Security Policy
IP Dynamics, Inc. VCN Software Suite
VCN Member Agent 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 Member Agent Cryptographic Module (SW Version 4.2) for IP DynamicsVCN Software Suite. This security policy describes how the VCN Member Agent 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
- RFC2409 Internet Key Exchange
- FIPS 180-1 (SHA-1)
- FIPS 197 (AES)
- FIPS 46-3 (Triple DES)
- FIPS PUB 198 (HMAC SHA-1)

This document concentrates on the security policy for the VCN Member Agent Cryptographic Module, a software library (combination of dlls, 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 DynamicsVCN Software Suite creates a network services layer above the flat Internet address space allowing 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 policy tables, 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 Member Agent and the Group Agent Software, both of which are client based, use the *VCN Member Agent Cryptographic Module Version #* and the Manager Software, which is server-based, uses the *VCN Manager Cryptographic Module Version #* for cryptographic operations including random key generation, message authentication and verification, hashing, and encryption/decryption. The VCN Member Agent 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	1
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 Table. Management of the membership and the IPsec policy table resides with a VCN Administrator working through the VCN Manager Cryptographic Module. The creation of dynamic IPsec tunnels between members is a function of the VCN Member Agent Cryptographic Module.

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.

Member Authentication

- A member authenticates himself to the server at join time.
- The member's initialization string is provided to him out-of-band via a secure physical channel such as a face-to-face meeting.

2.1 List of Algorithms

The VCN Member Agent 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)
- Encryption/Decryption of data using Triple DES in CBC mode with 168-bit keys (FIPS 46-3)
- Message Authentication using HMAC-SHA-1-128 (FIPS PUB 198)

The VCN Member Agent Cryptographic Module only supports FIPS-approved algorithms.

2.2 The PRNG

The cryptographic module implements the FIPS 140-2 approved FIPS 186-2 Appendix 3 Pseudorandom Number Generator.

2.3 Mode of Operation

The VCN Software Suite has only one mode of operation while running. It is either running in secure mode or, if an error occurs, it is halted.

A Member Agent running in secure mode supports two modes for connections between two members. These connections can be:

- Secured using IPsec
- In bypass mode with no encryption

Bypass mode is governed by a number of internal parameters that must match for continuing operation of bypass mode:

- Source IP
- Destination IP
- Source Port
- Destination Port
- Transport Type

3

The Cryptographic Module

3.1 Physical Module Boundary

The cryptographic module physical boundary lies at the outer case of a general-purpose PC hardware platform with the basic configuration given below. Standard PCs have enclosures that will completely surround the module. The actual hardware platform used may vary.

3.2 Minimum System Requirements

- 233 MHz or higher Pentium-compatible computer
- 64 MB RAM System Memory
- 40 MB Free Hard Disk Space
- CD-ROM Drive
- 10/100 Fast Ethernet NIC – Windows 98/2000/NT-compatible

3.3 Software Module Boundary

The VCN Member Agent Cryptographic Boundary includes:

1. The VCN Member Agent Cryptographic Module
2. One of the following operating systems:
    - A commercially available Intel 32-bit system running Windows 2000, Windows XP, Windows NT4.0.1 with service pack 6a, Windows 98 SE, or Windows 98 (Note that while Windows 2000 was used during FIPS 140-2 operational testing, all of the operating systems listed may be used with this cryptographic module).

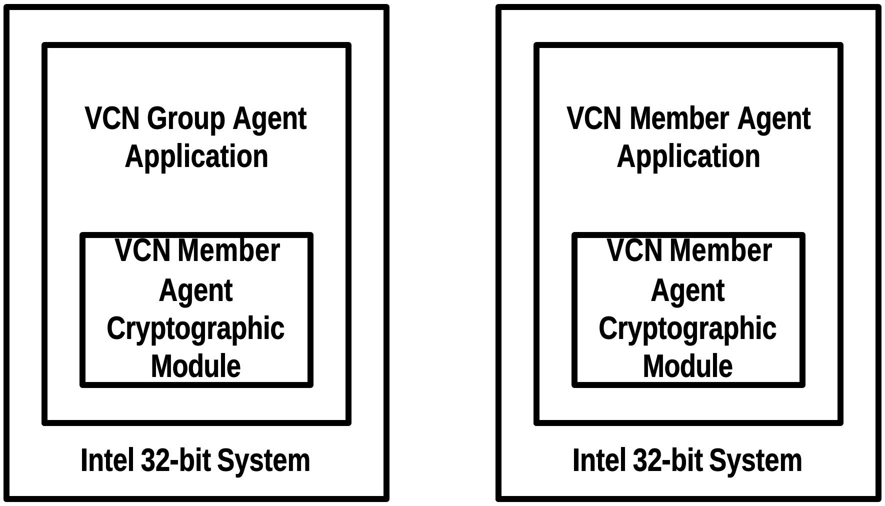
VCN Group Agent Application
VCN Member Agent Cryptographic Module
Intel 32-bit System
VCN Member Agent Application
VCN Member Agent Cryptographic Module
Intel 32-bit System

Figure 3.2 VCN Member Agent Cryptographic Module Software Boundary

3.4 Module Interfaces

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

4

Roles, Services, and Authentication

There are two roles in the VCN Member Agent: the VCN Member role and the VCN Administrator role. There is no Maintenance role.

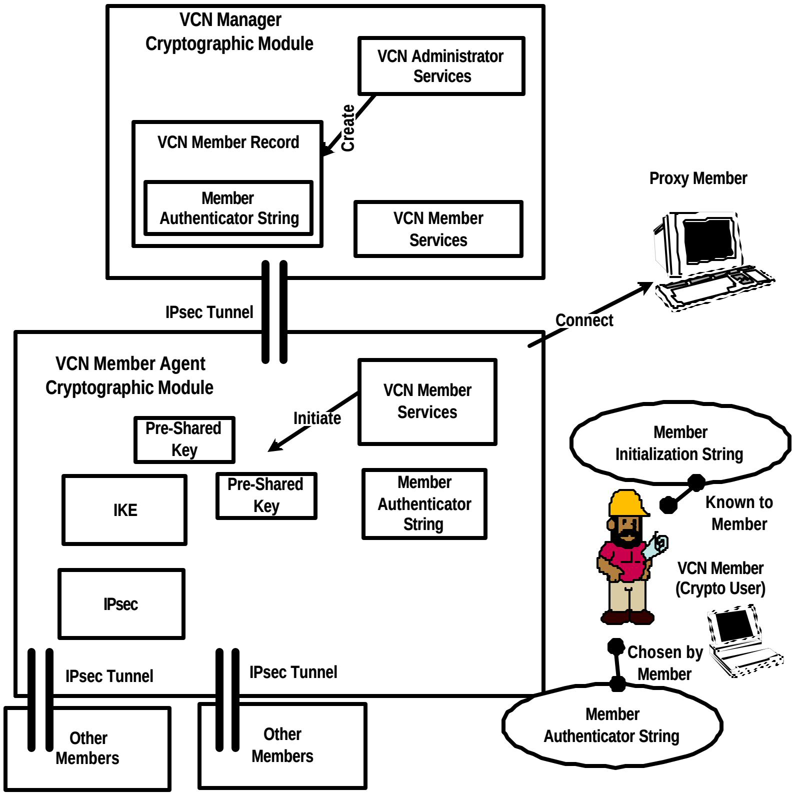

Figure 4.1 VCN Software Suite Member Agent Crypto Roles and Authentication

4.1 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.

4.1.1 VCN Member Services

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

- Register: Initialize a member using the registration process after it is first created by the Administrator.
- Perform self-tests: Perform self-tests on power recycle. This service is not initiated by the member but is automatically performed on power up.
- 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 via IKE: If the member is joined, he may request to connect-to-a-joined-peer-member in the community using a secure channel.
- Connect to active member in bypass: If the IPsec policy table for connecting two members is a bypass rule, then IKE is not invoked and no encryption occurs during the connection among members.
- Change Member VCN Password: Update member's VCN password (the Authenticator String).
- Leave VCN: Deactivate VCN Membership in the Virtual Community Network.
- Remove Membership in one VCN: Choose to remove identity by selecting a name from the GUI, click a delete button, and cause the VCN Member Agent Module to write zeros in the memory space where the keys and CSPs of the selected VCN are stored.
- Remove Member Agent software: Removal of the VCN Member Agent from a machine results in deletion of VCN Membership information for all locally registered VCN Memberships and causes the module to write zeros in the memory space of all keys and CSPs.
- Stop VCN services: Stops the VCN Member Agent software, which shuts down the crypto module.
- Monitor status: Monitor the VCN Member Agent Software by viewing the GUI and event log files.

- Export VCN Membership: This includes the member name, VCN Member key, and the VCN authentication key. These keys are encrypted using the group key before being exported to a file on the hard disk.
- Import VCN Membership: Import VCN Membership information into a new VCN Member Agent. This includes the member name, VCN Member key, and the VCN authentication key. These keys are decrypted using the group key from a file on the hard disk.

4.1.2 VCN Member Authentication

The user is also selects an authenticator string (a password) during initialization. This string is later checked during joining to further authenticate the user.

4.1.3 VCN Member Re-Authentication with User Obfuscator and Export Obfuscator

These obfuscator values are used to decrypt a configuration file (for the purposes of additional user authentication only).

4.2 VCN Administrator Role (Crypto Officer)

The VCN Administrator manages the members in one or more Virtual Community Networks or VCNs through the use of the VCN Manager Cryptographic Module.

4.2.1 VCN Administrator Services

A VCN Administrator has access to the following services offered by the VCN Member Agent Crypto Module:

- Load Member VCN Key: During the Registration process, the VCN Member 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 VCN Member Agent Cryptographic Module.

- Load Pre-shared Key for Member-to-Member IKE Protocol: 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 loads it 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. The integrity of the IPsec Policy is verified during each load via HMAC SHA-1.

4.2.2 VCN Administrator Authentication

All of the packets sent to the VCN Member Agent Cryptographic Module from the VCN Manager on behalf of the VCN Administrator are authenticated using HMAC SHA-1.

5

The Security Rules

The VCN Member Agent Cryptographic Module enforces the following security rules:

1. The module supports two roles:
    - VCN Member (User)
    - VCN Administrator (Crypto Officer)
2. Separation is maintained among the following logical interfaces: data input, data output, control input, and status output.
3. Re-authentication is required after power recycling.
4. The module only has a FIPS mode of operation; there is no non-FIPS mode.
5. At power up, the following self-tests are performed: cryptographic algorithm known answer test and software integrity check.
6. A continuous random number generator test is performed each time a random number is generated.
7. The random number generator uses the FIPS approved PRNG as specified in FIPS 186-2.
8. All HMAC-SHA-1 hashes shall be keyed using a minimum of 128-bit keys.
9. The data output interface is inhibited during all self-tests.
10. If the module fails during self-tests, it immediately halts the Member Agent and displays an error message.
11. The module does not support concurrent operators. The Operating system prevents more than one user from concurrently logging in to the module locally.

12. The initialization of the module is dictated by procedural controls as specified in the User Manual.
13. When the module is in an error state, the data output interface is inhibited. Only status information may be output from the system using the operating system services. No cryptographic functions are performed.
14. The user of the module has to properly login to the operating system to access the module prior to initialization.
15. The module does not keep static connections with other authenticated members, thus all connections with previous members are cleared when system powers down.
16. The module does not allow unencrypted connections with other members unless it has received, from the VCN Manager module, an authenticated IPsec policy table, allowing bypass mode with that member, which contains more than two independent parameters that are checked. The integrity of the IPsec Policy is verified during each load via HMAC SHA-1.
17. The module checks a number of logically independent parameters for every packet over a connection to another member and drops packets that do not match those parameters. Specifically, a connection in bypass mode (no encryption) has these parameters specified in the IPsec policy table and they are checked on an ongoing basis. The integrity of the IPsec Policy is verified during each load via HMAC SHA-1.

6

CSP Management

All keys are stored inside crypto module boundaries and never leave the boundary in unencrypted form. A Diffie-Hellman key agreement is used to establish a secure relationship between the VCN Member and the VCN Manager. IKE is used for key establishment between VCN Members.

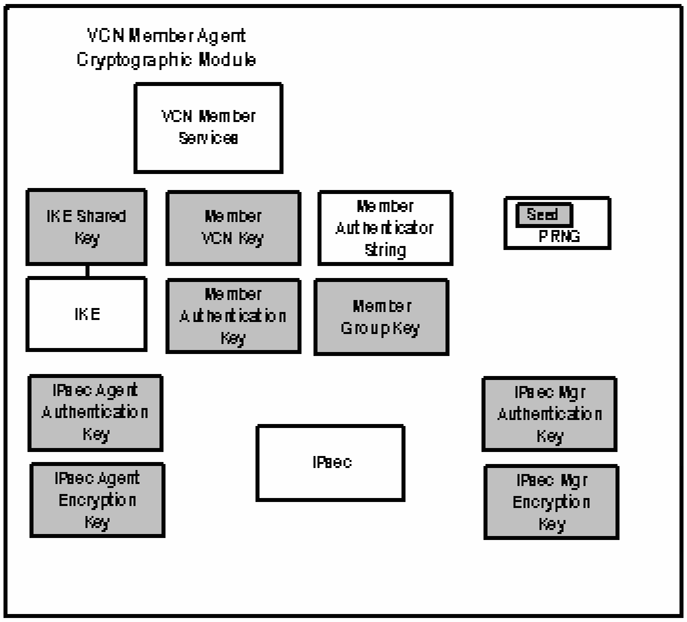

Figure 6.1 Cryptographic Critical Security Parameters

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 takes as input a seed, which is formed by computing a SHA-1 hash of a large amount of unpredictable system data.

6.1.2 Member VCN Key

This key is securely generated by the VCN Manager using the manager's seed and PRNG. It is created when the VCN member is established. 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. The member VCN key is then stored in the VCN Member Agent Cryptographic module on the hard drive. This key is zeroized when the membership is deleted.

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 the Diffie-Hellman key exchange protocol between the VCN Manager and the VCN Member. This key 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 the Diffie-Hellman key exchange protocol between the VCN Manager and the VCN Member. This key is saved on the hard drive and is zeroized when the membership 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. This key is used once and then zeroized.

6.1.6 VCN Agent – Agent IPsec Encryption Key

The VCN Agent – Agent Encryption Key is generated in the VCN Member using the Diffie-Hellman key-agreement protocol in IKE between the two VCN Members. This key is saved in memory and is zeroized when the Agent is stopped.

6.1.7 VCN Agent – Agent IPsec Authentication Key

The VCN Agent – Agent Authentication Key is generated in the VCN Member using the Diffie-Hellman key-agreement protocol in IKE between the two VCN Members. This key is saved in memory and is zeroized when the Agent is stopped.

6.1.8 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 sent to the VCN Member Agent AES encrypted using the Member VCN Key. This key is used in the IPsec module to encrypt IP packets between the VCN Member Agent Software and the VCN Manager Software. This key is saved in memory and is zeroized when the VCN Member leaves the VCN.

6.1.9 VCN Agent – Manager IPsec Authentication Key

The VCN Agent – Manager Authentication Key is generated in the VCN Manager using a FIPS-approved PRNG. It is sent to the VCN Member Agent AES encrypted using the Member VCN Key. This key is used in the IPsec module to authenticate IP packets between the VCN Member Agent Software and the VCN Manager Software. This key is saved in memory and is zeroized when the VCN Member leaves the VCN.

6.1.10 Group Member Key

The Group Member Key is used to AES encrypt the VCN Member Key and the VCN Authentication Key when they are exported from one Member Agent for import into another Member Agent. This key is saved on the hard disk and is zeroized when the VCN Member Agent software is removed.

6.1.11 User Obfuscator

The User Obfuscator is a 128-bit value derived through the SHA-1 hash of the VCN Member Authenticator string. *The module verifies the correctness of this value for VCN Member authentication only.* The configuration file is already stored on the hard drive cryptographically protected via AES by Group Member key. The User Obfuscator resides in memory and is zeroized when the VCN Member Agent is shut down.

6.1.12 VCN Export Obfuscator

The VCN Export Obfuscator is a 128-bit value derived through the SHA-1 hash of the VCN Export String. *The module verified the correctness of this value for VCN Member authentication only.* The configuration file is already cryptographically protected via AES with Group Member key before export. It resides in memory and is zeroized when the VCN Member Agent is shut down.

6.1.13 Member Registration Diffie-Hellman Private Key

The Member Registration Diffie-Hellman Private Key is a 576-bit key that is used to derive a shared secret during the Registration protocol. It resides in memory during the registration process and is zeroized after registration.

6.1.14 IKE Diffie-Hellman Private Key

The IKE Diffie-Hellman Private Key is a 576-bit key that is used to derive a shared secret during the IKE protocol between two members. It resides in memory during the IKE process and is zeroized after the member-to-member session is complete.

6.1.15 IKE SKEYID

The IKE SKEYID is 160-bit key used to establish the SKEYID_d, SKEYID_a, SKEYID_e key material for IKE via HMAC as per page 9 of RFC 2409. It is generated by applying HMAC keyed with the IKE Pre-shared key to a payload consisting of two nonces. It resides in memory and is zeroized after the member-to-member session is complete.

6.1.16 IKE SKEYID_d

The IKE SKEYID_d is a 160-bit HMAC key used to establish the IPsec ESP and AH keys. It resides in memory and is zeroized after the member-to-member session is complete.

6.1.17 IKE SKEYID_a

The IKE SKEYID_a is a 160-bit key used for liveliness and authentication of packets sent during the second phase of IKE. It resides in memory and is zeroized after the member-to-member session is complete.

6.1.18 IKE SKEYID_e

The IKE SKEYID_e is used to encrypt all packet data (except for the headers) during the second phase of IKE. It resides in memory and is zeroized after the member-to-member session is complete.

6.1.19 Hashed Initialization String

The Hashed Initialization String 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 Member Authenticator String

The user creates a VCN Member Authenticator String during the Registration of the VCN Member Agent. It is requested from the user to authenticate the user that is assuming the role of VCN Member at join time and is then zeroed out. The user may change it at any time.

6.2.2 VCN Member Initialization String

The VCN Administrator creates a VCN Member Initialization String when a new member is created. It is then securely sent to the VCN Member User through a separate channel.

6.2.3 VCN Export String

The user creates the VCN Export String during the Export VCN Membership service. This 8-character password is used as input to SHA-1 for the creation of the VCN Export Obfuscator.

6.3 The Configuration File

The VCN Member is able to export VCN Membership information. This includes the member name, VCN Member key, and the VCN authentication key. These keys are AES encrypted using the Member Group key before being exported to a file on the hard disk.

6.4 The IPsec Policy Table

When a VCN Member joins a VCN it receives the full list of IPsec Policy Tables for connecting to peer members in the VCN. This list is received from the VCN Manager AES encrypted with the Member VCN key and authenticated with VCN Member Authentication key. It resides in memory for use when peer connections are established and is zeroed out when the member leaves the VCN.

6.5 System Services, Roles, and CSPs

VCN Administrator / Crypto Officer Services	Critical Security Parameters									
	PRNG seed	Member VCN Key	VCN Member Reg. Enc. Key	VCN Member Auth Key	IKE Pre-shared key	VCN Agent-Agent ESP Key	VCN Agent-Agent AH Key	VCN Agent-MGR ESP Key	VCN Agent-MGR AH Key	IPsec Policy Table
Load Member VCN Key		r	u	u						
Load Pre-shared key for Member to Member IKE					R			u	u	
Load VCN Agent-Manager IPsec Encryption Key		u		u				r		
Load VCN Agent-Manager IPsec Authentication Key				u				u	r	
Load IPsec policy table.								u	u	R

z - zeroize; g – generate; e - encrypt; d - decrypt; s - seed PRNG; r – Receive from VCN Manager; u - Uses

Table 6.1 Services and the CSPs / Roles

VCN Member User Services	**Critical Security Parameters**									
	IPsec Policy Table	**Hashed Init. String**	**User Obfuscaotor**	**IKE SKEYID**	**IKE SKEYID_d**	**IKE SKEYID_a**	**IKE SKEYID_e**	**Export Obfuscator**	**DH Private Key IKE**	**DH Private Key Registration**
Register		u								g / u/ z
Perform Self-tests										
Join VCN	r		u							
Query VCN										
Connect to Active Member via IKE	u			u / z	u / z	u / z	u /z		u	
Change Member Password			u							
Leave VCN										
Remove Membership in one VCN	z	z	z							
Remove Member Agent Software	z	z	z	z	z	z	z	z	z	Z
Stop VCN Services									z	
Monitor Status										
Export VCN Membership								u		
Import VCN Membership								u		
Connect to Active Member via bypass	u									

z - zeroize; g – generate; e - encrypt; d - decrypt; s - seed PRNG; r – Receive from VCN Manager; u - Uses

Table 6.2 Services and the CSPs / Roles

VCN Member User Services	Critical Security Parameters									
	PRNG seed	Member VCN Key	VCN Member Reg. Enc. Key	VCN Member Auth Key	IKE Pre-shared key	VCN Agent-Agent ESP Key	VCN Agent-Agent AH Key	VCN Agent-MGR ESP Key	VCN Agent-MGR AH Key	Group Member Key (Built into Software)
Register	u	r / d	g / z	g						
Perform Self-tests	s									
Join VCN		u		u				r / d	r / d	
Query VCN				u				u	u	
Connect to Active Member via IKE	u			u	r / d / u / z	g	g	u	u	
Change Member Password				u				u	u	
Leave VCN				u				u /z	U /z	
Remove Membership in one VCN		z		z						
Remove Member Agent Software		z		z						z
Stop VCN Services	z					z	z	z	z	
Monitor Status										
Export VCN Membership		e		e						u
Import VCN Membership		d		d						u
Connect to Active Member via bypass										

z - zeroize; g – generate; e - encrypt; d - decrypt; s - seed PRNG; r – Receive from VCN Manager; u - Uses

Table 6.3 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. We assume that the VCN Member Agent software runs on a commercially available Intel Platform, and that physical access to the platform is limited to the Crypto User.

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, we perform the power-on self-tests immediately. Cryptographic known answer tests are performed for the following algorithms:

- Triple DES
  - This test performs TDES crypto algorithm Known Answer Tests for both encryption and decryption.
- 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 function is applied to the modules within the cryptographic boundary, and the result 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 pair. This test constitutes a Diffie-Hellman pair-wise test for key agreement.

8.2.3 Bypass Test

The first time the VCN Agent module receives a request for encrypted communication that relies on the IPsec Policy table (such as in a request from another VCN Agent), the VCN Agent performs the bypass test. Before an encrypted packet is sent out, the VCN Agent module compares the first 16 bytes of the outgoing packet before and after cryptographic processing has occurred. With very high probability, the data should not match. If the data does match, the VCN Member Agent Cryptographic Module enters the error state.

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.