CarrierAccess™

Broadmore/SSHield Management Module

Versions 4.0.0, 4.1.0, & 4.1.1

Security Policy

Document ENG-0016
Document Version *7.51*

Carrier Access Corporation

12/2/2005

TABLE OF CONTENTS

1. Module Overview

System Background

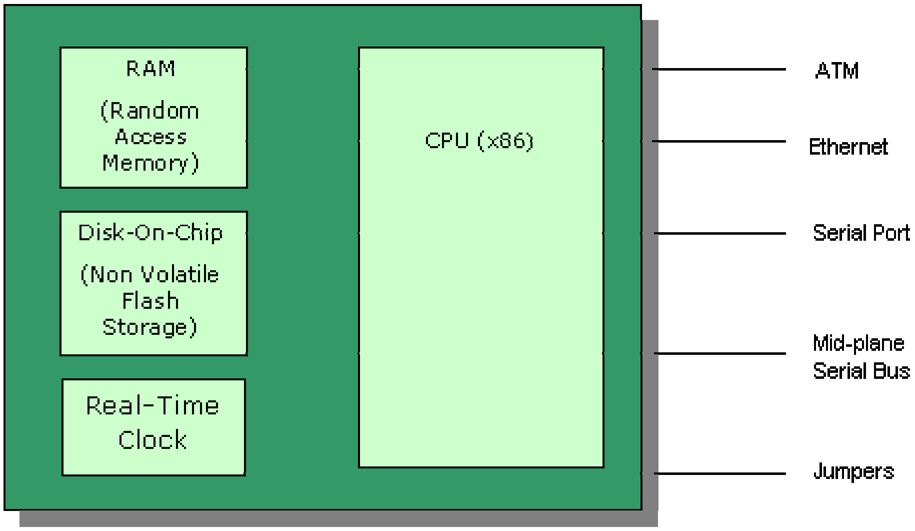
The Broadmore® family of products offers a unique economical means of provisioning, grooming, and routing services such as TDM DS3, DS1, E3, E1 and mixed-speed serial and cell data circuits to logical ATM connections. The cost and complexities of equipping and managing SONET and Digital Cross-Connect (DCS) circuits are replaced by the speed, capacity, and cost improvements of logical ATM circuit provisioning —leveraging existing SONET optical networks. TDM-to-ATM conversion is accomplished using standards-based ATM Circuit Emulation Service (CES) supporting both Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs). The integrity of voice, video and data traffic is maintained, while providing the benefits and efficiency of ATM transport for converged voice and data access networks. Designed to meet the specific needs of government, DoD, and Intel customers, the Broadmore supports asymmetrical data rates and encrypted networks and is the ideal platform for applications such as SATCOM extensions, supporting critical links, and secret and customized communications. It enables disaster recovery and circuit density improvements and supports network, global and local timing and the HSSI and CBI interfaces support Crypto re-sync for those environments that require added security. CPU mirroring, redundant power, network access and service protection are some of the additional reliability options that the Broadmore family of products provide.

Cryptographic Module

The Broadmore/SSHield Management Module is system management software and its primary business purpose is to manage the Broadmore models 500, 1700, and 1750 ATM configuration parameters in a secure manner while providing a user interface for operation and administration. The Broadmore/SSHield Management Module allows for the control and management of these parameters via a command line interface or a menu based interface, and provides security by the SSH (IETF SECSH) protocol to ensure that network connections are encrypted. The FIPS 140-2 Cryptographic Module for the Broadmore is a *software-only* module executing in a multi-chip embedded environment. This document describes security policies enforced by the device, as well as the policies imposed by Carrier Access Corporation ("vendor") to comply with the Federal Information processing Standard (FIPS) PUB 140-2 *Security Requirements for Cryptographic Modul*e. The Broadmore/SSHield Management Module meets the requirements of FIPS PUB 140-2 Level 1.

The following diagram shows the physical devices and ports accessed by the software-only Broadmore/SSHield Management Module and defines the physical boundary and interfaces of the cryptographic module:

Figure 1 – Block Diagram of Physical Boundary of Cryptographic Module



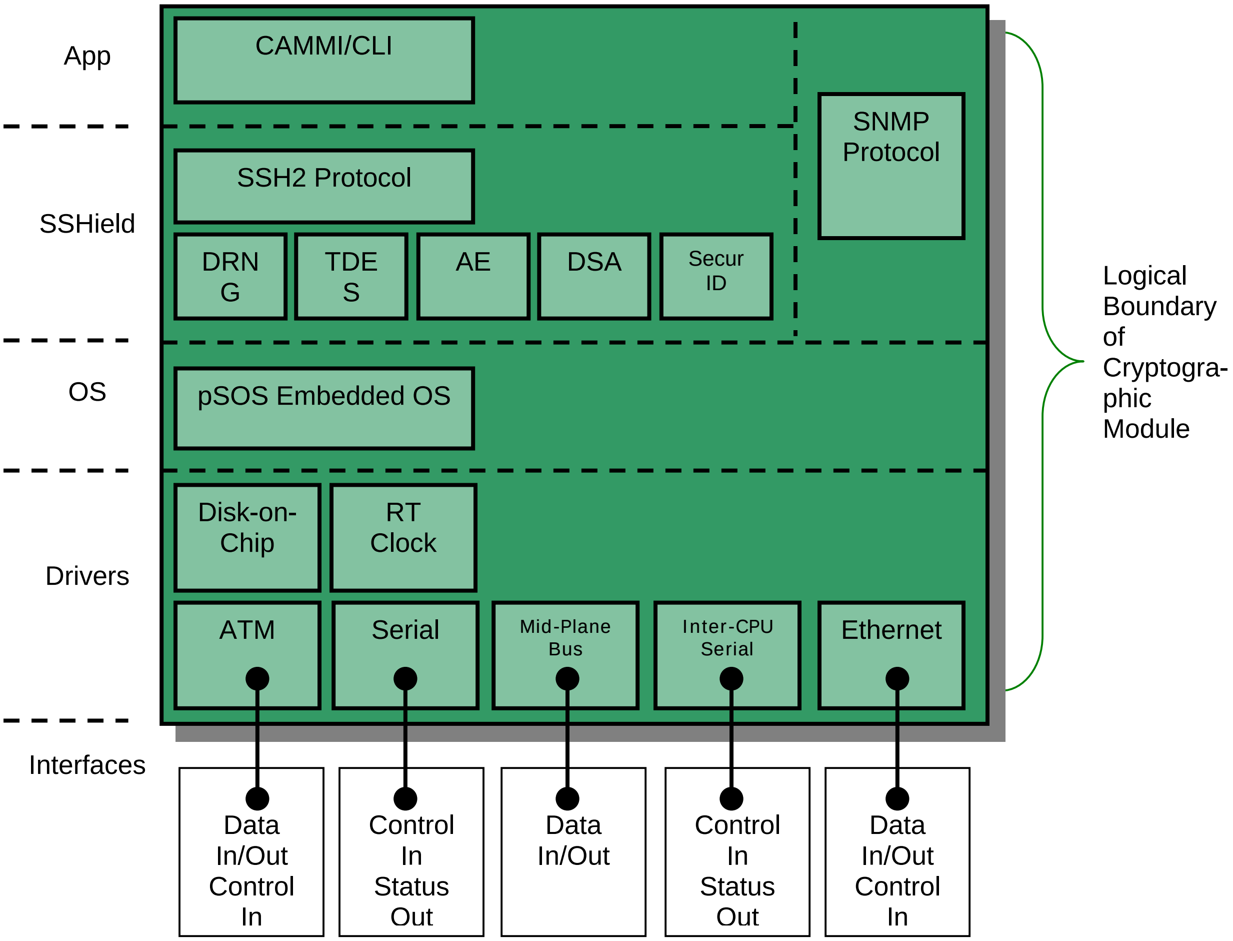
The Cryptographic Module consists of software that uses the following main components on the Broadmore "CPU" printed circuit board assembly:

- An Intel x86 general purpose microprocessor (CPU) that is responsible for executing machine code.
- RAM (Random Access Memory) that stores code for execution as well as data in a volatile fashion, so the CPU can access it and execute it or operate on it.
- A "Disk-on-Chip" non-volatile memory containing the binary image that is executed on power-up, an SSH cryptographic DSA key for identifying the board to the external world, user names and the corresponding SHA-1 hashed user passwords and other non-executable data files that need to be persistent across power cycles and reboots of the board. All stored CSP's are saved here.
- An ATM connection used to exchange management traffic encrypted and authenticated with SSHield's SSH implementation. Note that this is not the ATM dataplane traffic that is carried for the end-user, but only management traffic related to this CPU board carrier over a LANE (Lan Emulation) channel over ATM.
- An Ethernet port used to exchange management traffic encrypted and authenticated with SSHield's SSH implementation. Usually management traffic will be exchanged only over the LANE/ATM conection or the Ethernet port, so operation is identical from the software module's perspective.
- A Serial Port (called 'Craft port') used to manage the device from a console. Availability of this console port is only local to the physical location of the Broadmore equipment.
- A real-time clock used to generate timing events and also used by the Broadmore to seed the non-approved random number generator.
- A Mid-plane Serial Bus to Service & ATM Network cards carries bandwidth allocation and configuration messages from the CPU to the "data plane" cards in the chassis. This bus carries no security relevant information.

❖ Jumpers on the CPU used to provide a mechanical method to force a CPU reboot.

The following diagram shows the logical components of the Cryptographic Module. The border of the shaded box represents the logical boundary of the Cryptographic Module.

Figure 2 – Block Diagram of Logical Components



2. Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1 - Module Security Level Specification

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

3. Modes of Operation

Approved (FIPS) mode of operation

The Approved mode of operation uses username/password-based authentication over a secure channel. In addition to username/password, RSA SecurID® can be used. However, all FIPS 140-2 strength of authentication arguments are based on username/password arguments and SecurID is not relied upon.

The FIPS 140-2 validated mode of Broadmore/SSHield Management Module supports the following NIST certified algorithms:

- ❖ DSA (Certificate No. 100) with 1024 bit keys for digital signature generation and verification
- ❖ Triple-DES (Certificate No. 238) and AES 128/192/256 (Certificate No. 129) for encryption
- ❖ SHA-1 160-bit (Certificate No. 214)
- ❖ HMAC SHA-1 (Certificate No. 214, vendor affirmed)
- ❖ FIPS 186-2 DRNG Change Notice 1 (vendor affirmed)
- ❖ RSA (vendor affirmed, legacy self-test only, RSA is not used within the module)

The cryptographic module uses Diffie-Hellman Group 2 exchange for key establishment, and relies on a deterministic random number generator (DRNG) that is compliant with FIPS 186-2 change notice 1 with 160 bit Xkey and underlying G function constructed from SHA-1 for generation of all random numbers used by the module. The RSA algorithm confirms to PKCS #1.

FIPS mode of operation can be verified by the “show crypto status” service.

Non-FIPS mode of operation

Broadmore/SSHield Management Module supports a non-FIPS mode, which a customer may use when security is not as critical, or a FIPS 140-2 validated module is not a requirement. This mode is not an Approved Mode of Operation for the cryptographic module. Changing to FIPS mode (Approved) from non-FIPS (non-Approved) mode is supported by the Change FIPS Mode service. Changing from FIPS mode (Approved) to non-FIPS (non-Approved) mode can only be executed by a Superuser (Crypto Officer). Both changes include a reboot of the system and other specific steps taken internally by the system to ensure that the module conforms to FIPS 140-2 requirements for not sharing or making critical security parameters (CSPs) from one mode accessible in the other. These internal steps consist of the following:

- ❖ Encrypting the FIPS-mode plain-text CSPs (the host private key) with the FIPS approved AES-128 algorithm, when changing over from FIPS mode to non-FIPS mode using a FIPS-mode specific internal AES key that is part of the software image.
- ❖ Decrypting the FIPS-mode CSPs back to plain-text form (the host private key) with the FIPS approved AES-128 algorithm, when changing over from non-FIPS

mode to FIPS mode using the same FIPS-mode specific internal AES key that is part of the software image.

Similar encryption is performed on the non-FIPS mode CSPs when changing from non-FIPS mode to FIPS mode, and decryption is performed when changing over from FIPS mode to non-FIPS mode. The internal key that is part of the software image used for this purpose is a separate non-FIPS mode AES key.

The FIPS mode of operation of the cryptographic module only supports the FIPS approved algorithms, while the non-FIPS mode may use non-approved cryptography and other services. The Broadmore is initially shipped with factory default CSPs and with both FIPS mode and the SecurID mechanism disabled.

4. Ports and Interfaces

All management traffic carried over a network connection (LANE or Ethernet) is encrypted and authenticated using TeamF1's SSHield, which is a part of the Broadmore/SSHield Management module and is an implementation of the SSH (IETF SECSH) protocol v2 -- which includes authentication, strong encryption and message integrity checks.

A Mid-plane inter-CPU Serial Bus is used to coordinate data plane configurations with a “hot backup” CPU on the Broadmore 1700 and 1750 models. A Mid-plane Inter-Card Bus allows communication between multiple cards in the Broadmore chassis, including between the primary and "hot-backup" instances of the CPU module as well as between the primary CPU module and the other data plane cards. The Crypto Officer must set the Host Private Key on both CPUs to be the same using the Update Host Private Key service.

The following table describes the mappings between the physical interfaces on the Broadmore equipment, the Broadmore/SSHield Software Module logical interfaces and the Logical Interfaces identified by FIPS 140-2:

Table 2 – Physical and Logical Interface Summary

Software Module Logical Interfaces	Physical Interfaces (or Ports)	FIPS 140-2 Logical Interfaces
Local console input	Craft Serial Port	Control Input
Local console output		Status Output
SSH Protocol Input	Ethernet port, and Mid-plane Inter-Card bus (ATM ports using LANE)	Data Input
SSH Protocol Output		Data Output
RSA SecurID Ace Client Input		Data Input (plaintext)
RSA SecurID Ace Client Output		Data Output (plaintext)
Status from Cards	Mid-plane Inter-Card bus	Data Input (plaintext)
Configuration to Cards		Data Output (plaintext)
CPU to CPU Failover Status	Private Inter-CPU Serial bus	Status Output
CPU to CPU Failover Control		Control Input
SNMP Protocol Input	Ethernet port, and Mid-plane Inter-Card bus (ATM ports using LANE)	Control Input (plaintext)
SNMP Protocol Output		Status Output (plaintext)

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module supports distinct operator roles and enforces the separation of these roles using identity-based operator authentication. A username and password are always required to log in, whether or not the optional SecurID mechanism is enabled. The mandatory username is an alphanumeric string of characters whose minimum length can be set by the Crypto Officer (see section 8 for minimum values). The password is a string of characters from the 94 printable and human-readable characters whose length can be set by the Crypto Officer (see section 8 for minimum values). Upon successful authentication, the role and privilege-level is selected based on the identity (username) of the operator. At the end of a session, the operator should log-off. However, the user is automatically logged off after a configurable period of inactivity (see section 8 for minimum value).

Table 3 - Roles and Required Identification and Authentication

Role	Privilege Level	Type of Authentication	Authentication Data
User	Browser, Operations, SysAdmin	Identity-based operator authentication	Username and Password
Crypto Officer	Superuser	Identity-based operator authentication	Username and Password

Since this is a software module with no maintenance interface, there is no provision for a Maintenance role.

Table 4 –Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	The minimum length of the username is 6 while the total number of acceptable characters is 94 which implies that the probability a random attempt will succeed or a false acceptance will occur is 1/689,869,781,056. The minimum length of the password is 6 while the total number of acceptable characters is 94 which implies that the probability a random attempt will succeed or a false acceptance will occur is 1/689,869,781,056. On unsuccessful username/password combinations, after 3 failed attempts, the system introduces a delay of 10 seconds during which no authentication can be attempted. Assuming the worst case condition (i.e. entering a username/password combination takes zero time), this implies the probability of successfully authenticating to the module within 1 minute is 1/38,326,098,947

6. Access Control Policy

Services

The cryptographic module provides the following authenticated services:

Table 5 - Authenticated Services

Service #	Service Name	Description
U01	Execute Self Tests	This service executes self-tests.
U02	Execute KATs	This service executes known-answer tests.
U03	Establish Session Keys	This service establishes session keys using Diffie-Hellman Group 2 exchange.
U04	Encrypt Data	This service encrypts plaintext data passed into the cryptographic module before sending the data over the network. It uses the 3DES or AES algorithm and Session Key.
U05	Decrypt Data	This service decrypts encrypted data passed into the cryptographic module. It uses the 3DES or AES algorithm and Session Keys.
U06	Authenticate Data packets	This service runs each packet through a vendor affirmed hashed message authentication code (HMAC) check for data integrity.
U07	Verify Signature	This service verifies the digital signature of signed data with DSA using the CAC Public Key.
U08	Logout	This service logs out the currently logged-in user.
U09	Show Crypto Status	Shows the status of the crypto module. Displays whether the FIPS mode is active or not, the FIPS library version, and the image build date.
U10	Configure ATM parameters	This service sets parameters for ATM-side of the traffic (outside the crypto boundary).
U11	Change password	This service allows a user to change password.
U12	System diagnostic display	Each record in the log has a minimum privilege level marked for viewing. Users are only shown records they are authorized to see.
CO01	Create User	This service creates a new user.
CO02	Delete User	This service deletes an existing user.
CO03	Modify User	Allows the user to change the following attributes of a user: Name, Password, Privilege Level, Remote Access Permission, Craft Access Permission.
CO04	File Transfer	Transfer configuration files, software executable image, DSA private key and non-security relevant files over encrypted SSH2 channel.
CO05	Update software	Upgrade the device to the newly downloaded software.

Service #	Service Name	Description
CO06	Update host private key	This service allows crypto officers to change host private key by supplying a key from outside of the crypto module using SFTP. There are no seed keys being used.
CO07	Restore factory defaults	This service allows crypto officers to reset user name/password file to the factory default value.
CO08	Synchronization	This service synchronizes user data and other application data with stand-by module to ensure high availability of services to device end users.
CO09	FIPS Zeroize global	This service actively zeroizes all Critical Security Parameters (CSPs) and reformats the Disk on Chip Flash memory on both CPUs in a redundant system.
CO10	FIPS Zeroize standby	This service actively zeroizes all Critical Security Parameters (CSPs) and low-level formats the Disk on Chip Flash memory on the standby CPU in a redundant system (to allow it to be removed for maintenance).
CO11	FIPS Mode change	This service is used to change to non-FIPS mode. All CSPs are converted back to factory defaults or encrypted for later FIPS mode use upon execution.
CO12	Constrain User List	This service sets a minimum length for the username and passwords. It does not affect existing entries; only subsequent creation or modification of usernames and passwords. This value is saved in non-volatile storage and mirrored as necessary to the backup CPU, but is distinct from the User List itself.
CO13	Display SSH Status	Show status of SSH – includes connection information and SSH configuration information.

Unauthenticated Services

The crypto module does not provide any unauthenticated services except for self-test services that are executed automatically during power-up and non-security related services associated with the business function of the device.

SNMP is one of the unauthenticated services offered by the module. SNMP service is also available in the FIPS approved mode of operation for Broadmore/SSHield Management Module Release 4.1.0 and above. SNMPv3 uses cryptographic services in the module, but its use of cryptography (whether using FIPS approved algorithms or not) is only included to support the underlying protocol, and does not provide any data confidentiality or protection. Hence it is treated as a plain-text service and is subject to the restrictions required of a plain-text port in a FIPS 140-2 Level 1 validated module, including that no CSPs be accessible via this port. All implementations of FIPS-approved cryptographic algorithms in use are ones that already have FIPS 140-2 certificates.

Roles and Services

Several operator roles (which determine user privileges) are defined for the Broadmore. The general philosophy is that each increased privilege level adds more capabilities to the allowed set. Note that except for the "Superuser" privilege level (equivalent to the Crypto Officer Role), all other privilege levels are normal User roles as defined in FIPS 140-2 specifications. There is no Maintenance role required or specified. The defined roles are:

Table 6 – Services Authorized for FIPS Mode Roles

Role	Authorized Services
User: Browser – Is able to look at most all data plane information; able to affect nothing. To protect security data, no file access is permitted. This role cannot access the “security” settings. Operations – Is able to perform data plane configurations, such as defining PVCs, SVCs, configuring service card parameters. To protect security data, no file access is permitted under this privilege level. This role cannot access the “security” settings. SysAdmin – Is able to perform global configuration operations such as redundancy. To protect security data, no file access is permitted. This role cannot access the “security” settings.	The services numbered U01-U12 are used by this role. This role is not allowed to use CO01-CO13 services.
Crypto Officer: Superuser – This role is required to maintain system accounts, use SFTP, and alter security settings. Only users at this privilege level may turn FIPS mode on or off.	This role is authorized to use services numbered U01-U12 and CO01-CO13.

Table 7 - Specification of Service Inputs & Outputs

Service Name	Control Input	Data Input	Data Output	Status Output
Execute Self Tests	CLI Command.	None	None	Success/fail
Execute KATs	CLI Command or power-on event	Known plaintext and ciphertext	Known ciphertext and plaintext	Success/fail
Establish Session Keys	Header info.	Plaintext data	Plaintext data	Success/fail

Encrypt Data	Header info.	Plaintext data	Ciphertext data	Success/fail
Service Name	**Control Input**	**Data Input**	**Data Output**	**Status Output**
Decrypt Data	Header info.	Ciphertext data	Plaintext data	Success/fail
Authenticate Data packets	Header info.	Plaintext data	Keyed Message Digest	Success/fail
Verify Signature	Power-on event	Plain text data (software image), public key and signature	None	Success/fail
Logout	Header info or CLI command	None	None	Session close
Show Crypto Status	CLI Command	None	None	Status of crypto module
Configure ATM parameters	CLI Command	Plain text data	None	Success/fail
Change password	CLI Command	Plain text data	Hashed password data	Success/fail
System diagnostic display	CLI Command	None	None	Status of diagnostics
Create User	CLI Command	Plain text data	Plain text data	Success/fail
Delete User	CLI Command	Plain text data	None	Success/fail
Modify User	CLI Command	Plain text data	Plain text data	Success/fail
File Transfer	Header info	Plain text data	Plain text data that is transferred as Ciphertext data	Success/fail
Update software	Header info	Plain text data	Plain text data that is transferred as Ciphertext data	Success/fail
Update host private key	Header info	Plain text data	Plain text data that is	Success/fail

Service Name	Control Input	Data Input	Data Output	Status Output
			transferred as Ciphertext	
Restore factory defaults	CLI command or hardware-triggered event (shorting jumpers)	Plain text data	Plain text data	Success/fail
Synchronization	CLI command or external event	Plain text data	Plain text data	Success/fail
FIPS Zeroize global	CLI command	None	None	Success/fail
FIPS Zeroize standby	CLI command	None	Plain text data	Success/fail
FIPS Mode change	CLI command	Plain text data for private key	Cipher text data for private key	Success/fail
Constrain User List	CLI command	Plain text data	None	Success/fail
Display SSH Status	CLI command	None	None	SSH status

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- Host DSA Private Key: This is the private part of the host's DSA Public/Private key pair that is unique to each crypto module instance and identifies it. The client uses the corresponding public key to verify that it is communicating with the specific Broadmore/SSHield Management Module instance. This key is stored on the disk-on-chip device, and starts off with a factory-default value that is installed in each crypto module that is shipped and can be updated over the SSH-encrypted channel at any time by the Crypto Officer. It is destroyed when the zeroize functionality is invoked. The only entity associated with the host private key in the Broadmore/SSHield module is the module itself, and there is no way to invalidate this association. The Host DSA Private Key is unique per module and is not mirrored between the active and standby CPUs.
- Session Keys and IV's: The session keys and IV's are established using Diffie-Hellman (DH) exchange and are used to encrypt/decrypt/MAC all data exchanged between the client and the cryptographic module. Also, the DH exchange is session-specific and hence each SSH connection exchanges a new set of keys and IV's. This ensures that different authenticated users and hence roles are separated since they effectively use channels encrypted by different keys and IV's for the approved symmetric algorithms on the cryptographic modules. Session Keys and IV's are not stored in any persistent medium and

are not mirrored between the active and standby CPUs.

The key material exchanged during DH results in the following:

- The key used by the symmetric key algorithms (AES, TDES) for encryption and decryption
- The IV (initialization vector) used by the Symmetric key algorithms AES and TDES
- The message digest key

- Passwords: The password of the user used in authenticating the user. All users are authenticated using user's name and password. Whenever a password is entered in the module, it is immediately hashed using the FIPS-approved SHA-1 hashing algorithm. In case a new user is being added or existing user credentials are being modified, this hashed password is stored in the authentication database. In case of the authentication process this hashed password is compared to passwords in the authentication database. The FIPS-approved SHA-1 hashing algorithm is used to protect the passwords in the authentication database, so that this security sensitive information is not in plain-text form when it is mirrored from the active CPU to the standby CPU.
- Mode Switch CSPs: The FIPS to Non-FIPS mode switchover (and vice-versa) involves encrypting/decrypting the host private key. The encryption/decryption is done using the AES algorithm. The AES Key and IV used in the process are hard-coded in the Broadmore/SSHield module and are identified as CSP's. These values are protected as they are part of the Broadmore/SSHield module image and are neither displayed, nor updated during the operation of the module. Also, these values are not accessible by any function other than the core routines responsible for encryption and decryption of the host private key. Mode Switch CSPs are not mirrored between the active and standby CPUs.

Definition of Public Keys

The following are the public keys contained in the module:

- Host DSA Public Key: This is the public part of the host's Public/Private key pair. The host public key is embedded the host DSA private key file. When a client make an SSH connection to the Broadmore/SSHield Management Module, this key is sent to the client. The client uses this public key to verify that it is talking to the right Broadmore/SSHield Management Module. The Host DSA Public Key is unique per module and is not mirrored between the active and standby CPUs.
- CAC Public Key: This is the public part of the digital signature verification Public/Private key pair. The client uses this public key to verify that the software version installed on the Broadmore/SSHield Management Module is pristine. The private key corresponding to this key is maintained by Carrier Access (outside of the crypto module). The private key is used for signing the binary executable images that can be loaded on the Broadmore. The CAC Public Key is installed by the factory on each module and is not mirrored.

Definition of CSPs Modes of Access

Table 8 below defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Establish Session Key: The session key is established using Diffie-Hellman (DH) exchange and are used to encrypt/decrypt all data exchanged between the client and the cryptographic module. This operation is initiated when a client establishes an SSH session with the Cryptographic module.
- Establish Session IV: The session IV is established using Diffie-Hellman (DH) exchange and are used to encrypt/decrypt all data exchanged between the client and the cryptographic module. This operation is initiated when a client establishes an SSH session with the Cryptographic module.
- Encrypt Data using Session Key/IV: This operation encrypts all data sent from the cryptographic module to the client using the Session Key and IV.
- Decrypt Data using Session Key/IV: This operation decrypts all data sent from the client to the cryptographic module using the Session Key and IV.
- Encrypt negotiation data using Host Private Key: The Diffie-Hellman (DH) exchange uses the Host Private Key to encrypt negotiation information sent from the cryptographic module to the client.
- Decrypt negotiation data using Host Private Key: The Diffie-Hellman (DH) exchange uses the Host Private Key to decrypt negotiation information sent from the client to the cryptographic module.
- Destroy Session Key: This operation erases the Session Key that was used to encrypt the messages sent from the cryptographic module to the client during an SSH session. This operation is performed once an SSH session is terminated or in case zeroize is called during an active SSH session.
- Destroy Session IV: This operation erases the IV that was used to encrypt the messages sent from the cryptographic module to the client during an SSH session. This operation is performed once an SSH session is terminated or in case zeroize is called during an active SSH session.
- Hash Password: This operation creates a SHA-1 hash of the password entered by a user during authentication or entered via cammi while changing user credentials. This hash'ed password is then added to the authentication database.
- Read Host Private Key: This operation is performed during the DH exchange.
- Encrypt Host Private Key: This operation is performed during the switch from FIPS to Non-FIPS mode.
- Destroy Host Private Key: This operation is performed as part of the zeroization process or in case factory defaults are restored.
- Decrypt Host Private Key: This operation is performed as part of the switch from Non-FIPS to FIPS mode.
- Read FIPS mode switch Key: This operation is performed during the switch from FIPS to Non-FIPS mode. The key is used to encrypt the Host Private Key.
- Read FIPS mode switch IV: This operation is performed during the switch from FIPS to Non-FIPS mode. The IV is used to encrypt the Host Private Key.
- Destroy FIPS mode switch Key: This operation is performed as part of the zeroization process.
- Destroy FIPS mode switch IV: This operation is performed as part of the zeroization process.

- Read CAC Public Key: This operation is performed during the Image Signature Verification Self Test.
- Destroy CAC Public Key: This operation is performed as part of the zeroization process.

Table 8 - CSP Access Rights within Services

Service	Cryptographic Keys and CSPs Access Operation
Execute Self Tests	None
Execute KATs	None
Establish Session Keys	Encrypt negotiation data using Host Private Key Decrypt negotiation data using Host Private Key
Encrypt Data	Encrypt Data using Session Key/IV
Decrypt Data	Decrypt Data using Session Key/IV
Authenticate Data packets	None
Verify Signature	Read CAC Public Key
Logout	Destroy Session Key Destroy Session IV
Show Crypto Status	None
Configure ATM parameters	None
Change password	Hash Password
System diagnostic display	None
Create User	Hash Password
Delete User	None
Modify User	Hash Password
File Transfer	Establish Session Key Establish Session IV Encrypt Data using Session Key/IV Decrypt Data using Session Key/IV Hash Password
Update software	Establish Session Key Establish Session IV Encrypt Data using Session Key/IV Decrypt Data using Session Key/IV Hash Password

Service	Cryptographic Keys and CSPs Access Operation
Update host private key	Establish Session Key Establish Session IV Encrypt Data using Session Key/IV Decrypt Data using Session Key/IV Hash Password
Restore factory defaults	Destroy Host Private Key
Synchronization	None
FIPS Zeroize global	Destroy Session Key Destroy Session IV Destroy Host Private Key Destroy FIPS mode switch Key Destroy FIPS mode switch IV Destroy CAC Public Key
FIPS Zeroize standby	Destroy Session Key Destroy Session IV Destroy Host Private Key Destroy FIPS mode switch Key Destroy FIPS mode switch IV Destroy CAC Public Key
FIPS Mode change	Read FIPS mode switch Key Read FIPS mode switch IV Encrypt Host Private Key (FIPS to Non-FIPS)
Constrain User List	None
Display SSH Status	None

Key Management

The SSH protocol uses the Diffie-Hellman (DH) Group 2 key exchange for secure establishment of session keys. DH Group 2 has 1024 bits of keying material and these 1024 bits are considered to provide 80 bits of security.

The Broadmore/SSHield Management Module supports only the AES and TDES symmetric key cryptographic algorithms and the keys for these algorithms are exchanged as a part of the DH exchange. The only CSP that passes over an external port is a 1024-bit DSA private key from a client to the Broadmore board when a Crypto Officer wants to update the host private key for the module. If any of these symmetric-key ciphers in the Broadmore/SSHield Management Module is being used for encryption of the channel, it is stronger than the CSP (1024-bit DSA private key) being transferred.

7. Operational Environment

The Broadmore/SSHield Management Module runs on the pSOS embedded operating system (version 2.2.7). The cryptographic module is an executable binary image executed on the Broadmore hardware that includes pSOS and other software with non-security functionality.

The binary image is stored on disk-on-chip along with a digital signature, and the signature is verified at boot time.

The Broadmore/SSHield Management Module permits only one user to use the system at a time.

8. Security Rules

The Broadmore/SSHield Management Module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 validated module.

- The cryptographic module provides two distinct FIPS 140-2 operator roles. These are User and Crypto Officer. These role definitions have specific operator privileges associated to them. The User role has three associated privilege levels; Browser, Operations, and SysAdmin. The Crypto Officer role has Superuser privileges. (Table 5 lists a description of each role and the services performed).
- The cryptographic module provides identity-based authentication based on User names assigned to each of these roles.
- The Broadmore/SSHield Management Module requires two inputs to authenticate users: user name and password. These parameters are encrypted using the TDES algorithm before being sent by the client to the cryptographic module. The user name and the SHA-1 hashed user password are compared against user name/SHA-1 hashed password database, and the user is allowed to use the system only after this check is successful. A SecurID token value entry is optionally required before allowing for authentication to allow the username/password authentication phase to proceed. This mechanism is optional and is not relied upon for providing any authentication strength.
- The Broadmore/SSHield Management Module encrypts all message traffic using the TDES and AES algorithms, and uses vendor affirmed HMAC-SHA1 message integrity checks on each data packet of the traffic. Enabling and disabling the FIPS mode of operation can only be done by the Crypto Officer using the FIPS Mode Change service. The Crypto Officer should ensure that all minimum values are set per Table 9 before initiating FIPS mode. The Crypto Officer should validate that FIPS mode initiated properly by reviewing the FIPS Status.
- Only a Crypto Officer (SuperUser) can change the security modes. The Broadmore is shipped from the factory with FIPS mode turned off. The security mode can only be changed after successfully logging into the Broadmore for the first time. Changing into FIPS mode requires following *all* the steps of the procedure given below:

  <u>Step 1</u>

  Run the command fipsmode with the argument 'on', on the Broadmore prompt to turn FIPS mode on.

  <u>Step 2</u>

  Set the username and password length parameters according to their minimum specified in Table 9. Note that the SSH session timeout minimum is enforced automatically by the module. In addition, to set the Craft port pShell session timeout, use the command 'settimeout' on the Broadmore prompt.

  <u>Step 3</u>

  Reboot the module to bring the changes into effect. When the module boots up it will be in the FIPS mode.

Steps 1 ensures that the module only uses FIPS mode algorithms as specified in Section 3. Step 2 ensures that configuration options listed in Table 9 are set accordingly for the FIPS mode of operation.

- ❖ To find out whether the module is in FIPS mode or in Non-FIPS follow the steps given below…

  Step 1

  Use the menu item *Help→About Security*. Any user regardless of his role can use this command. This menu item displays the message "FIPS Mode Active" when the module is in FIPS mode and the message "Security inactive; non-FIPS mode" when the module is in Non-FIPS mode.

  Step 2

  Check that the username and password length parameters satisfy the minimums as specified in Table 9. The current Craft port pShell session timeout value can be found out by running the command 'settimeout' from the Broadmore prompt.

- ❖ If the minimums are staisfied (Step 2 above) and the module indicates "FIPS Mode Active" (Step 1 above), then the module is considered to be in the FIPS mode of operation.
- ❖ The Broadmore/SSHield Management Module performs the following tests:

A. Power up Self-Tests

- ❖ Cryptographic algorithm tests:
  - ❖ AES Known Answer Test confirms the AES algorithm functionality using 128, 192 and 256 bit keys.
  - ❖ DES Known Answer Test (part of the TDES KAT – DES is not used by itself) tests the DES algorithm using 64-bit (including parity) keys
  - ❖ TDES Known Answer Test tests the TDES algorithm using 192-bit (including parity) keys.
  - ❖ SHA-1 Known Answer Test tests the SHS algorithm with a 160-bit hash
  - ❖ Vendor affirmed HMAC-SHA1 Known Answer Test tests the HMAC-SHA1 algorithm
  - ❖ DSA Pair-wise Consistency Test tests the DSA algorithm with a 1024-bit key pair
  - ❖ RSA Known Answer Test (though RSA encryption is tested, it is never used in the module and is not available by any service in FIPS mode)
- ❖ Software Integrity Test (DSA signature verification)
- ❖ Random number generator tests: The TeamF1 FIPS 186-2 change notice 1 DRNG executes a known answer test (KAT).

B. Conditional Self-Tests

- ❖ Continuous Random Number Generator (DRNG) tests as described below are run every time the respective random number generator is used during the operation of the module. The TeamF1 FIPS 186-2 change notice 1 DRNG runs an internal check every time it is executed to verify that two consecutive numbers of 16 bits or more are not identical, and fails if they are. The non-approved DRNG runs a similar test every time it is executed as well.

- ❖ A self-test using a KAT is run when the Continuous Random Number Generator test indicates a failure. If the KAT fails, the module enters an error state; otherwise it reverts back to normal operation.
- ❖ The Execute Self Test service can be used to invoke all of the Known Answer Tests and the DRNG self-test on-demand.
- ❖ Software Load Test: External software cannot be loaded onto this module and run. Only a complete software upgrade using an updated signed image loaded by the Crypto Officer into the module via a secure, authenticated connection is allowed.

The results of all self tests, for both power-up and conditional, are recorded in the system log or are output to the local console. This includes logging both passing and failing results.

This section documents the security rules imposed by the vendor:

- ❖ The module does not support the update of the logical serial number or vendor ID.
- ❖ The module only supports a single user at a time when operating in FIPS mode.
- ❖ If the cryptographic module remains inactive in any valid role, the module automatically logs the operator off. The time value for automatic log off is configurable at customer site, but the customer must set the minimum value (see table below) to be FIPS 140-2 compliant.
- ❖ The Broadmore's flexible design allows configuration of a number of parameters that must be procedurally reviewed and controlled. The following table shows the minimum values for these parameters to remain FIPS 140-2 compliant. The Crypto Officer must ensure that these minimums are met for the module to be FIPS 140-2 compliant.

Table 9 –Parameter Minimums to Meet FIPS 140-2

Parameter	Minimums for FIPS 140-2
Duration of inactive session before the user is logged out automatically	5 min
User name length	6 characters
User password length	6 characters

- ❖ To remain FIPS 140-2 compliant, the Crypto Officer must not overwrite the FIPS binary image on Disk-on-Chip with any other executable image. Software upgrades must be performed using new FIPS 140-2 validated versions from the vendor.
- ❖ The Broadmore is initially shipped from the factory with FIPS mode and SecurID Disabled and factory default CSPs installed. The Crypto Officer must change CSPs and ensure FIPS mode is enabled per the Security chapter of the Users Manual to place the module into FIPS mode and to be FIPS compliant.

- All CPU units sent to the vendor for repair or upgrade will be returned with factory default keys and CSPs installed.
- The Broadmore/SSHield Management Module does not perform key generation. The Crypto Officer is responsible for supplying the host private key using the update host private key service.

9. Physical Security Policy

Physical Security Mechanisms

None

Operator Required Actions

None

10. Design Assurance

Testing of the Broadmore to the specifications stated herein occurred at the offices of TeamF1, Inc., 39159 Paseo Padre Parkway, #121, Fremont, California, 94538 with the participation of the vendor, Carrier Access Corporation, 5395 Pearl Parkway, Boulder, Colorado, 80301.

The Broadmore/SSHield Management Module version 4.1.0 was tested on a Broadmore 1700 unit. The Broadmore 1750 and 500 use the same Cryptographic module as the Broadmore 1700. Broadmore 1750 differs from the 1700 only by non-security relevant SAM protection and Broadmore 500 does not accommodate a redundant CPU unit.

11. Mitigation of Other Attacks

The Broadmore/SSHield Management Module is not designed to mitigate any specific attacks and no additional security mechanisms have been implemented or tested.

12. References, Definitions, Glossary and Acronyms

References

- ❖ Broadmore 1750, 1700 and Broadmore 500 Users manuals.
- ❖ FIPS PUB 140-2, "Security Requirements for Cryptographic Modules."

Definitions and Glossary of Terms

Asynchronous Transfer Mode	A fast, cell-switched transmission technology based on a fixed-length 53-byte cell combining the best advantages of both circuit switching (for constant bit rate services) and packet switching (for variable bit rate services) that provides guaranteed service levels.
Network Interface Module	Functional module used by the Broadmore to communicate with the network typically by cell or ATM
Service Access Module	Functional module used by the Broadmore to communicate with TDM, voice, data, video and cell devices.
Time Division Multiplex	A technique for transmitting a number of separate data, voice, and/or video signals simultaneously over one communications medium by quickly interleaving a piece of each signal one after another.

Acronyms

AES - Advanced Encryption Standard

ATM – Asynchronous Transfer Mode

CPU – Central Processing Unit

CSP - Critical Security Parameter

DES/TDES - Data Encryption Standard / Triple-DES

DH – Diffie-Hellman

DSA - Digital Signature Algorithm

HMAC-SHA1 - Hashed Message Authentication Code - Secure Hash Algorithm 1

IV – Initialization Vector

LANE - Local Area Network Emulation

NIM – Network Interface Module

SHA1 - Secure Hash Algorithm 1

SAM – Service Access Module

TDM – Time Division Multiplex