CA100 Security Policy

Version 1.5
Revision Date: August 17, 2007

Cryptek Inc.
1501 Moran Road
Sterling, VA. 20166-9309

CRYPTEK

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary cryptographic module security policy for the Cryptek CA100 IPSec software client version 2.4. The security policy describes how CA100 client meets the security requirements of FIPS 140-2 level 1 and how to operate the module securely in FIPS mode. The information contained in this document is provided to fulfill FIPS 140-2 requirements.

1.2 References

The following NIST Federal Information Processing Standards (FIPS) publications are referenced throughout this document:

- FIPS 140-2 Security Requirements for Cryptographic Modules
- FIPS 180-2 Secure Hash Standard
- FIPS 198 The Keyed-Hash Message Authentication Code (HMAC)
- FIPS 46-3 Data Encryption Standard (DES)
- FIPS 186-2 Digital Signature Standard (DSS)

For more information on Cryptek and the Cryptek product line visit the Cryptek website at http://www.cryptek.com. For information on validated Cryptek products visit the Common Criteria Evaluation and Validation Scheme (CCEVS) website at http://niap.nist.gov/cc-scheme/ValidatedProducts.html, and the NIST validated Modules List website at http://csrc.nist.gov/cryptval/140-1/140val-all.htm.

1.3 Product Line Name Change

The Cryptek network security product line has recently undergone a branding change that affects the product names. The new product names are not yet reflected in all documents. Please refer to Table 1-1 below to map the old nomenclature to the new nomenclature. Note: the Cryptek Secure Facsimile product line is not affected by this name change.

Table 1-1. Summary of Product Name Changes

Previous Nomenclature	New Nomenclature	Description
Diamond*Central*™, cCentral	CC200	Security policy manager for all Cryptek network security products.
Diamond*Pak*™, PAK, cPAK	CP102, 104, 106	IPSec security device that protects up to 6 network devices.
Diamond*Link*™, Link, cLink, cPoint	CL100, 150	IPSec security device that protects a single host.
Diamond*UTC*™, UTC, SUTC, cTerm	CT100	An Integrated Sun Ray-based ultra thin client and IPSec security device.
Diamond*VPN*™, cVPN	CV100	IPSec security device that protects a LAN or WAN perimeter.
Diamond*SAT*™, cSAT	CS100, 101, 102	IPSec security device that protects Satellite network connections.
Diamond*Agent*™, cAgent	CA100	IPSec software-based security application.
cVDL	CVDL100	Database firewall network appliance that uses Virtual Data Labeling (VDL) technology.
Diamond*NIC*, NIC, cNIC, NSD-Prime	CN100	IPSec security device that protects a single host. PCI form factor (found only in the CC200).

2 Security Level

The CA100 IPSec software client is classified as a Multiple-chip standalone cryptographic module designed to meet the FIPS 140-2 level 1 security requirements. Table 2 below identifies the security level supported for each security requirement section.

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

Table 2 - Module Security Level Specification

3 CA100 Overview

The Cryptek CA100 IPSec software client represents a new level of security and functionality in the IPSec software client market. As with all of Diamond*TEK* products, the CA100 client is easy to deploy, easy to manage, and easy to control through the CC200 policy manager. The CC200 allows the administrator to configure, manage, view and control all aspects of deployed Cryptek IPSec hardware and software including: user policies, VPN and firewall functionality, and security audits and alarms. The CA100 software client is designed to control the flow of information to and from nodes and access to nodes on a network based on network addresses, and ports. Unlike traditional IPSec software clients that have both the software client and associated policy locally stored on the client's systems, CA100 user policies are centrally stored on the CC200 manager and dynamically downloaded when coming online. The central storage and management of policies through CC200 provides a significant life cycle cost savings to an organization. Now, if you have to modify, change, or add policy rules to your CA100 software client community, you make a single change at the CC200 policy manager and the change is automatically propagated to the appropriate user community.

Diamond*TEK* is the family name of a group of products designed and developed by Cryptek to provide the highest level of protection for information assets inside your enterprise network. Flexible in design, Diamond*TEK*: Will not impact application or user performance; Is complementary to other security components and non-intrusive to your business process; Integrated with other IPSec products and provides a mechanism for including them in a secure managed network; Features an operating system and platform-independent design that is: Unaffected by security leaks or flaws in the operating system or applications; Compatible with your legacy systems and applications; Adaptable to virtually any network configuration; Easily upgradeable and extremely flexible. The diagram below is an example of how the Cryptek family of product might be deployed in a network.

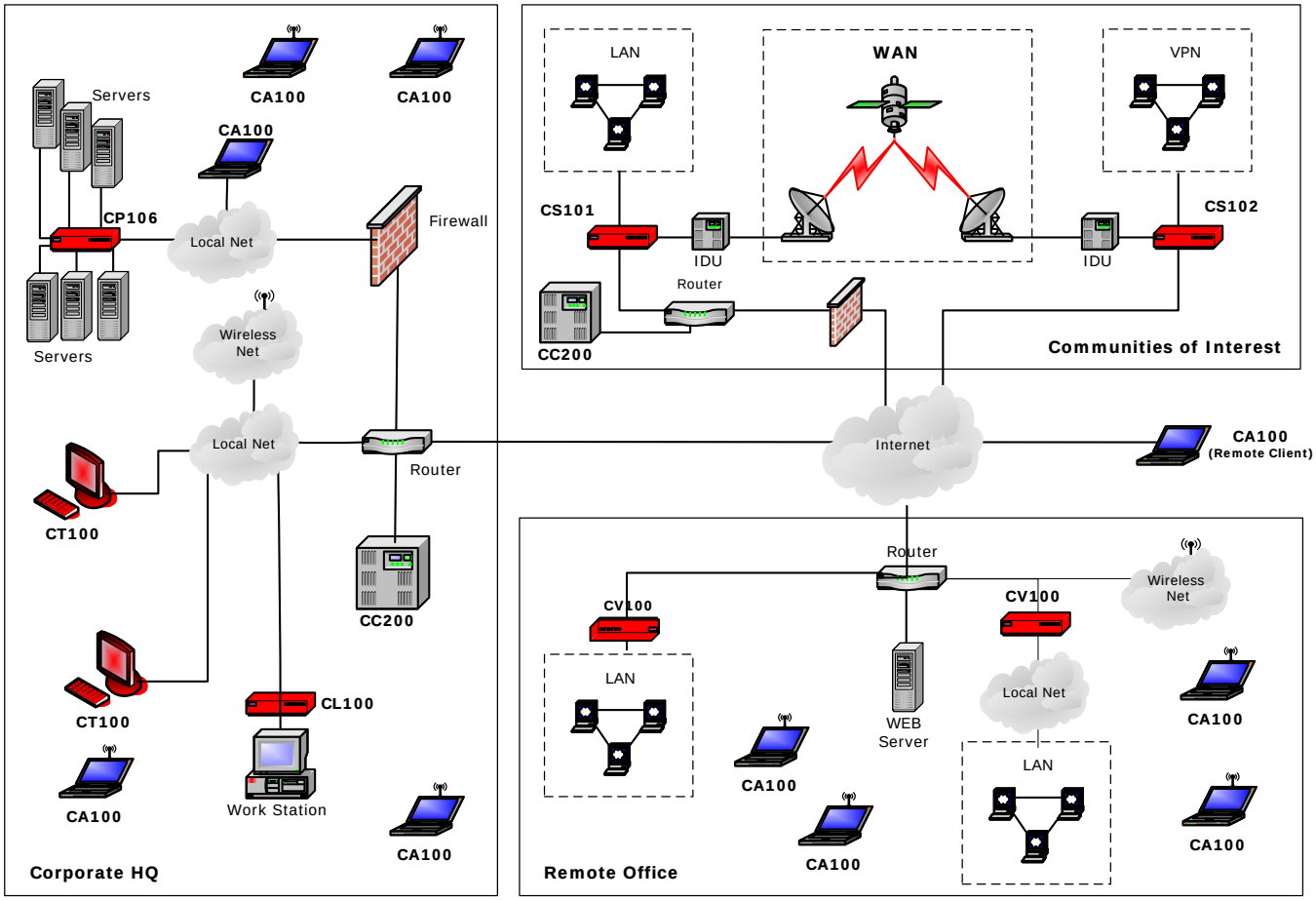

Figure 1 - Cryptek product deployment example

4 Modes of Operation

The CA100 software client supports the three modes of operation, ONLINE, ONLINE-SECURE, and SUSPENDED. The ONLINE mode signifies the CA100 client is configured by the Administrator to communicate to both secure (Cryptek IPSec hardware, Other IPSec (OIPs) nodes, CA100 software clients) and unsecured (Clear Text Nodes (CTNs)) nodes. CA100 software clients will talk encrypted to assigned CA100 clients, Cryptek IPSec hardware, and OIPs nodes and enforce the information flow controls (port filtering) set by the Administrator when in the ONLINE mode. CA100 clients will talk to assigned CTNs in the clear (unencrypted) and enforce the information flow controls set by the Administrator. The ONLINE-SECURE mode signifies the CA100 is configured to only communicate with secure nodes (CA100 clients, Cryptek IPSec hardware, OIPs). All communication between these nodes will employ encryption and enforce the information flow controls set by the Administrator. The SUSPENDED mode is activated by the Administrator and only allows communication with the CC200 policy manager.

4.1 FIPS Approved Operation

In FIPS mode, the CA100 cryptographic module only supports FIPS Approved algorithms as follows:

- Triple-DES – CBC mode for encryption, (Cert. #340)
- SHA-1 – Cert. #334, for hashing and signature generation.
- HMAC-SHA-1 – Cert. #69, for message authentication and software integrity

- ANSI x9.31- 1998 – Cert. #92, Appendix A.2.4 Deterministic Random Number Generator.

The CA100 client cryptographic module also provides the following cryptographic support in all modes of operation;

- Diffie-Hellman (DH) (key agreement provides 80 bits of strength).

4.2 Non-FIPS Approved Algorithms

When not in FIPS mode the CA100 software client supports DES for encryption, DES-MAC for checksums and MD5, HMAC-MD5 algorithms for signature generation and hashing.

4.3 Setting FIPS Mode

The CA100 software client can be configured to operate in FIPS mode during initial setup by the Administrator at the CC200[1]. Setup of the CA100 is accomplished by traversing the various menu screens and entering the appropriate values. Initial setup instructions are provided below;

1. At the **Action Bar** select the "ADD NSD" icon.
2. Enter the ID number and name of the CA100. Click *Next>* to advance to the "Addressing" window.
3. Enter all the appropriate addressing information (e.g. Ethernet address, proxy Ethernet address, IP address, subnet mask, default router, type). Click *Next>* to advance to the "key Type" window.
4. Within the "Key Type" window make the following selections;
    - DES Key Length (Min = 168[2]) (Max = 168)
    - Authentication Type HMAC SHA-1
    - MODP Groups 1024
5. Click *Next>* to advance to the "Audit Threshold" window. Default values will remain unchanged.
6. Click *Next>* to advance to the "Profiles" window. Select the appropriate communication policy for the CA100 by scrolling through the "Security Profiles:" window.
7. Click the *Finish* button and the setting of the FIPS mode is complete for the CA100.

To view the FIPS settings of the CA100 the Administrator must go to the CC200 and select the "View NSD" icon. This will allow the Administrator to confirm the security values set for the CA100 without making any changes to it.

4.4 Cryptographic Boundary

The software boundary for the CA100 for all host platforms consists of the following files:

1. DaAppStarter.exe
2. DaDaemon.exe
3. dac.exe
4. sshipm.exe
5. sshIPSec.sys
6. da_ali.bin

---

[1] Note: The CC200 is also known as the Network Security Center (NSC) and was previously sold under the product name Diamond*Central*.

[2] Note: Setting the minimum and maximum key size to 168 disables single DES use with IPSec.

7. *.dai

5 Ports and Interfaces

The CA100 client supports nine physical interfaces: keyboard, mouse, CD/DVD drive, floppy disk, video, serial, parallel, USB, and network ports. The mapping of the physical ports to the logical interfaces is provided below in table form.

Physical ports	Logical Interface(s)
Keyboard, mouse, network port, USB, floppy drive, CD/DVD drive	Data Input
Network port, Video	Data Output
Keyboard, mouse, network port	Control Input
Video, Network port	Status Output
Power port	Power interface

6 Roles, Services, and Authentication

6.1 Assumption of Roles

The CA100 software client is designed to support Role based Authentication and three distinct roles: User Role, Crypto Officer Role and Administrator Role.

Authentication Type	Authentication Strength of Mechanism
Shared Secret	The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{112}$ which is less than 1/1,000,000
Password	The probability that a random attempt will succeed or a false acceptance will occur is between $1/10^{6}$ and $1/10^{17}$ which is less than 1/1,000,000. Note to meet the FIPS requirements the password must be at least 6 digits. Note: the password only supports the use of numeric characters.

6.2 User Role

The possession of the authentication credential provided by the Administrator provides accesses to the CA100 client. The authentication credentials are comprised of a unique user/ID password combination and a shared secret. The User uses the user/ID and password to logon to the CA100 client application and the shared secret to communicate with the CC200 policy manager (Administrator Role). Once the CA100 client has validated the authentication credentials they are sent to the CC200 using a trusted channel for policy download. If the validation fails or the policy request is denied an error message will be displayed by the status output (monitor). A successful validation and policy request will result in authorized services being provided to the User in accordance with the security policy download. Three consecutive failed authentication attempts will disable the CA100 client, and require Administrator action.

6.3 Crypto Officer Role

The Crypto Officer Role is responsible for installation and initialization of the CA100 client. The possession of the authentication credentials provided by the Administrator provides accesses to the CA100 client. The authentication credentials consist of all the configuration settings for the CA100 client and a shared secret (14 bytes) to communicate with the CC200 policy manager (Administrator Role). The Crypto Officer presents the credential to the CA100 client for validation. A failed validation results in a failed installation and an error message being displayed by the status output (monitor). A successful validation results in authorized services being provided to the Crypto officer.

6.4 Administrator Role

The possession of the shared secret (14 bytes) provides authentication for the CC200 policy manager (Administrator role) to the CA100. The Administrator presents the authentication credentials to the CA100 client using a trusted channel. A failed validation by the CA100 client will require the CA100 client be re-installed by the Crypto officer. A successful validation will allow the Administrator access to the CA100 client to provide authorized services.

6.5 Services

The following table provides information about the Services to Security functions and Roles availability to services within the CA100.

Services	Security Functions	User Role	Crypto Officer Role	Administrator Role
Show Status	None	X	X	X
Transmit Packets Process	3DES, SHA-1, HMAC-SHA-1	X		
Receive Packets Process	3DES, SHA-1, HMAC-SHA-1	X		
Initiate State change of CA100	3DES, SHA-1, HMAC-SHA-1	X		X
Initiate Self-test of CA100[3]	3DES, HMAC-SHA-1, SHA-1	X		
Install CC200 shared secret	HMAC-SHA-1		X	
Configure the CA100 per predefined policy	3DES, SHA-1 HMAC-SHA-1			X
Zeroize CA100[4]	3DES, SHA-1, HMAC-SHA-1			X

[3] A complete list of power-up and conditional self-test can be found in section 10.

[4] Sections 7.1 and 8 contain additional information on zeroized CSPs and SRDIs.

7 Definition of Critical Security Parameters (CSPs)

The following table contains the description of the Critical Security Parameters (CSP) in the CA100 client.

CSP	Description
CC200 shared secret (**CCSS**)	Used to provide encrypted communication between the CA100 software client and the CC200 policy manager for the Administrator (used as an IKE pre-shared secret). [112 bits]
Traffic encryption keys (**TEK**s)	Used to encrypt the traffic between the CA100 client and other CA100 clients, Cryptek IPSec hardware, or other IPSec device. These are generated as part of the IKE key generation process. [168 bits for 3DES]
Traffic authentication keys (**TAK**s)	Used to authenticate the traffic between the CA100 client and other CA100 clients, Cryptek IPSec hardware, or other IPSec device. These are generated as part of the IKE key generation process. [160 bits]
Diffie-Hellman private keys (**DHPK**)	Generated by the CA100 client for each used level of classification and used as part of the IKE key generation process. [1024 bits]
Node authentication values (**NAV)**	A shared secret is used as the authentication mechanism for the IKE key generation process. [112 bits]
Password **(PSW)**	A numeric value 6 – 17 bytes long used to authenticate the user to the CA100 client.
Deterministic Random Number Generator (RNG)	A RNG is used to generate random numbers. The CA100 client supports a deterministic random number generator (DRNG), in accordance with ANSI X9.31.
Hardware Random Identifier **(HRI)**	Random data used as part of the authentication mechanism for the IKE key generation process

The following table contains a description of a Security Relevant Data Items (SRDIs) not considered CSPs. The SRDIs are protected within the cryptographic boundary against unauthorized modification and substitution.

SRDI	Description
Discretionary Access Control List (**DAT**)	The list of approved source and destination addresses (IP address, TCP/UDP port numbers).
DH Public Key (**DHLK**)	Generated by the CA100 for each used level of classification and used as part of the IKE key generation process.

7.1 CSP/SRDI to Services Relationship

Transmit Packet Processing: The operation to transmit a packet shall first access the current state of the CA100 client. If the CA100 client application is off-line then the packet will not be processed by the CA100 client. If the CA100 client is online, then the discretionary access control list (**DAT**) is checked to determine if communication is allowable based on the destination IP address and TCP/UDP port number.

- If the destination is not allowable (because of IP address or TCP/UDP port number) then the packet is destroyed and an audit event is generated.

- If the **DAT** signifies that the communication is allowable (based on IP address and TCP/UDP port number) and the destination is a clear text (CTN), then the CA100 client transmits the packet.

- If the **DAT** signifies that the destination (CA100 client, Cryptek IPSec hardware, or OIPs) is allowable and communication is to be encrypted, then the keys associated with the destination (**TEK** and **TAK**) are accessed.

    - If a key exists, then it is used to encrypt the packet and the key associated with the authentication mechanism (**TAK**) is used to perform the authentication of the packet. If the lifetime of the key has expired, then the keys (**TEK** and **TAK**) associated with the destination address are destroyed.

    - If no key exists for the destination IP address, then the packet is destroyed and an IKE process is instigated. The IKE process will utilize the list of approved encryption algorithms (**ACAL**) and the list of approved authentication algorithms (**AAAL**) to negotiate an acceptable combination to secure the information between the new nodes.

    - If the CA100 client does not have a Diffie-Hellman private value, then a Diffie-Hellman public (**DHLK**) and private (**DHPK**) keys are generated. The Diffie-Hellman data, the shared secret (**NAV**) associated with the destination IP address and random data (**HRI**) generated as part of the IKE protocol are used to generate the keying material (**TEK** and **TAK**) to secure the communications between the CA100 client and the destination IP address. After the encryption and authentication are complete, the packet is transmitted to the network. If the destination is not allowable (because of IP address or TCP/UDP port number) then the packet is destroyed and an audit event is generated.

Receive Packet Processing: The operation to receive a packet shall first access the current state of the CA100 client. If the CA100 client application is off-line then no packets will be processed by the CA100 client. If the CA100 client is online, then the discretionary access control list (**DAT**) is checked to determine if communication is allowable based on source IP address and TCP/UPD port number.

- If communication with the source is not allowable (because of IP address and SPI number) then the packet is destroyed and an audit is generated.

- If the **DAT** signifies that communication with the source is allowable and is clear text (CTN), CA100 client checks the port number. If the port number is acceptable then the packet is given to the host. If the port number is not allowed then the packet is destroyed and an audit event is generated.

- If the **DAT** signifies that the source (CA100 client, Cryptek IPSec hardware, or OIPs) is allowable and communication is supposed to be encrypted, then the keys associated with the destination (**TEK** and **TAK**) are accessed.

    - If a key exists, then it is used to decrypt the packet and the key associated with the authentication mechanism (**TAK**) is used to perform the authentication of the packet. After the decryption and the authentication are complete, the packet is checked for allowable TCP/UDP port numbers. If the **DAT** signifies that the TCP/UDP port number is acceptable, then the packet is given to the host system. If the port number is not acceptable then the packet is destroyed and an audit is generated. If the lifetime of the key has expired, then the keys (**TEK** and **TAK**) associated with the destination address are destroyed.

    - If no key exists for the source then the packet is destroyed and an IKE process is instigated. The IKE process will utilize the list of approved encryption algorithms (**ACAL**) and the list of approved authentication algorithms (**AAAL**) to negotiate an acceptable combination to secure the information between the new nodes.

    - If the CA100 client does not have a Diffie-Hellman private value generated for the classification level, then a Diffie-Hellman public (**DHLK**) and private (**DHPK**) key is generated. The Diffie-Hellman data, the shared

secret (**NAV**) associated with the source address and random data (**HRI**) generated as part of the IKE protocol are used to generate the keying material (**TEK** and **TAK**) to secure the communications between the CA100 client and the source address. If key material exists for the communications channel, then the old keying material (**TEK** and **TAK**) are destroyed and replaced with the new values.

Install CC200 shared secret: The install CC200 shared secret function is accomplished during the initialization of the CA100 by the Crypto officer. The Crypto officer presents his authentication credentials containing the shared secret and configuration data used by the CA100 client for communication with the CC200. The CA100 client will copy the encrypted information from the credentials and store it in non-volatile memory.

Configure the CA100 client per a predefined policy: The Administrator (via the CC200) shall download (under protection of the encrypted communication between the CA100 and the CC200 using the **CCSS**) the defined discretionary access control list (**DAT**) and node authentication values (**NAV**) each time a user successfully logs into the CA100. Configuration changes could be an addition or a removal of the ability to send/receive packets to other host systems. In the case of a removal, any traffic encryption keys (**TEK**) or traffic authentication keys (**TAK**) used for communication between the node and the removed destination node are zeroized.

Zeroize CA100 client: The Administrator can zeroize all the CSPs and SRDIs stored and in use by the CA100 client using the encrypted communication channel setup by the **CCSS**. Note: The User can zeroize most CSPs and SRDIs (TEKs, TAKs, DHPK, NAV, RNG, DAT, DHLK) by cycling the power, logging off, or by exiting the application.

Initiate State change of CA100: The Administrator can initiate a state change (e.g. suspend, shutdown, and online) using the encrypted channel setup by the **CCSS**. The User can initiate a state change by cycling the power of the CA100 client or logon/logoff.

Initiate Self-test of CA100: The User can initiate the CA100 client to perform self-tests by logon/logoff.

Show Status: The User, Administrator, and Crypto Officer are able to read the module status at all times.

8 Service to CSPs/SRDI Access Operation Relationship

The table on this page has been devised to show the Services vs. CSPs/SRDI and Role access.

Services vs. CSPs Access/SRDI	**CCSS**	**TEK**	**TAK**	**DHPK**	**DAT**	**NAV**	**PSW**	**RNG**	**HRI**	**U**	**C**	**A**
Show Status										X	X	X
Transmit Packet Processing		WAZ	WAZ	WA	AZ	AZ		AZ	WAZ	X		
Receive Packet Processing		WAZ	WAZ	WA	AZ	AZ		AZ	WAZ	X		
Initiate Self-test of CA100	A						W			X		
Initiate State change of CA100	A	WAZ	WAZ	WA		AZ	WAZ	AZ	WAZ	X		X
Install CC200 shared secret	W										X	
Configure the CA100 per a predefined policy	A	Z	Z		W	W						X
Zeroize CA100	Z	Z	Z	Z	Z	Z	Z	Z	Z			X

In the above table, access to the CSPs/SRDI via the service utilizes the following abbreviations:

A = Access (note that the actual value is never seen outside the security perimeter so it is not technically a read)
W = Write
Z = Zeroize

In the table above, access to services by individuals is shown by placing an X in the appropriate column at the right of the table. The following abbreviations apply:

U = User
C = Crypto Officer
A = Administrator

9 Operational Environment

The CA100 client was tested using two general purpose operating systems Microsoft Windows 2000 and Microsoft XP. To comply with FIPS 140-2 requirements the operating systems must be configured for single user mode. Instructions for configuring the operating systems for single user mode can be found in section 13.

10 Security Rules

This section documents the security rules enforced by the CA100 client to implement the security requirements of this FIPS 140-2 Level 1 module[5].

1. The CA100 module shall reside on a general purpose computer (GPC) that conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).
2. The CA100 shall support three distinct roles: User, Crypto officer, and Administrator.
3. The CA100 shall provide Role-Based authentication.
    a. Possession of the User authentication credentials provides access to the CA100. Possession of the Crypto officer authentication credentials provides authentication for the Crypto officer. Possession of the shared secret provides authentication for the Administrator role.
4. The cryptographic module shall encrypt message traffic using the TDES algorithm.
5. The cryptographic module shall perform the following tests:
   A. Power up Self-Tests:
        1. Cryptographic algorithm tests:
            a. TDES Known Answer Test
            b. DES Known Answer Test
            c. DES_MAC Known Answer Test
            d. SHA-1 Known Answer Test
            e. HMAC-SHA-1 Known Answer Test
            f. MD-5 Known Answer Test
            g. HMAC-MD-5 Known Answer Test
            h. DRNG Know Answer Test
        2. Software Integrity Test [HMAC-SHA-1]

   B. Conditional Self-Tests:
        1. Continuous Random Number Generator (RNG) test – performed on DRNG
        2. Policy Integrity Test (Alternating Bypass test)

6. When the CA100 is in the no bypass state the status output will display “ONLINE-SECURE”. When the CA100 is in the alternating bypass state the status output will display “ONLINE”. Prior to each use, the internal DRNG shall be tested. Testing is accomplished using the continuous Random number generator test.
7. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data.
9. The CA100 client shall not support concurrent operators.
10. The CA100 client shall generate audits for all attempted Discretionary Access Control (DAC) violations.
11. The User shall not have access to any cryptographic services unless the CA100 client has been commanded to transition to the ONLINE or ONLINE-SECURE state by the CC200 (Administrator role).
12. The CA100 client shall accept state control commands (suspend, online, and shutdown) commands from the CC200 (Administrator role) over the trusted channel.
13. The CC200 (Administrator role) shall be capable of zeroizing CSP and SRDI values stored in the CA100 client.
14. The User shall be capable of commanding the device to perform the power-up self-tests by logon/logoff or cycling the power.

[5] Security rules are contained in the numbered paragraphs. Additional information is provided for background purpose only.

15. The Administrator shall verify at the CC200 the authentication type reads SHA-1, when operating in FIPS mode.
16. The CA100 client shall send all auditable events to the CC200 (Administrator role) for logging.
17. The CC200 (Administrator role) shall download communication rules (DAC policy) to the CA100 client. The policy shall be re-configurable by the CC200 (Administrator role) at any time. These rules define the communication paths as follows:
    - Valid destination addresses for packets sent from the attached host to the network.
    - Valid source addresses for packets being sent to the attached host from the network.
    - Allowable/prohibited TCP and UDP port values for transmission and reception by the host.
    - Allowable/prohibited protocols for transmission and reception by the host.

11 Physical Security

The CA100 client is implemented completely in software such that the physical security is provided by the host platform, and is thus not subject to the physical security requirements of FIPS 140-2. The CA100 client is classified as a Multi-chip standalone module designed to be placed into a general purpose computer (GPC) with a commercial grade enclosure for operations. The GPC platform used for validation conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

12 Mitigation of Other Attacks Policy

The CA100 client cryptographic module makes no additional claims to mitigating other attacks.

13 OS Single User Mode

The Windows operating system on the machine running CA100 client must be configured to prevent remote login and/or access. To do this, the operating system must be configured to run in single-user mode. The following steps must be performed to install and initialize cAgent to operate in a FIPS 140-2 compliant manner:

Disable all additional user accounts (other than the account used by the user of the CA100) found in the **Control Panel | User Accounts**.

Disable the **Server** and **RunAsService** (if present) services using the **Control Panel | Services** program. Note: performing these actions may require Administrator privileges.

Disable the **Run As…** feature of Windows XP:

A) Start the Registry Editor.
To do this, click **Start**, click **Run…**, type **regedit** in the **Open** box, and then click **OK**.

B) Locate, and then click the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer

C) Click the **Edit** menu, point to **New**, click **DWORD Value**, and then type **HideRunAsVerb**.

D) Double-click **HideRunAsVerb**, and then type **1** in the **Value data** area, and then click **OK**.

E) Reboot the PC.

Note: performing these actions may require Administrator privileges.

The **Remote Desktop** feature must be disabled. To do this open
Start | Control Panel | System.
Under the Remote tab, clear the
Allow users to connect remotely to your computer
check box, and then click **OK**. Note: performing these actions may require Administrator privileges.

The Fast User Switching feature of Windows is automatically disabled once cAgent is installed. This occurs because Microsoft's Gina.dll is replaced with a custom version (DaGina.dll) needed for cAgent operation.

The paging file (Virtual memory) must be configured to reside on a local drive on the machine, not a network drive. Note: performing this action may require Administrator privileges.

14 Acronym List

AAAL	Approved Authentication Algorithms
ACAL	Approved Encryption Algorithms
AES	Advanced Encryption Algorithm
CCEVS	Common Criteria Evaluation and Validation Scheme
CSP	Critical Security Parameters
CTN	Clear Text Node
DAC	Discretionary Access Control
DAT	Discretionary Access Control List
CCSS	CC200 Shared Secret
DES	Data Encryption Standard
DES-MAC	Date Encryption Standard – Message Authentication Code
DHLK	Diffie-Hellman Public Key
DHPK	Diffie-Hellman Private Key
DRNG	Deterministic Random Number Generator
DSS	Digital Signature Standard
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
GPU	General Purpose Computer
HMAC	Hash Message Authentication Code
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAC	Mandatory Access Control
MD5	Message Digest v.5
MODP	Modular Exponential
NAV	Node Authentication Value

NSC	Network Security Center
NSD	Network Security Device
OIPS	Other IPSec
PIN	Personal Identification Number
PKCS#7	Public Key Cryptographic Standard #7 (Cryptographic Message Syntax Standard)
PKI	Public Key Infrastructure
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman
RSW	Receive Security Window
SC	Secure Channel
TAK	Traffic Authentication Key
TCP	Transmission Control Protocol
TEK	Traffic Encryption Key
TSW	Transmit Security Window
UDP	User Datagram Protocol
X.509	Authentication Framework for Directory Services