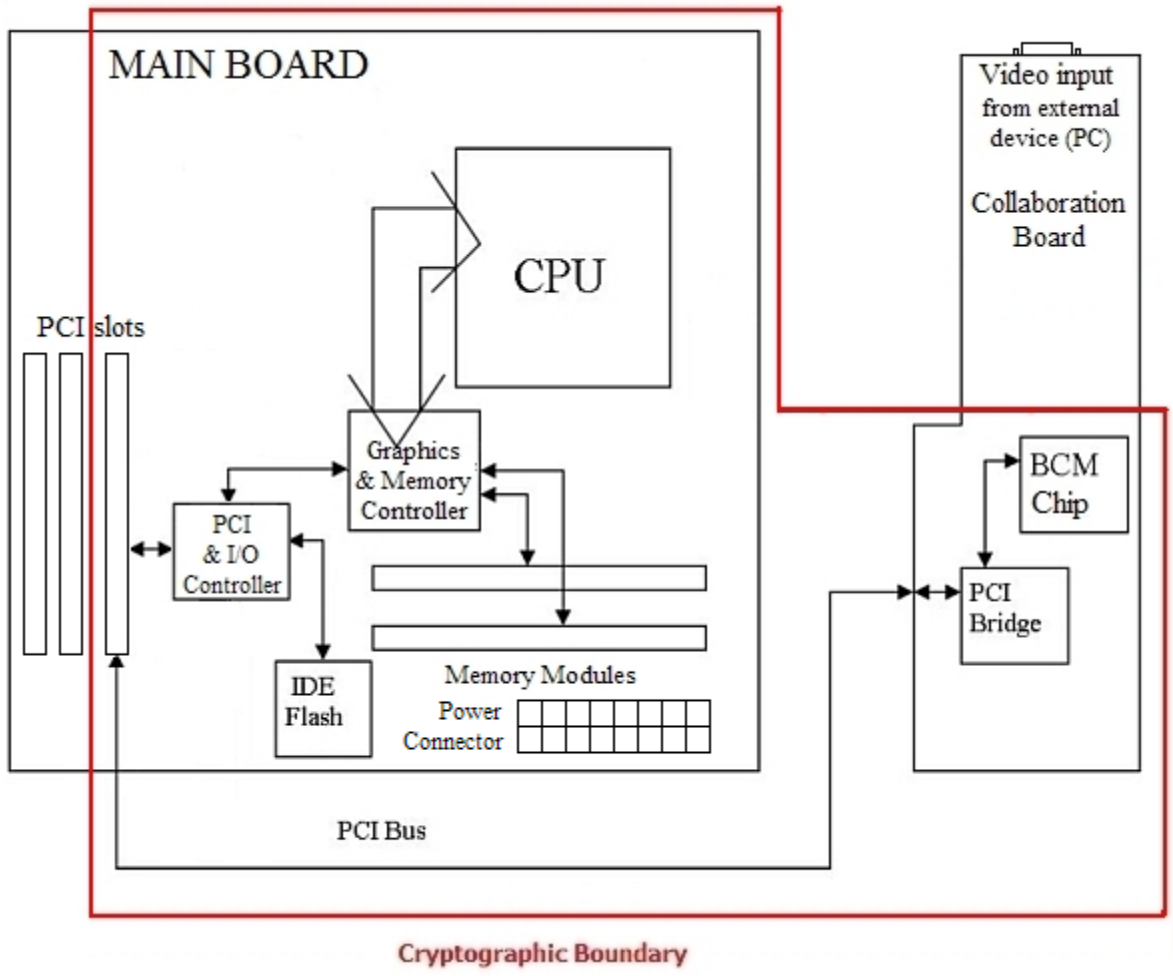

Figure 7: ViPr Cryptographic Module Boundary and Major Components

The ViPr Cryptographic Module is enclosed within the VMC Terminal. It utilizes three primary sets of internal components to provide its communications encryption features:

- a main processor board containing:
  - a CPU
  - System RAM
  - an IDE Flash drive for storage of the Redhat Linux 2.4.31 OS and ViPr Media Center application firmware v3.0.5 used in the operation of the VMC Terminal

- PCI Slots and a PCI Bridge chipset for communications between the CPU, RAM, IDE Flash drive and other devices via the motherboard's PCI bus

- an Aastra USA-designed PCI card containing:
  - a Broadcom BCM5812 (ver.A0) Security Processor chip (see image below) that performs two cryptographic functions: 1) it seeds RNG calculations in the crypto module performed by an ANSI X9.31 RNG from OpenSSL; and 2) it also performs AES-128 encryption and decryption of voice and video data being transmitted and received.

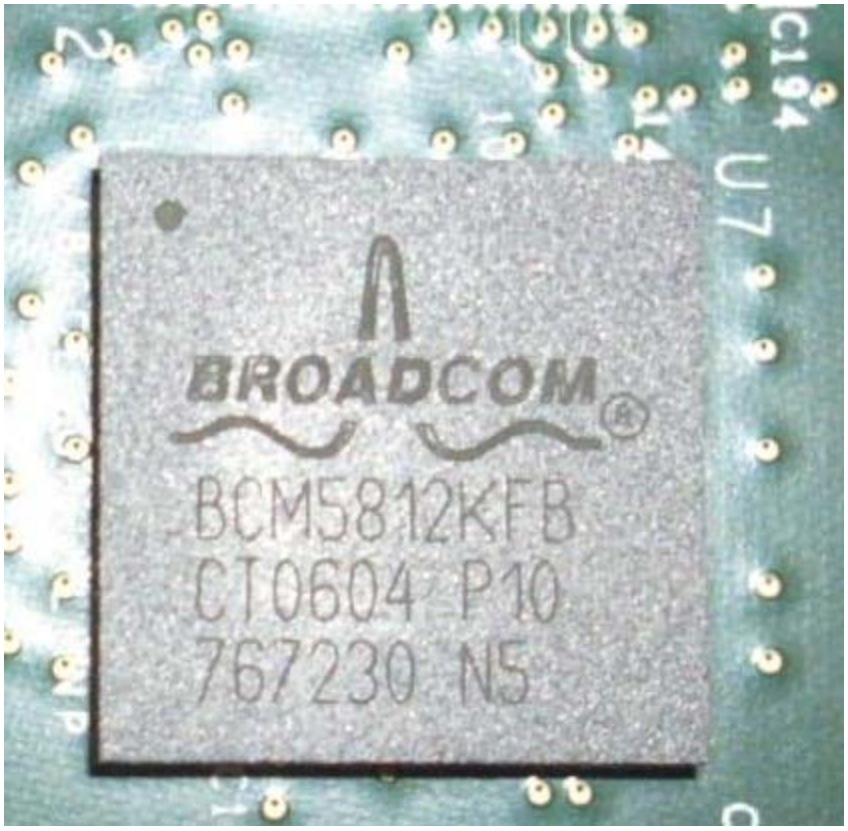

Figure 8: Broadcom BCM5812 Security Processor

  - a Intel PCI bridge chipset for communications between the Security Processor chip and the motherboard RAM via the main board PCI slot into which the card is inserted.

- The Aastra USA-developed ViPr Media Center (VMC) application firmware v3.0.5 running on the underlying Redhat Linux 2.4.31 OS. This firmware is loaded into system RAM from the IDE Flash drive and is executed by the CPU. All services available by the "ViPr Cryptographic Module" to include those provided by the BMC5812 are directed through the VMC application firmware. No services execute without first going through the VMC application firmware.

The cryptographic boundary of the module is the physical boundary of the ViPr Terminal components that execute the module as shown in Figure 7 above.

Per FIPS 140-2 terminology, the ViPr Cryptographic Module is a multi-chip standalone module that meets overall level 1 FIPS 140-2 requirements. The ViPr Cryptographic Module is validated at the following FIPS 140-2 Section levels:

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	NA
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	NA

1.5 Module Ports and Interfaces

The ViPr Terminal, which contains the ViPr cryptographic module, consists of a general-purpose PC mounted in a specially designed case that incorporates a touchscreen display, stereo speakers, a microphone array, a Pan-Tilt-Zoom (PTZ) camera, a telephone handset, and several standard PC-type interfaces including a 10/100 RJ-45 Ethernet interface, external video input interface, a mouse port, and a keyboard port. All of these interfaces are under the control of the ViPr Media Center (VMC) application firmware that is incorporated into the ViPr Cryptographic Module and may not be utilized for input or output outside of the module's control.

The module ports correspond to the physical ports of the ViPr Terminal executing the module, and the module interfaces correspond to the logical interfaces to the module. The module's logical interfaces exist within the operational boundaries of the VMC firmware that is executing within the module. Physically, ports and interfaces are located on the front (see Fig. 2) and bottom of the ViPr Terminal. The interfaces can be categorized as defined by FIPS 140-2 and shown below:

- Data Input Interface
- Data Out Interface
- Control Input Interface
- Status Output Interface
- Power Interface

All of these logical interfaces are described in the following table:

Table 2 - FIPS 140-2 Logical Interfaces

FIPS 140-2 Interface	Module Physical Ports/Interfaces	Module Logical Interfaces
Data Input	Data is input to the module containing either: a) unencrypted video & audio data from the VMC Terminal's camera and microphone array which passes through its Encoder card for H.264 encoding; or b) encrypted video & audio data received via the VMC Terminal's NIC from partner communications devices (other VMC Terminals)	Input parameters of module function calls
Data Output	Data is output from the module containing either: a) encrypted video & audio data for transmission via the Ethernet NIC to other VMC Terminals; or b) decrypted video & audio data from other VMC Terminals to be forwarded to the VMC Terminal's display screen and speakers (through the Encoder card).	Output parameters of module function calls
Control Input	API calls generated by touchscreen (virtual keyboard, callpad, on-screen buttons); or by external keyboard or mouse input; or by VMC application firmware controls or VAS control inputs received over the Ethernet NIC.	Module function calls
Status Output	Status output is forwarded from the module to the VMC Terminal's screen and/or LEDs for display to the Operator	Return codes of module function calls
Power Interface	Power connector to the module main board	None

1.6 Roles, Services and Authentication

Two roles are supported by the module: a Crypto Officer (CO) role and a User role. Both of these roles and their responsibilities are described below. The module does not support multiple or concurrent operators and is designed and intended for use by a single operator, although it may establish multiple concurrent communications sessions with other VMC Terminals (as illustrated in Fig. 3); thus it always operates in a single-user mode of operation.

1.6.1 Crypto Officer Role

Once the VAS is installed and configured, it then exercises the Crypto Officer role by enforcing use of the cryptographic services and functions performed by the User role, including making and receiving encrypted calls. This is done through a number of automated processes which use role-based authentication to assume the role of Crypto Officer:

- After any VMC Terminal is powered on, it connects to the VAS it has been assigned to in order to get any updated configuration information such as FIPS Mode operation settings and encryption licenses.
- The VAS maintains userid and password configurations for all Users, so when a User attempts to login to a VMC Terminal, their userid and password are forwarded to the VAS for authentication. If they cannot be authenticated, they cannot use the VMC Terminal to make calls.
- The VAS acts as an intermediary router for the exchange of cipher keys when calls are made between VMC Terminals. The VAS implements a SIP "proxy" function, which is responsible for

the routing of SIP calls between SIP endpoints that have established TLS connections with the proxy. The VAS does not retain or store the cipher keys exchanged between VMC Terminals; it merely forwards them between the VMC Terminals that are establishing a session with one another.

Descriptions of the services available to the Crypto Officer role are provided in the table below.

Table 3 - Mapping of Crypto Officer Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Configure module for encryption	VAS configures VMC Terminals to operate in FIPS Mode on power up requiring use of Encryption for all calls on all licensed Terminals	Upon power up, VMC Terminals retrieve configuration settings from VAS requiring FIPS Mode operations for all licensed Terminals	Encryption is **required** (FIPS mode) for VMC Terminals operation	Physical access to VMC Terminal for User to power it on; network connection to VAS to pull down configuration settings to Terminal
Authentication for VMC Terminal users	Users login to VAS via VMC Terminals to utilize terminals for communications sessions	VAS compares userids and passwords entered by users from VMC Terminals	Users are authenticated by VAS to use VMC Terminals for communications	Userid & password input via VMC Terminal for authentication of users on VAS

1.6.2 User Role

The User role is selected implicitly by the service that is invoked. The User role, which utilizes identity-based authentication, accesses the module's cryptographic services that include utilizing the VMC Terminals to make or receive encrypted "calls" (communications sessions) with other Users. An operator performs the User role by powering up and logging in to a VMC Terminal configured to use AES-encrypted network communications services, which are all automated by the VMC application firmware and require no operator intervention to utlize.

In order to operate the Crypto Module in FIPS Approved Mode, all Users must power down their VMC Terminals and then power them on again to force a configuration update from the VAS. A User must then login to a VMC Terminal with a valid userid and password to make calls in FIPS Approved Mode; this also causes the user's name to be displayed in any communications sessions that they initiate or join.

The default setting for User password security is that all passwords must contain a minimum of 8 characters; there is no maximum number of characters that may be used for a password. Passwords must consist of at least 2 upper case, 2 numeric, 2 non-alphanumeric and the others can be any of the available characters (26 upper case + 26 lowercase + 10 numeric + 33 special characters = 95 possible characters):

95^8 = 6,634,204,312,890,625

Therefore, a random guess at a user's password has a 1 in 6,634,204,312,890,625 of being correct.

The following table lists the services available to the User role; an unauthorized (non-authenticated) user can only perform three of these services: power off module, power-on/restart that initiates a self-test, and view status of FIPS self-tests.

Table 4 - Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Power down and restart of VMC Terminals	User powers down and restarts VMC Terminals to cause it to operate in "FIPS Mode"	VAS provides encryption configuration settings to operate Terminal in FIPS Mode	AES Encryption is **required** (FIPS mode) for VMC Terminals after they are powered down and restarted.	Physical access to VMC Terminals; network connection to VAS from Terminal
Crypto Module Startup or Reset	Startup or Reset of Crypto Module by User	Power on or off via VMC Terminal power switch or shut down VMC Terminal by pressing touchscreen "Logoff and Shutdown" or "Logoff and Restart" button	VMC Terminal and Crypto Module are started, powered off, or restarted	Physical access to VMC Terminals
Operator Initiates Power-on Self-test	Self-test of Crypto module is automatically run when VMC Terminal is powered on	Operator powers on the VMC Terminal	The terminal's Crypto module runs FIPS Self-test and displays the test results on the screen	Physical access to the terminal; Self-test Status – read; Screen display - write
Log-on to VMC Terminal	Operator logs in via VMC Terminal user interface	Valid userid and password (default password settings require a minimum of 8 characters with 2 uppercase, 2 numeric, and 2 non-alphanumeric characters)	Userid and password are forwarded to VAS for authentication – if valid, operator is authenticated	Userid and password – read and write
Begin Encrypted Communications Session	Initiate or Receive a call or take a call off hold to start an encrypted communications session	Operator initiates or accepts a call, or takes a call off hold, to start an encrypted communications session	Crypto module creates new cipher keys, exchanges keys with partner VMC Terminal via the VAS over TLS sesssions, and begins encrypted communications session with other VMC Terminal	Random Number – Read; Cipher keys – write
Operator Initiates Conditional Self-test	Self-test is initiated automatically by making or accepting a "call" or by powering down and restarting the VMC terminal	Operator initiates or accepts a call to start an encrypted communications session; or the operator restarts the VMC Terminal	Self-test status is updated with test results; if an error occurs, a message is displayed to the operator and further communications are disabled until errors are corrected	Crypto algorithms are tested; Test Results output to log file and display (if error)
View Self-test Status	Operator can view the status of previous Self-test	Operator presses the "Help – Show Status" button	Results of most recent Self-Test is displayed on the screen	Self-test log file – Read; Screen display - write

Service	Description	Input	Output	CSP and Type of Access
Key Zeroization	Zeroize current encrypted session cipher keys	Operator ends communications session, puts a call on hold, or powers down or Resets the VMC Terminal	Crypto Module zeriozes current communications session cipher keys	Cipher Keys – delete

1.7 Physical Security

The VMC Terminal device that executes the module is manufactured using industry standard integrated circuits and meets the FIPS 140-2 Level 1 physical security requirements.

The VMC Terminal device has been tested by Underwriter Laboratories and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules for EMI. Since it does not connect directly to a telephony system, it cannot be tested for Part 68 and has thus no FCC Part 68 ID assigned to it.

1.8 Mitigation of Other Attacks

The cryptographic module is not designed to mitigate any other specific attacks.

1.9 Operational Environment

The module runs on the underlying unmodified Redhat Linux 2.4.31 OS running on a general purpose PC mounted in the VMC Terminal using ViPr Media Center Applicaton Firmware 3.0.5. All operator authentication is done by using the user interface to enter a valid userid and password. No separate authentication mechanism is provided to the User for the ViPr Cryptographic Module or the underlying Linux OS. Users who have logged in to a VMC Terminal are implicitly authorized to access any cryptographic module services in making calls to other Terminals.

1.10 Cryptographic Key Management

The ViPr Cryptographic Module implements the following FIPS-approved algorithms:

- AES-128 CTR-mode encryption (certificate #1075) is used for all calls.
- Cipher keys are exchanged between endpoints using TLS (for key agreement and key establishment methodology with 128-bits of encryption strength[1]).
- ANSI X9.31 RNG from OpenSSL v1.1.2 (certificate #563) is used for pseudo-random number generation to create cipher keys.

Additionally, the cryptographic module utilizes the following non-FIPS-approved algorithm implementation:

[1] In order to operate in an Approved mode of operation compliant to FIPS 140-2, keys of 128-bits are used.

- RNG: The Broadcom Security Processor chip has a true hardware Random Number Generator, which is used for seeding the OpenSSL FIPS module at startup; the module then uses the seed to perform ANSI X9.31 compliant pseudorandom number generation.
- MD5: The MD5 algorithm is utilized for the firmware integrity test that is executed at module initialization.

The module supports the following critical security parameters (CSPs):

Table 5 - List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use/Access
Seed	Random number (bits) generated by Pseudo Random Number Generator (PRNG)	Broadcom BCM5812 Security Processor chip generates initial seed for PRNG at module initialization; subsequent calls use previous random number to form the seed.	Seed number utilized in ANSI X9.31 RNG in OpenSSL module executing in System RAM	System RAM	Seed is zeroized when Terminal is powered off or Reset.	Seed for generation of Random Number by ANSI X9.31 RNG in OpenSSL module; Operators have no access to it.
Seed Key	Random numbers (2 or more 64-bit numbers)	Broadcom BCM5812 Security Processor chip generates two seed keys for PRNG at module initialization.	Random Numbers for use as Seed Keys to generate Cipher Keys for each call	System RAM	Seed Keys are zeroized when Terminal is powered off or Reset.	Used by OpenSSL RNG to generate Cipher keys; Operators have no access to them.
Cipher Key	AES-128	ANSI X9.31 RNG in OpenSSL modules creates session keys using Random Numbers from the RNG	Cipher Keys for each individual communications session	System RAM in VMC Terminal	Keys are zeroized when call is ended or put on hold, or when Terminal is powered off or Reset.	Used by Broadcom Security Processor for encryption and decryption of communications session data; Operators have no access to them.
Password	Password (8 characters by default)	Entered by operator (User)	Password string verified per userid	Authentication database in VAS	Deleted in System RAM once operator is authenticated	Authentication of VMC Terminal operator; Operators have write access and Crypto Officer has read access.
Firmware integrity checksum	MD5 (non-FIPS-approved algorithm)	Module powerup process uses MD5 algorithm to check the integrity of the module's firmware image.	If firmware image checksum passes the MD5 integrity test, module startup continues; if not, the module enters an error state and the system is halted.	Calculated and stored in RAM during startup verification	Zeroized once firmware image integrity is verified	Used by CPU to validate firmware image integrity; Operators have no access to the MD5 checksum value.

1.11 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to ensure that all components are functioning correctly. This cryptographic module performs the following self-tests:

- Power-Up Self-Tests:
  - ViPr Firmware Integrity Test - EDC MD5
  - BCM-5812 Security Processor RNG seed self-test – continuous RNG test
  - OpenSSL ANSI X9.31 RNG test – continuous RNG test
  - Known Answer Tests (KATs)
    - AES-128 KAT - The module implements a KAT for AES-128. The KAT passes if and only if the calculated output equals the expected output.
    - OpenSSL ANSI X9.31 RNG KAT - The module implements a KAT for the OpenSSL ANSI X9.31 RNG. The KAT passes if and only if the calculated output equals the expected output.

- Conditional Self-tests: The conditional self-tests are run prior to initiating or accepting a call. The ViPr Cryptographic Module conditional self-tests consists of all of the power-up Self-Tests except the Firmware Integrity Test. The Firmware Integrity Test is only performed at only at power up because the firmware is not externally loaded onto the module.

If ANY of the above tests fail, FIPS mode will be disabled and all cryptographic functions are halted; no encrypted data streams will be initiated or accepted, and secure (encrypted) calls will be disabled until any failures are corrected. After such a failure, the VMC Terminal must be powered off and back on again and all FIPS mode self-tests passed successfully before any calls can be made or received again.

Status output of self-tests are logged to a log file and the VMC Terminal screen (available via the “Help – Show Status” button). Any time a User initiates or accepts a call, the module executes its internal “FIPS Mode” self-tests prior to making the call. A User may also initiate a self-test at other times by resetting the module using the “Logoff and shut down” button, then powering the terminal back on, or by making or receiving a call.

1.12 Design Assurance

Configuration management for all of the ViPr Media Center systems’ source code files is provided by an internal Software Configuration Management (SCM) system. Only authorized developers and management personnel are assigned userids and passwords to access this system.

The SCM system provides version control, workspace management, atomic change transactions and a branching model to develop and maintain multiple code lines. The source code revisions are maintained in several UNIX servers that have been deployed as software build repositories.

Additionally, an internal CM System is used to provide configuration management for the ViPr Cryptographic Module’s FIPS documentation. This system utilizes a back-end database system and web servers along with a web browser-based front end for user input and database searches. It is an ISO-9001-compliant system used by Aastra’s engineering, manufacturing, shipping and documentation departments. Access to any of these CM system areas requires a valid userid and password. This CM software provides access control, versioning, and logging.

2 Secure Operation

The ViPr Cryptographic Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to configure and maintain the module in a FIPS 140-2 Approved mode of operation. Operating the module without following this guidance will remove the module from the FIPS 140-2 Approved mode of operation.

2.1 Initial Setup

Setup of the ViPr Cryptographic Module to operate in FIPS 140-2 Approved mode requires four steps:

I. Install an encryption license file on the ViPr Application Server (VAS).

II. Configure Userids and assign Passwords on the VAS to allow Users to login and use VMC Terminals.

III. Set "Enable FIPS 140-2 Strict Security Mode" to YES on the VAS for all VMC Terminals under its control.

IV. Power down and restart VMC Terminals to operate in FIPS 140-2 Approved mode.

The first three steps would be performed by the VAS system administrator; detailed instructions are provided in the "ViPr Cryptographic Module FIPS 140-2 Mode Configuration Guide" and the "ViPr™ System Administration Guide" [Ch. 5.1]. The last step can be performed by either the system administrator or the individual Users.

2.2 Crypto Officer Guidance

Once the initial setup is completed, the Crypto Office role is performed by the VAS which will, by means of automated processes,

1. Push the FIPS encryption license setting from the VAS to the VMC Terminal to enable the VMC terminal to use encryption.

2. Push the FIPS Mode setting from the VAS to the VMC terminal. The VMC terminal will be set to operate in FIPS Mode.

3. Verify that the userid and password entered on the VMC terminal during user login is valid.

2.3 User Guidance

2.3.1 Setup/Operation

Once the system administrator has completed the first two steps listed in Sec. 2.1 to configure the VAS to enable FIPS Mode operations, the VMC Terminals must be powered down, then back on again; no additional setup is required for Users to make or receive encrypted (secure) calls on a VMC Terminal operating in FIPS 140-2 Approved mode. Any operator who logs on to a VMC Terminal with a valid userid and password automatically assumes the "User" role. They may then utilize the configured encryption settings as described above to make or receive calls.

Encryption of calls is handled automatically by the ViPr Cryptographic Module without any operator intervention. In fact, once a terminal has been properly configured to operate in FIPS 140-2 Approved

mode, the User can NOT change this configuration on the terminal itself; the “Require Secure Calls” configuration options located under “Tools -> Call Handling” will show as enabled but grayed out so they may not be changed by the User as shown below:

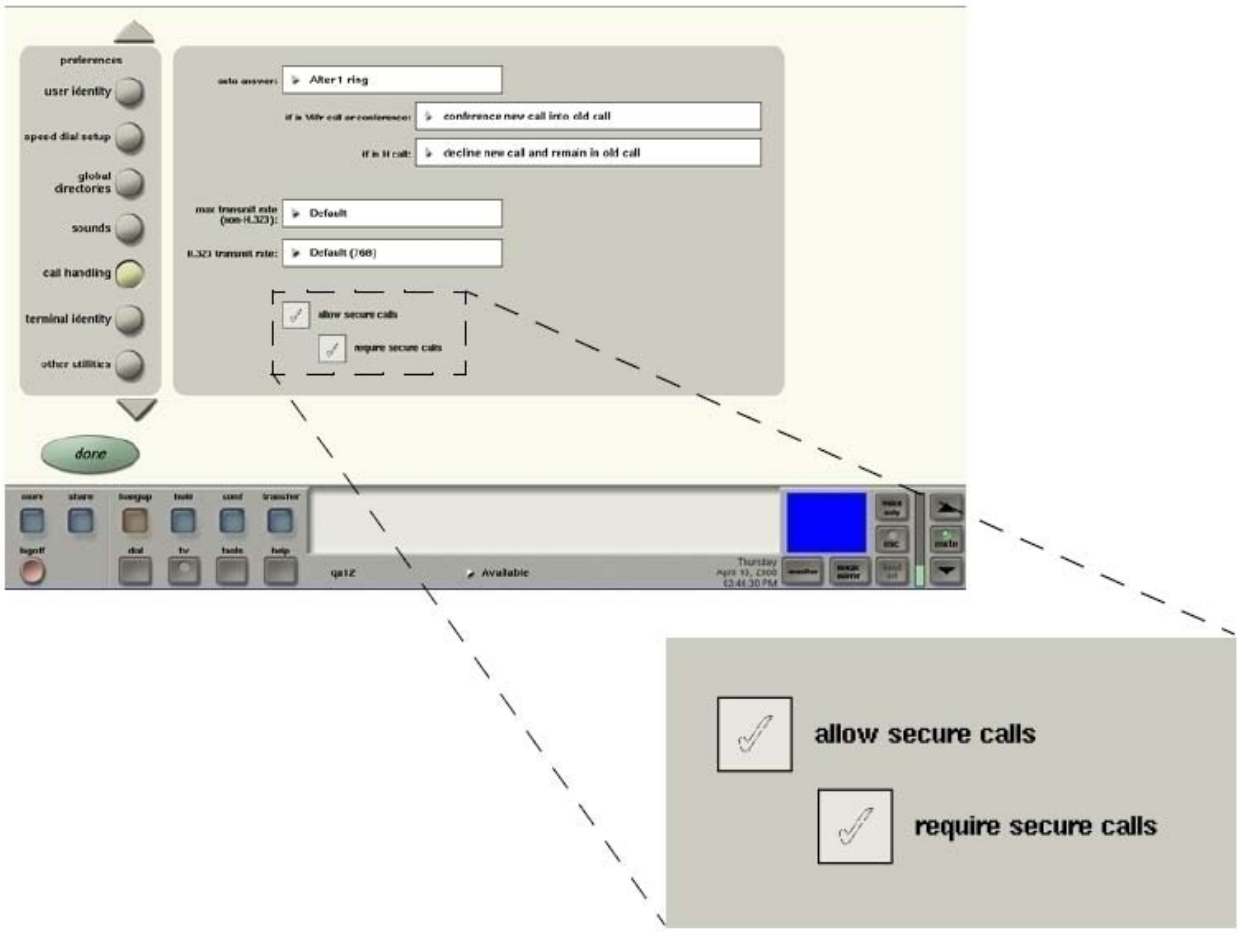

Figure 9: VMC Terminal Security Settings when in FIPS Approved Mode

Any time a User initiates or accepts a call, the module executes its internal “FIPS Mode” conditional self-tests prior to making or accepting the call. A User may also initiate a power-on self-test by resetting the module using the “Logoff and shut down” button, then powering the terminal back on.

If any of the ViPr Cryptographic Module’s “FIPS Mode” self-tests fail, the module prevents any further calls from being made or received. Any attempt to do so will result in a “Call failed” error message. The VMC Terminal must be powered off and back on again and successfully pass all of the self-tests before any encrypted calls can be made or received.

2.3.2 FIPS Mode Status Indicators

Notification of “FIPS Mode” operational status to the User is obtained by pressing the “Help -> Show Status” button and viewing the “FIPS Self-Test Status” section of information presented there. If there is no “FIPS Self-Test Status” information displayed, then the VMC Terminal is not operating in FIPS 140-2 Approved mode; if “FIPS Self-Test Status” information is displayed, it will show the results of the most recent FIPS Mode self-test that was run, either from the terminal’s power-on self test or from the most recently made call (communications session) on that terminal (a self-test is run prior to making or

receiving all calls on a terminal operating in FIPS Approved mode). An example of a successful "FIPS Mode" self-test display is shown below:

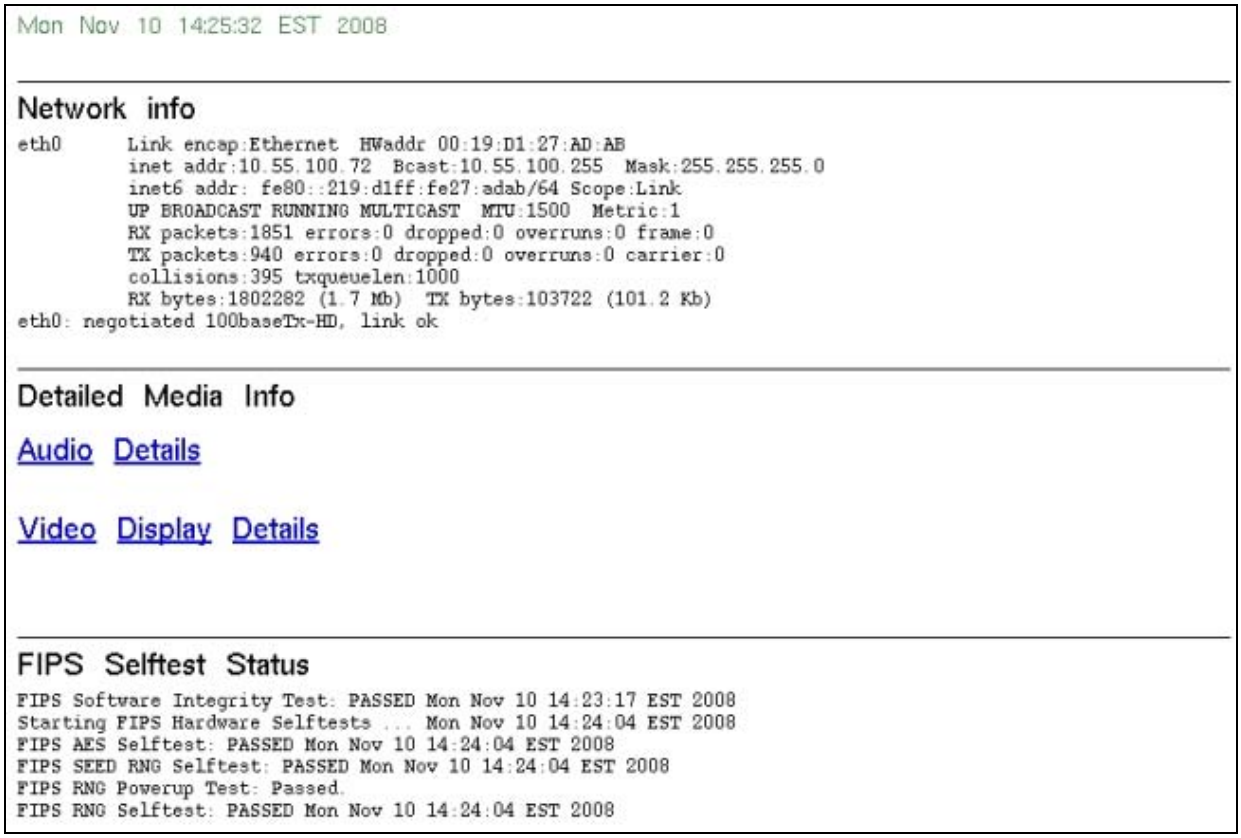

Figure 10: Successful FIPS Self-test Status Screen

As shown in the lower section of the screen shot above, all of the FIPS self-tests have passed; therefore, the crypto module is operating in FIPS Approved mode. A User could also review the "Tools -> Call Handling" configuration of the "Allow Secure Calls" and "Require Secure Calls" options on the terminal and verify that the check marks are enabled but grayed out and cannot be changed by the User as shown in Figure 10 above.

If encryption is enabled by an operator when the Terminal is running in non-FIPS mode, the Crypto Module provides the same encryption services, uses the same cryptographic function and algorithms, and operates in the same way as when running in FIPS Mode. However, enforcement of encrypted communications operations would then be left up to the individual users, which would mean that the Terminal is operating in non-FIPS Mode. Notification of encrypted call status to the User in either mode is indicated by the secure call "lock" icon that appears in the top left corner of the video window as show in the Figure below:

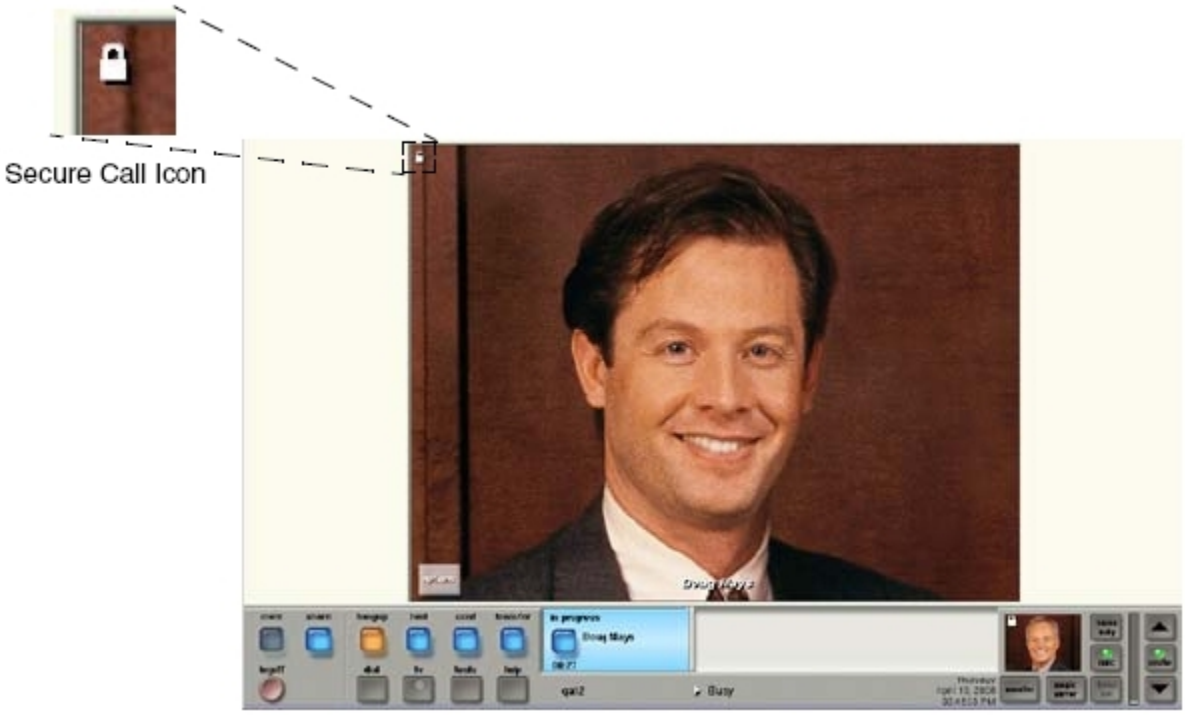

Figure 11: VMC Terminal Secure Call Status - Lock Icon

The absence of this lock icon would be an indicator to the Operator that the VMC Terminal is NOT operating in FIPS 140-2 Approved mode. However, the presence of this status icon does not necessarily indicate that the VMC Terminal is operating in FIPS 140-2 Approved mode since call encryption can be enabled by any user on their terminal even if "FIPS Mode" operations are not configured on the VAS (as explained in the previous section). As also noted, once a terminal has been properly configured to operate in FIPS 140-2 Approved mode, the Operator can NOT change this configuration on the terminal.

No crypto bypass capability is currently implemented in the ViPr Cryptographic Module. In FIPS 140-2 Approved mode, only secure (encrypted) calls to other parties can be made or received. Once an encrypted call has been created, it cannot add parties that do not support security, and a non-secure call cannot add parties that require security (those operating in FIPS 140-2 Approved mode). Any attempts to make "mixed-mode" calls will fail with a "Call could not be completed" message.

Acronyms

Table 6 - Acronyms

Acronym	Definition
AES	Advance Encryption Standard
CSP	Critical Security Parameter
CPU	Central Processing Unit
EMI	Electro-Magnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FSM	Finite State Machine
GUI	Graphical User Interface
KAT	Known Answer Test
LED	Light emitting diode
PRNG	Pseudo Random Number Generator
PSTN	Public Switched Telephone Network
PUB	Publication
RNG	Random number generator
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
UAM	Universal Audio Mixer
USB	Universal serial bus
VAS	ViPr Application Server
VMC	ViPr Media Center