# Security Policy:
# IP Dynamics, Inc. VCN Software Suite
# VCN Manager Cryptographic Module

Public Version 1.1

 

# Document History

This document was prepared by Farid Elwailly, Zulfikar Ramzan, and Vikki Wei.

# Table of Contents

# 1

# Introduction and Overview

## 1.1 Purpose

This document is a FIPS 140-2 Security Policy for the VCN Manager Cryptographic Module for IP Dynamics' VCN Software Suite. This security policy describes how the VCN Manager Cryptographic Module meets all FIPS 140-2 level-1 requirements.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2) is a U.S. government standard entitled "Security Requirements for Cryptographic Modules." This standard mandates the security requirements that should be satisfied by a cryptographic module.

## 1.2 References

- FIPS 140-2 Security Requirement for Cryptographic Modules
- FIPS 186-2 Appendix 3 Random Number Generation For The DSA
- RFC2401 IPsec Architecture
- FIPS 180-1 (SHA-1)
- FIPS 197 (AES)
- FIPS 46-3 (Triple DES)
- FIPS PUB 198 (HMAC-SHA-1)
- Solaris 8 Security Target

This document concentrates on the security policy for the VCN Manager Cryptographic Module, a software library (combination of shared objects, executables, and configuration files) used by the VCN Software Suite. You may find more product information about the VCN Software Suite at: http://www.ipdynamics.com

## 1.3 Product Overview

The IP Dynamics' VCN Software Suite creates a network services layer above the flat Internet address space allowing for the creation of dynamic

communities. This layer facilitates the introduction of a variety of policy-based network services with centralized management such as Virtual Private Networks, IP-telephony domains, and IP-based PDA communities.

VCNs, or Virtual Community Networks, are dynamic groups of individual workstations and other network resources that share an integrated set of IPsec policies, naming conventions, and directory resources. The basic VCN function allows systems to make secure, peer-to-peer, connections with other systems, regardless of the placement and addressing of the peers. VCN administrators create VCNs on an as-needed basis and do not need to be acquainted with the underlying network architecture of member systems and resources.

The VCN Software Suite consists of many software components, including the VCN Member Agent Software, the VCN Group Agent Software, and the VCN Manager Software. The VCN Member Agent and the VCN Group Agent Software use the *VCN Agent Cryptographic Module Version 4.2* and the VCN Manager Software uses the *VCN Manager Cryptographic Module Version 4.2* for cryptographic operations including random key generation, message authentication and verification, hashing, and encryption/decryption.

The VCN Manager Cryptographic Module is a software-only module with a multi-chip stand-alone embodiment that meets the overall requirements applicable to FIPS 140-2 security level 1.

| Security Requirements Section | Level |
|---|---|
| Cryptographic Module Specification | 1 |
| Module Ports and Interfaces | 1 |
| Roles, Services and Authentication | 1 |
| Finite State model | 1 |
| Physical Security | N/A |
| Operational Environment | 2 |
| Cryptographic Key Management | 1 |
| EMI/EMC | 3 |
| Self-Tests | 1 |
| Design Assurance | 1 |
| Mitigation of Other Attacks | N/A |

*Table 1.1 – Module Security Level Specification*

# 2

# Design and Functionality

The VCN Software Suite is a product that provides dynamic peer-to-peer Virtual Private Network connections on demand. Groups of member computers are brought together into virtual community networks, called VCNs, abiding by a community IPsec Policy. Management of the membership and the IPsec policy resides with a VCN Manager.

The system has the following features:

*Member to VCN Manager Connections:*

- Member-to-server connections are protected using IPsec.

*Member to member connections*

- Member-to-member connections are protected using IPsec where the AH and ESP keys are derived from the Internet Key Exchange (IKE) protocol.

*Source of Keying Material*

- From a cryptographic perspective, the source of keying material is a FIPS-approved PRNG that runs in both the VCN Manager and the member.

## 2.1 List of Algorithms

The VCN Manager Cryptographic Module includes the following algorithms:

- Key agreement using the Diffie-Hellman protocol
- Hashing using SHA-1 (FIPS PUB 180-1)
- Encryption/Decryption of data using AES in CBC mode with 128-bit keys (FIPS PUB 197)

- Message Authentication using HMAC-SHA-1-128 with a minimum of a 128-bit key (FIPS PUB 198)

The module only has a FIPS mode of operation; there is no non-FIPS mode.

## 2.2 The PRNG

The cryptographic module implements the FIPS 140-2 approved FIPS 186-2 Appendix 3 PRNG.

## 2.3 Mode of Operation

The VCN Manager Cryptographic Module has only one mode of operation while running. It is either running in secure mode or, if an error occurs, it is halted. There is no crypto bypass mode or maintenance mode of operation.

Successfully starting the software as indicated by the instructions provided in the Crypto Officer's user manual either results in the secure mode of operation or results in a halt condition with error message. The module relies on the trusted operating system for auditing events required under Section 6 – Operational Environment of FIPS 140-2.

# 3

# The Cryptographic Module

## 3.1 Physical Module Boundary

The cryptographic module physical boundary lies at the outer case of a general-purpose platform with the following basic configuration. General-purpose computers have enclosures that will completely surround the module. The actual hardware platform used may vary, but is **limited exclusively** to one of the platforms listed in Section 3.2 below.

# 3.2 Minimum System Requirement

| Characteristics | Value |
|---|---|
| Platform | **Hardware platform limited exclusively to one of the following:**<br>• Sun Ultra 1 Model 170 with UltraSPARC I 166MHz<br>• Sun Ultra 10 with UltraSPARC IIi 333MHz<br>• Sun Enterprise E450 with UltraSPARC II 300MHz<br>• Sun Enterprise E4500 with Dual UltraSPARC II 336MHz<br>• Dell OptiPlex GXa with Pentium II 233MHz<br>• Dell OptiPlex GX1 with Pentium III 500MHz<br><br>Note that while the Sun Ultra 10 with UltraSPARC IIi 333MHz was used during FIPS 140-2 operational testing, any of the hardware platforms listed above may be used. |
| Operating System | Sun Solaris Version 8 First Customer Shipment (FCS)<br>AdminSuite Version 3.0.1 FCS<br>with patches:<br>- 108875-07 and 108879-02 for SPARC platforms<br>- 108876-07 and 108881-02 for Pentium platforms<br><br>Please see Solaris 8 Security Target for details |
| | |
| Memory | 1 GB RAM |
| Free Hard Disk Space | 9 – 36 GB (Depending on the database) |
| CD-ROM | Any |
| NIC | 100 Mbps Ethernet card |
| Video Card | 1024 x 768, 16 bit color PCI graphics card |

# 3.3 Software Module Boundary

The VCN Manager Cryptographic Boundary includes:

1. The VCN Manager Cryptographic Module (including JDK1.4.0)
    - 2.The following operating system:Solaris Version 8 First Customer Shipment (FCS); AdminSuite Version 3.0.1 FCS with patches: 108875-07 and 108879-02 for SPARC platforms; 108876-07 and 108881-02 for Pentium platforms.

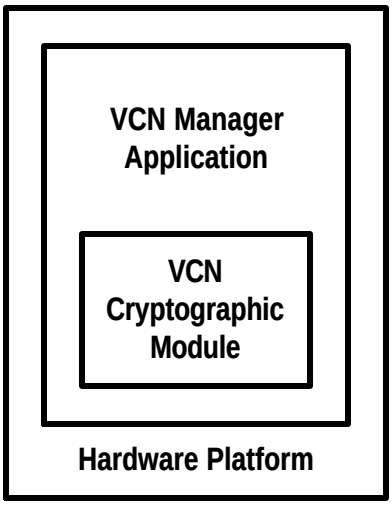


*Figure 3.2 VCN Manager Cryptographic Module Software Boundary*

## 3.4 Module Interfaces

The VCN Software logical interfaces comprise data input, data output, control input, and status output. The interfaces are separated by GUI fields and controls. **As this is a software only module, the actual interface to the module is cryptographic module API.**

# 4

# Roles, Services, and Authentication

Every operator is given one of three roles: VCN Manager Administrator role, VCN Member role, or VCN Administrator role.

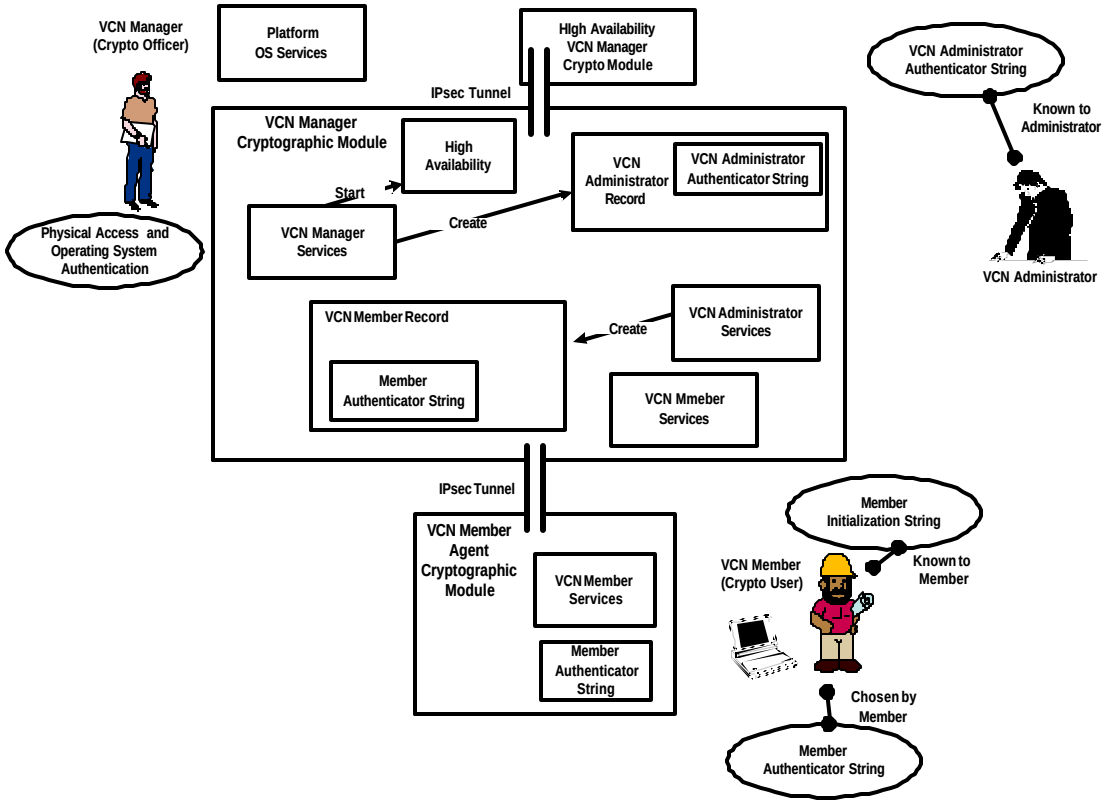


*Figure 4.1 VCN Software Suite Crypto Roles and Authentication*

# 4.1 VCN Manager Administrator Role (Crypto Officer)

The VCN Manager Administrator is the only role that has physical access to the VCN Manager Crypto Module. He is the operator for the system, and is the only operator allowed to have root access to the operating system.

## 4.1.1 VCN Manager Administrator Services

VCN Manager Administrator Services are only available locally at the server running the VCN Manager Cryptographic Module. Once authenticated, the VCN Manager Administrator can access the following services offered by the VCN Manager Cryptographic Module:

- Install / Uninstall: The VCN Manager Cryptographic Module.
- Module Initialization: Power up self-tests, firmware integrity test, and initialization of the PRNG.
- Create Domain: Establish the root domain under which virtual communities will reside.
- Edit Domain: Edit properties of a customer domain such as the maximum number of members allowed in the domain.
- Delete Domain: Delete an entire domain, the VCNs in that domain, and the members in those VCNs.
- Create VCN Administrators: Create a database record that contains VCN administrator name and authenticator string.
- Delete VCN Administrators: The keys in the VCN administrator's record are zeroed by writing zeros in the memory and disk location where the record is stored.
- Start High Availability: The VCN Manager Cryptographic Module can be run on a second platform for the purpose of maintaining high availability.
- Stop High Availability: The VCN Manager Administrator can stop the high-availability replication and close the IPsec tunnel between the two platforms.
- Zeroize selected keys and CSPs: Deletion of a VCN causes the module to write zeros in the memory space and disk location where the keys and CSPs for the members of that VCN are stored.
- Zeroize all keys and CSPs: Deletion of all VCNs causes the module to write zeros in the memory space and disk location of all keys and CSPs. To zeroize the CSPs in the database the Manager Administrator must operationally invoke an existing manual command that causes zeros to be written to the whole database.
- Monitor status: monitor the VCN Software Suite by checking system log files that track VCN administrators' activities and VCN members' activities.
- Stop VCN services: stops the VCN manager daemon.

 

### 4.1.2 VCN Manager Administrator Authentication

The VCN Manager Administrator is authenticated to the VCN Manager Cryptographic Module locally through the Operating System, with a username and password. The operating system must be configured to use a minimum 8-character password with all printable and human-readable ASCII characters.

## 4.2 VCN Administrator Role

The VCN Administrator manages the members in one or more Virtual Community Networks or VCNs. The VCN Administrators access the server remotely using secure web access. A username / password (Authenticator string) are used to authenticate the Administrator.

### 4.2.1 VCN Administrator Services

A VCN administrator manages users using the following services:

- Create VCN members: Establish a database record that contains the VCN member name and initialization string. Also, as part of the creation of VCN Members, the VCN Administrator will select a set of IPsec policies for that member.
- Add VCN: Establish a database record that contains VCN management information.
- Edit VCN: Edit VCN management information.
- Delete VCN: Remove the database record that contains the VCN information. All the member records of the VCN are also removed. The relevant keys are zeroized.
- Delete proxied member: Remove the member from our list of proxied members. The deleted members are no longer proxied by the group agent.
- Delete group agent: Remove group agent status from a given member. The group agent's proxy members are no longer proxied members.
- Create Group Agent: A group agent is a member that is able to proxy for other members called the proxied members. The Group Agent behaves identically to a normal member.
- Create Proxied Member: A proxied member is established as a record in the VCN Manager database but is never initialized in its own platform. Instead, it is attached to a Group Agent at creation time and from then on the Group Agent will perform all the functions of the VCN Member Agent for that proxied member.
- Delete VCN member: the keys in the VCN member's record are zeroized by writing zeros to the memory and disk location where the record is stored.
- Load Member VCN Key: During the Registration process, the VCN Member Key is generated on the VCN Manager Cryptographic module loaded into the VCN Member Agent Cryptographic module via an IPsec tunnel between the VCN Manager Cryptographic Module and VCN Member Agent Cryptographic Module.
- Load Pre-shared Key for Member-to-Member IKE Protocol: To facilitate member-to-member connections, the Pre-shared Key for Member-to-Member IKE is generated on the VCN Manager

Cryptographic module and loaded into the source member's VCN Member Agent Cryptographic module via an IPsec tunnel between the VCN Manager Cryptographic Module and the source member's VCN Member Agent Cryptographic Module.

- Load VCN Agent-Manager IPsec Encryption Key: During the Join process, the VCN Agent-Manager IPsec Encryption Key is generated on the VCN Manager Cryptographic Module and loaded into the VCN Member Agent Cryptographic module via an IPsec tunnel between the VCN Manager Cryptographic Module and the VCN Member Agent Cryptographic Module.
- Load VCN Agent-Manager IPsec Authentication Key: During the Join process, the Agent-Manager IPsec Authentication Key is generated on the VCN Manager Cryptographic Module and is loaded into the VCN Member Agent Cryptographic module via an IPsec tunnel between the VCN Manager Cryptographic Module and the VCN Member Agent Cryptographic Module.
- Load IPsec Policy Table: During the Join process, the IPsec Policy Table is generated on the VCN Manager Cryptographic Module and loaded into the VCN Member Agent Cryptographic module via an IPsec tunnel between the VCN Manager Cryptographic Module and the VCN Member Agent Cryptographic Module.
- Complete Registration Handshake: During the registration process the Diffie-Hellman key exchange is used to establish keys for securing the registration process. The complete registration handshake service constitutes the completion of the Diffie-Hellman protocol.

### 4.2.2 VCN Administrator Authentication

The VCN Manager Administrator selects the initial Authenticator String for the VCN Administrator (the password) that is at least 8 characters long.

The user is authenticated to the Crypto module remotely through a browser, using a user name and password.

# 4.3 VCN Member Role (User)

VCN Members are the end users of the system. A VCN Member device is initialized using a Registration process. Once initialized the user can run applications on the VCN Member that utilize the VCN Member Agent to dynamically create secure IPsec connections to other members.

## 4.3.1 VCN Member Services

A VCN Member is able to use the following services offered by the VCN Manager Crypto Module:

- Initialize Member: Initialize a member using the registration process after it is first created by the Administrator.
- Join VCN: Authenticate member and activate VCN Membership in the Virtual Community Network.
- Query VCN: Retrieve a list of active members in the Virtual Community Network.
- Connect to an active member: If the member is joined, he may request to connect-to-a-joined-peer-member in the community using a secure channel.
- Change Member VCN Password: Update member's VCN password (the Authenticator String).
- Leave VCN: Deactivate VCN Membership in the Virtual Community Network.

## 4.3.2 VCN Member Authentication

The VCN Administrator selects an initial Initialization String for the VCN Member that is at least 8-characters long.

During the registration and join protocols, packets sent from the member to the VCN Manager are authenticated using HMAC-SHA-1.

 

# 5

# The Security Rules

The VCN Manager Cryptographic Module enforces the following security rules:

1. Cryptographic services are only available upon successful authentication to one of the following roles:
    - VCN Manager Administrator (Crypto Officer)
    - VCN Member (User)
    - VCN Administrator
2. There shall be no bypass mode.
3. Separation of the following logical interfaces is maintained:
    - Data input
    - Data output
    - Control input
    - Status output
4. Re-authentication is required after power recycling.
5. The module only has a FIPS mode of operation; there is no non-FIPS mode.
6. At power up, the following self-tests are performed:
    - Cryptographic algorithm known-answer test
    - Software integrity check.
7. A continuous random number generator test is performed each time a random number is generated.
8. The random generator uses the FIPS approved PRNG as specified in FIPS publication 186-2 appendix 3, change notice 1.
9. The data output interface is inhibited during all self-tests.
10. If the module fails during self-tests, it immediately halts.

 

11. The module does not support concurrent operators. The operating system prevents more than one user from concurrently logging-in to the module locally. Although there are multiple remote requests to the module, the requests are processed in serial manner based on a processing queue.
12. Initialization of the module is dictated by procedural controls as specified in the VCN Manager Administrator User Manual.
13. When the module is in an error state, the system is halted and the data output interface is inhibited. Only status information may be retrieved from the module. No cryptographic functions are performed.
14. The user of the module has to properly log in to the operating system to access the module prior to initialization.
15. The module does not keep static connections with an authenticated user, thus all connections with previous authenticated users are cleared when system powers down.
16. It shall be an operational requirement that when the VCN Manager Administrator deletes all VCNs, he shall cause the database engine to zeroize the whole database, including all CSP items, using an existing manual command.

# 6

# CSP Management

All keys are stored inside crypto module boundaries and never leave the boundary in unencrypted form. A Diffie-Hellman key exchange is used to establish a secure relationship between the VCN Manager and a number of VCN Members. Human roles are authenticated using authenticator strings (and physical access in the case of the crypto officer).

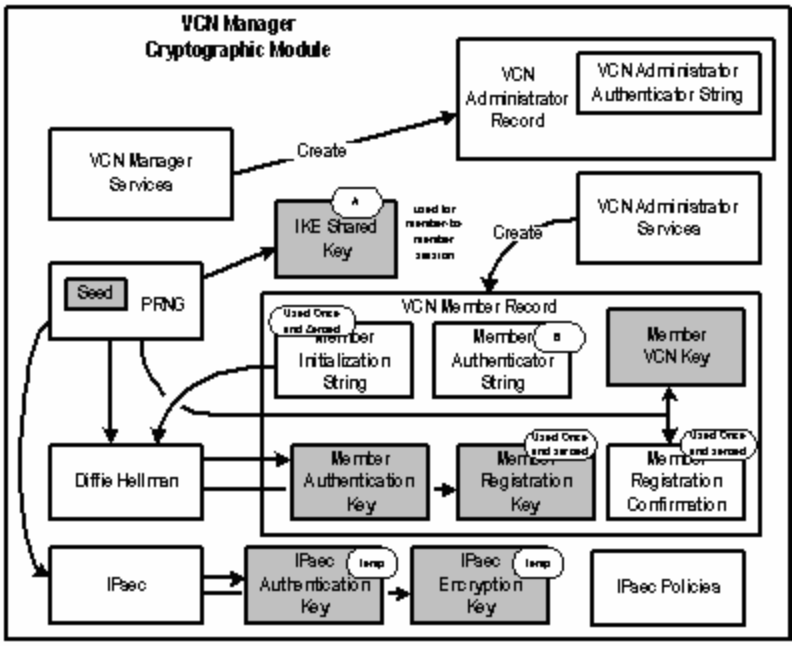


*Figure 6.1 Cryptographic Critical Security Parameters*

## 6.1 Critical Cryptographic Keys

### 6.1.1 PRNG Seed

All cryptographic algorithms involving the use of a key utilize one generated by a FIPS-approved PRNG. The PRNG is the one specified in FIPS 186-2, appendix

3. The underlying one-way function is constructed using SHA-1 as indicated in the standard. The generator is driven by a seed, which is formed by gathering a large amount of unpredictable data that is hashed to form the actual seed for input to the PRNG. The seed is stored in program memory and is zeroized upon termination of the program.

### 6.1.2 Member VCN Key

This key is securely generated by the VCN Manager. It is created when the VCN member is established. The member VCN key is then stored in the cryptographic module on the hard drive. When the member registers with the VCN Manager using a VCN Member Agent, the member VCN key is transmitted to the member in AES encrypted form.

### 6.1.3 VCN Member Registration Encryption Key

This key is generated in the VCN Manager and the VCN Member during the VCN Member Registration protocol using Diffie-Hellman key exchange between the VCN Manager and the VCN Member. This key is stored in program memory until used. It is used once at registration to AES encrypt the Member VCN key for transmittal to the member and is then zeroed out.

### 6.1.4 VCN Member Authentication Key

This key is generated in the VCN Manager and the VCN Member during the VCN Member Registration protocol using Diffie-Hellman key exchange between the VCN Manager and the VCN Member. This key is used to authenticate join packets between VCN Member Agent and VCN Manager when a member joins a VCN. This key is stored on the hard drive and is destroyed and zeroized when the member is deleted.

### 6.1.5 Pre-shared Key for Member-to-Member IKE Protocol

The VCN manager generates a pre-shared key when a member tries to start a communication with another member. The IKE service of the VCN Member Cryptographic Modules uses the pre-shared key to authenticate each other during IKE phase 1.

### 6.1.6 VCN Agent – Manager IPsec Encryption Key

The VCN Agent – Manager Encryption Key is generated in the VCN Manager using a FIPS-approved PRNG. It is zeroized when the member leaves the VCN.

### 6.1.7 VCN Agent – Manager IPsec Authentication Key

The VCN Agent – Manager Authentication Key is generated in the VCN Manager using FIPS approved PRNG. It is zeroized when the member leaves the VCN.

### 6.1.8 HA Service ESP Key

This key is a built in 128-bit AES CBC key that is part of the VCN Manager Cryptographic Module at installation time. It is used as the ESP key for the IPsec tunnel to a second VCN Manager over which the database is replicated for High Availability purposes. It is stored on the hard drive and zeroized when the module is uninstalled.

### 6.1.9 HA Service AH Key

This key is a built in 160-bit HMAC key that is part of the VCN Manager Cryptographic Module at installation time. It is used as the AH key for the IPsec tunnel to a second VCN Manager over which the database is replicated for High Availability purposes. It is stored on the hard drive and zeroized when the module is uninstalled.

### 6.1.10 Server Registration Diffie-Hellman Private Key

This 576-bit secret value is used to derive a shared secret during the Registration protocol. The Diffie-Hellman exponent is generated through the FIPS 186-2 PRNG. It resides in memory during the registration process and is zeroized after registration.

### 6.1.11 Hashed Initialization String

It is used to authenticate packets using HMAC during the initial portion of the registration process. It resides in memory and is zeroized after the session is complete.

## 6.2 Authentication and Initialization Strings

### 6.2.1 VCN Administrator Authenticator String

A VCN Administrator Authenticator String is generated during the creation of a VCN administrator and stored on the hard drive. It is then used to authenticate the user who is assuming the role of VCN Administrator. The user may change the value of this string at any time and it is zeroized when the Administrator is deleted.

### 6.2.2 VCN Member Authenticator String

The user creates a VCN Member Authenticator String during the Initialization of the VCN Member Agent. It is then stored in the module on the hard drive and used to authenticate the user that is assuming the role of VCN Member. The user may change it at any time. The string is zeroized when the member is deleted.

### 6.2.3 VCN Member Initialization String

The VCN Administrator creates a VCN Member Initialization String when a new member is created. It is then stored in the module on the hard drive and used to authenticate the VCN Member Agent at the start of member initialization in the Registration process. The user may keep it as the initial VCN Member Authenticator String or he may select his own Authenticator String in which case the Initialization String is zeroed out after the initial use.

### 6.2.4 VCN Member Registration Confirmation String

This string is generated at random by the system using the PRNG. It is used once and then zeroed out.

## 6.3 The IPsec Policy Table

The IPsec Policies contain no keys or other CSPs, and do not influence cryptographic processes on the VCN Manager. They do, however, indicate whether connections can be established between members, what kind of encryption to use, and whether bypass mode is turned on.

# 6.4 System Services, Roles, and CSPs

| User Services | CSPs | | | | | | | | | | | | Roles | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PRNG Seed | Member VCN Key | DH Private Value | IPsec Policy Table | Hashed Initialization String | VCN Member Reg Enc Key | VCN Member Auth Key | Pre-shared key for Mem-Mem IKE Protocol | VCN Agent-Mgr IPsec Enc Key | VCN Agent-Mgr IPsec Auth Key | HA Service ESP Key | HA Service AH Key | VCN Manager Admin | VCN Admin | VCN Member |
| **Install / Uninstall** | z | z | | | | | z | | | | z | z | x | | |
| **Module initialization** | s | | | | | | | | | | | | x | | |
| **Create VCN Administrators** | | | | | | | | | | | | | x | | |
| **Delete VCN Administrators** | | | | | | | | | | | | | x | | |
| **Start High Availability** | | | | | | | | | | | u | u | x | | |
| **Stop High Availability** | | | | | | | | | | | | | x | | |
| **Zeroize selected keys and CSPs / Delete VCN** | | z | | z | z | z | z | | | | z | z | x | | |
| **Zeroize all keys and CSPs / Delete Domain** | | z | | z | z | z | z | | | | z | z | x | | |
| **Monitor Status** | | | | | | | | | | | | | x | | |
| **Stop VCN Services** | z | | | | | | | | z | z | | | x | | |
| **Create VCN Member** | | g | | u | g | | | | | | | | | x | |
| **Create Group Agent** | | g | | | | | | | | | | | | x | |
| **Create Proxied Member** | | g | | | z | | | | | | | | | x | |
| **Delete VCN Member** | | z | | | | | z | | z | z | | | | x | |
| **Initialize Member** | u | e / t | g/u /z | | u | g / u /z | g | | | | | | | | x |
| **Join VCN** | | u | | e | | | u | | g / e / t | g / e / t | | | | | x |
| **Query VCN** | | | | | | | u | | u | u | | | | | x |
| **Connect to an Active Member** | u | | | u | | | u | g / e / t / z | u | u | | | | | x |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Change Member VCN Password** | | | | | | | u | | u | u | | | | | x |
| **Leave VCN** | | | | | | | u | | u / z | u / z | | | | | x |
| **Add, Edit VCN** | | | | g, c | | | | | | | | | | x | |
| **Create, Edit Domain** | | | | | | | | | | | | | x | | |
| **Load IPsec policy table** | | | | u | | | | | | u | u | | | x | |
| **Load VCN Agent-Mgr IPsec Encryption Key** | | | | | | | | | u | | | | | x | |
| **Load VCN Agent Mgr IPsec Authenticatoin Key** | | | | | | | | | | u | | | | x | |
| **Load Preshared Key for Member to Member IKE** | | | | | | | | u / z | u | u | | | | x | |
| **Load Member VCN Key** | | u | | | | u | u | | | | | | | x | |
| **Delete Proxied Member** | | | | | | | | | | | | | | x | |
| **Delete Group Agent** | | | | | | | | | | | | | | x | |

*z - zeroize; g - generate; e - encrypt; d - decrypt; s - seed PRNG; t – Transmit to Member; u – Use; c - Change*

*Table 6.1 Services and the CSPs / Roles*

# 7

# Physical Security

Because FIPS 140-2 level 1 does not mandate any physical security requirements beyond the use of commercial-grade equipment, additional physical protection is beyond the scope of this document. The VCN Manager software runs exclusively on one of the commercially available hardware platforms listed in Section 3.2 above. Physical access to the workstation is limited to the Crypto Officer.

# 8

# Self-Tests

## 8.1 Power-up Tests

### 8.1.1 Cryptographic Algorithm Known Answer Test

When the VCN Manager Cryptographic Module is invoked for the first time, power-on self-tests are immediately performed. Cryptographic known answer tests are performed for the following algorithms:

- AES
  - This test performs AES crypto algorithm Known Answer Tests for both encryption and decryption
- SHA-1
  - This test performs SHA-1 Known Answer Tests.
- HMAC-SHA-1
  - This test performs HMAC-SHA-1 Known Answer Tests.

If any of these tests fails, the VCN Manager Cryptographic Module is put into an error state (it halts). An error message is logged to the log file and no cryptographic operations are performed. To exit this error state, the module must be restarted.

### 8.1.2 Software Integrity Test

Initial software integrity tests are performed each time the VCN software is powered on. The HMAC-SHA-1 hash of the modules within the cryptographic boundary is compared to known answers. If the values do not match, the VCN software logs an error message and exits.

# 8.2 Conditional Tests

## 8.2.1 Continuous RNG test

The continuous random number generator test is performed every time a random number is generated. The first data block that the PRNG generates is never used for any purpose other than initiating the continuous PRNG test wherein every newly generated block is compared with the block that was generated previously. If the blocks are same, the test fails. In this case, the module logs an error message and enters an error state. To exit this error state, the module must be restarted.

## 8.2.2 Pair-wise consistency test

Every time an asymmetric key pair is generated, a pair-wise consistency test is performed using the newly generated key pair. This test constitutes a Diffie-Hellman pair-wise test for key agreement

# 9

# Mitigation of other attacks

The mitigation of specific attacks outside of the FIPS 140-2 level 1 requirements is beyond the scope of this document.