SmartGate®

(Software Version: 4.5)

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation
Version 0.91

May 2006

Table of Contents

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the SmartGate v4.5 from AEP Networks. This Security Policy describes how the SmartGate meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/cryptval/.

The SmartGate is referred to in this document as the SmartGate, the Module or the Server.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The AEP website (http://www.aepnetworks.com) contains information on the full line of products from AEP. The SmartGate product details can be found at: http://www.aepnetworks.com/products/ssl_vpn/smartgate/overview.htm .
- The CMVP website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to AEP Networks. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to AEP Networks and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact AEP Networks.

2. SmartGate v4.5

2.1 Overview

SmartGate is one of the most comprehensive security products on the market. It is a client/server virtual private network (VPN) software security system that provides secure encrypted channels between users outside your network and the applications and data contained within your network. Fine-grain access control ensures that authorized users are allowed access to specific applications only.

SmartGate enables organizations to provide secure access to organizational networks for remote employees, customers, and business partners. SmartGate is specifically designed to address the challenges of deploying and managing large VPN user populations.

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

Table 1 – Security Level per FIPS 140-2 Section

2.2 Module Interfaces

The SmartGate is classified as a multi-chip standalone module that meets overall level 1 FIPS 140-2 requirements. The module is composed of a set of software binaries and is evaluated for use on a standard PC running RedHat Linux 7.2 or Sun Solaris 8. In addition to the binaries, the module consists of the integrated circuits of the motherboard, the central processing unit (CPU), random access memory (RAM), read only memory (ROM), PC case, keyboard, mouse, video interfaces, expansion cards, and other hardware components included in the PC such as hard disk, floppy disk, CD-ROM drive, power supply, and fans.

Logically, the cryptographic boundary of the SmartGate is composed of the SmartGate software running on the Sun Solaris or RedHat Linux.

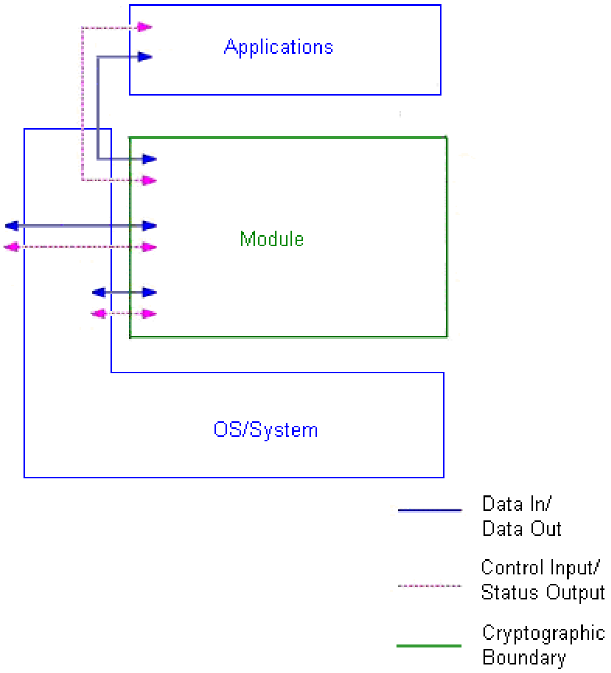

Figure 1 – Logical Block Diagram

Physically, the cryptographic boundary of the module is the PC case, which physically encloses the complete set of hardware and software.

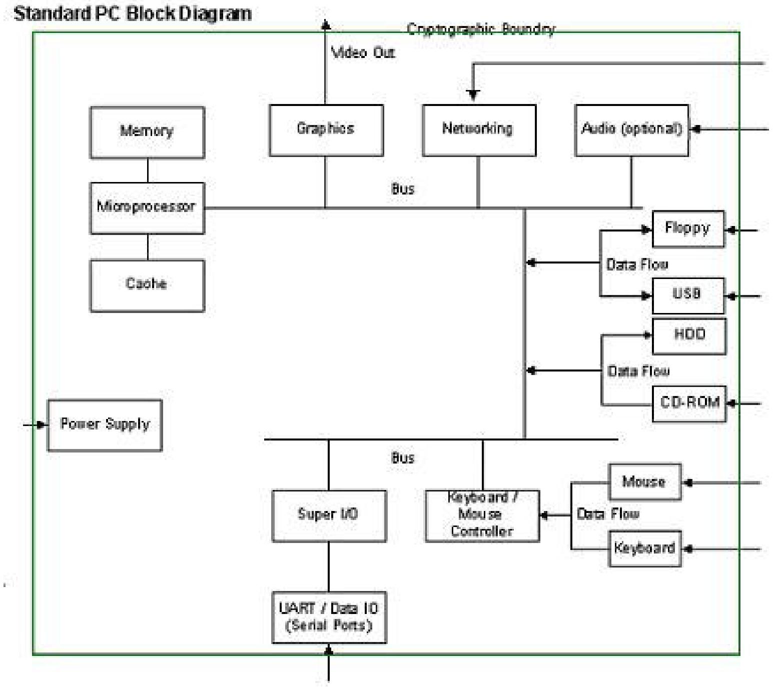

Figure 2 – Physical Block Diagram

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

Module Physical Interface	Logical Interface	FIPS 140-2 Logical Interface
Keyboard, mouse, CD-ROM, floppy disk, and serial/USB/parallel/network ports	Data received via the SmartGate Single Port Proxy (sgproxy) and data received as variables passed to the module's API	Data Input Interface
Floppy disk, monitor, and serial/USB/parallel/network ports	Data output via the SmartGate Single Port Proxy (sgproxy) and data returned from the module's API	Data Output Interface
Keyboard, CD-ROM, floppy disk, mouse, power button, and serial/USB/parallel/network port	Data read from configuration files, data input via the SmartAdmin or command line interface, and data received as variables passed to the module's API	Control Input Interface
Floppy disk, LEDs, monitor, and serial/USB/parallel/network ports	Data output to log files, command line interface, and the SmartAdmin Web Adminstration tool	Status Output Interface
Power Connector	Power Interface	Power Interface

Table 2 –Physical Ports and Logical Interfaces

2.3 Roles and Services

The module supports three roles: Local Crypto Officer, Remote Crypto Officer, and Client User.

The local administrator of the module assumes the Crypto Officer role and can configure the SmartGate via console administration (command line or GUI API calls) and manually editing configuration files. An operator assuming the role of Remote Crypto Officer has some administrative privileges but is limited to accessing SmartGate remotely through the SmartAdmin Web Tool (GUI API calls). Although not required by FIPS 140-2 at level 1, both roles require identity-based authentication; however, these authentication mechanisms are not tested on a Level 1 FIPS 140-2 validation. The Client User accesses the module's VPN services.

2.3.1 Local Crypto Officer Role

The Local Crypto Officer (CO) is expected to install and configure the SmartGate. Once the SmartGate is running, the Local CO can perform all management, configuration and administration of the SmartGate. The Local CO can locally manage the SmartGate through console administration (command line or GUI API calls) and manually editing configuration files.

There is no factory default password that allows access to the Local Crypto Officer role ("root" account for the Operating System). Instead, SmartGate allows a user with administrative privileges on the host Operating System to completely manage the SmartGate and its users.

The following table lists the Local Crypto Officer services. For a complete explanation of the Remote CO services see the SmartGate Administrator's Guide.

Service	Description	Input	Output	CSP	CSP Access
Installation	Installing the SmartGate	Commands	Result of installation	RSA public/private key pair	Write
Login	Authenticate the Crypto Officer	Login information	Result of login attempt	Administrative Crypto Officer password	Read
Public/Private key configuration	To generate, change the size and test the RSA public/private key pair	Command options	Status of command, response and results	RSA public/private key pair ANSI X9.31 RNG Seed-Key ANSI X9.31 Seed	Read/Write Read Write
License	View license information and features	Command option	License information		
OLR setup configuration	Server On-Line Registration Setup	Command options	Command response		
Access Permissions	Remote administrator and user permissions	Command options	Command response		
View proxy configuration	View Server single port proxy configuration	Command option	View port proxy status		
Extensible components	Start, stop or configure any third-party authentication methods	Command options	Command response		
Client configuration	Client software packages customization	Command options	Command response		
Back up configuration	Back up current configuration or restore files	Command options	Command response		
Uninstall	Uninstall the server software	Command options	Command response		
Start/Restart/Stop	Effects all the Server services except the disabled third party authentication methods. The self tests are performed	Command options	Status of command		

Service	Description	Input	Output	CSP	CSP Access
	during the module start/restart.				
Show status	Status messages for the module written to log file.	Commands	Status info in log file		
Zeroization	Reformatting the hard-drive to zeroize keys	Command options		All	Write

Table 3 – Local Crypto Officer Services, Descriptions, CSPs

2.3.2 Remote Crypto Officer

The Remote Crypto Officer (CO) can perform *most* of the SmartGate's management, configuration and administration operations. The User does not have local access to SmartGate and therefore can perform only the functions allowed through the SmartAdmin web tool.

Any registered user can be setup as Remote CO. The authentication used for the user is used to authenticate the Remote CO also.
It should be noted that Remote Crypto Officer can be assigned varying levels (or degrees) of administrative control. There are five levels of administrative privileges for the Remote Crypto Officer.

1. None: Administrators at this level have the ability to view user information only. Access at this level may be limited to certain groups.
2. Minimal: Administrators at this level can only enable or disable users and edit a user's name in the event of a name change or a typographical error. Access at this level may be limited to administration of certain groups.
3. Restricted: In addition to those rights provided at the minimal level, administrators can view OLR info, and edit and delete end users. Access at this level may be limited to administration of certain groups.
4. Standard: In addition to those rights provided at the restricted level, administrators can add, edit, or delete all access permissions and groups. Access at this level may be limited to administration of certain groups.
5. Superuser: Administrators at this level have access to all settings and all groups.

For the services available to the Remote CO, setup as Superuser, has a privilege as the Local CO. The following table lists the Remote Crypto Officer services. For a complete explanation of the Remote CO services see the SmartGate Administrator's Guide.

Service	Description	Privilege Level	Input	Output	CSP	CSP Access
Managing users	View user information and access permissions Enable, disable users, edit user's name Add and delete users, edit all user information, view user's OLR data	All Minimal, Restricted, Standard, Superuser Restricted, Standard, Superuser	Commands and configuration data	Configuration information	Shared Secret Key	Read/ Write
Managing groups	Add, edit, rename, merge, delete groups and authentication timeout values	Standard, Superuser	Commands and configuration data	Configuration information		
Web access control	Access and deny rules for web	Standard, Superuser	Commands and configuration data	Configuration information		
TCP access control	TCP access and deny rules	Standard, Superuser	Commands and configuration data	Configuration information		
OLR setup	OLR webpage options	Superuser	Configuration data			
Administrator rights	Manipulating administrative user and privileges	Superuser	Commands and configuration data	Configuration information		
Port map data	Port Map table displays the port map rules file for the specified server	Superuser	Configuration data	Configuration information		
Configuration	Authentication methods, Proxy encryption methods, configuring server and host port, Logging and backup settings	Superuser	Commands and configuration data	Configuration information		
License information	License Key information	All	Command	License information		

Table 4 – Remote Crypto Officer Services, Descriptions, CSP's

2.3.3 User Role

The User roles access the modules VPN services and authenticates to the module using shared secret key. The User has access to the module's VPN and proxy services, authenticating during the establishment of a VPN session using a shared secret key.

Service	Role Description	Input	Output	CSP	CSP Access
VPN session	Use the VPN services	Encrypted/decrypted data	Encrypt/decrypted data	Session keys	Read/Write
OLR	Establish an account with shared secret key	API calls with account information and shared secret key components (transported via RSA)	Result of OLR negotiation	Shared secret Session key	Read/Write Read/Write
VPN session establishment	Establish VPN session and authenticate using shared secret key	API calls, including proper messages to authenticate with shared secret key	Result of negotiation and session key	Shared secret RDV RDV encryption key FIPS 186-2 Seed-Key FIPS 186-2 Seed Ticket encrypting key Session key	Read Write Read Write Write Write Write
Proxy services	Use proxy services for use with VPN session	Data for proxies (wrapped in VPN session)	Data for proxies (wrapped in VPN session)		

Table 5 – User Services, Descriptions, Inputs and Outputs

2.3.4 Authentication Mechanisms

Passwords (Local Crypto Officer) and Shared secret key (Remote Crypto Officer, Client User) are used to authenticate and authorize users for access to various services based on user permissions and policies.

Role	Authentication Type	Strength
Local Crypto Officer	Passwords	Passwords are required to be at least 6 characters in length. Considering only the case sensitive English alphabet and the numerals 0-9 using a 6 digit password with repetition, the number of potential passwords is 62^6, which equates to a 1 in 62^6 chance of false positive.
User, Remote Crypto Officer	Shared secrets	A shared secret DES/3DES key is used to authenticate the User or Remote Crypto Officer to the module during the VPN handshake. This mechanism is as strong as the DES/3DES using a 56 (DES) or 112 (3DES) bit key, which equates to a 1 in 2^56 (DES) and 2^112 (3DES) chance of false positive.

Table 6 – Roles supported, Authentication type and Strength of Authentication

2.4 Physical Security

The physical security requirements do not apply to this module. SmartGate v4.5 is a software module and does not implement any physical security mechanisms.

Although SmartGate consists entirely of software, the FIPS 140-2 evaluated platform is a standard PC which has been tested for and meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined in Subpart B of FCC Part 15.

2.5 Operational Environment

The SmartGate runs on the general purpose Operating Systems, RedHat Linux or Sun Solaris, which must be configured for single user mode per NIST CMVP guidance for FIPS 140-2 compliance. The module was tested on Red Hat Linux 7.2 and Sun Solaris 8. Configuration of these Operating Systems for single user mode can be found in section 3. Secure Operation.

2.6 Cryptographic Key Management

The module utilizes the following FIPS Approved software algorithm implementations:

- AES (ECB, CBC, CFB, OFB) – FIPS 197 (certificate 35)
  Key Sizes: 128, 192, 256 bits
- DES (ECB, CBC, CFB) – FIPS 46-3 (certificate 159)
  Key Sizes: 56 bits
  Note: DES can only be used for legacy systems.
- Triple DES (ECB, CBC, CFB, OFB) – FIPS 46-3 (certificate 263)

Key Sizes: 112, 168 bits

- SHA-1 – FIPS 180-2 (certificate 87)
- DES-MAC – FIPS 113 (vendor affirmed; DES certificate 159)
- RSA encryption/decryption (key transport) – PKCS#1 (certificate 11 for digital signature generation/verification)
- ANSI X9.31 RNG – Appendix A.2.4 of ANSI X9.31 (certificate 9)
- FIPS 186-2 RNG – General purpose implementation of FIPS 186-2 [(x-Change Notice); (SHA-1)] (certificate 9)

The module implements the following non-FIPS Approved algorithm:

- RC4
- MD5

Only FIPS Approved algorithms may be used when operating the Server in a FIPS 140-2 compliant manner.

The module supports the following critical security parameters:

Key	Key type	Generation	Storage	Zeroization	Use
Shared secret key	DES (56 bits), Triple-DES (112 bits)	Agreed upon during OLR - ½ of the key is generated by the client, the other ½ is generated by SmartGate using the FIPS Approved ANSI X9.31 PRNG. Both the client and the SmartGate exchange their halves of the shared secret key encrypted by the OLR session key. Note: For non-FIPS authentication, the key is generated by client and sent to the SmartGate for the duration of session.	Non-volatile memory (hard drive - plaintext)	Zeroized when the user is deleted	Used for authenticating the user (non-OLR sessions) for client / SmartGate transactions
OLR session key	DES (56 bits), Triple-DES (168 bits), AES (128, 192, 256 bits)	Externally generated by the client and sent to the SmartGate encrypted by the RSA public key.	Volatile memory only (plaintext)	Zeroized when not needed or the module reboots	Used for client / SmartGate communication during the later half of OLR
Session key	DES (56 bits), Triple-DES (168 bits), AES (128, 192, 256 bits)	Externally generated by the client and sent to the SmartGate encrypted by the Ticket Encrypting Key.	Volatile memory only (plaintext)	Zeroized when not needed or the module reboots	Used for client / SmartGate after OLR is successfully completed

Crypto-Officer password (local access)	N/A	Externally generated by the Crypto-Officer and entered over a local port.	Non-volatile memory (hard drive - plaintext)	Zeroized when the password is updated with a new one	Authenticate the Crypto-Officer role when logging into the console
ANSI X9.31 PRNG seed keys	Triple-DES (112 bits)	Externally generated predetermined value.	Non-volatile memory (hard drive – plaintext)	Zeroized by uninstalling the module and then overwriting all addressable locations with a single character and reformatting the module's hard drive	Used by ANSI X9.31 PRNG
ANSI X9.31 PRNG seed	Seed (64 bits)	Internally generated by gathering entropy.	Volatile memory only (plaintext)	Zeroized when the module reboots	Used by ANSI X9.31 PRNG
RSA private key	RSA (1024 bits)	Internally generated using RSA key generation seeded with the ANSI X9.31 PRNG.	Non-volatile memory (hard drive – plaintext)	Zeroized by uninstalling the module and then overwriting all addressable locations with a single character and reformatting the module's hard drive	Key transport from client to SmartGate during OLR
RSA public key	RSA (1024 bits)	Internally generated using RSA key generation seeded with the ANSI X9.31 PRNG.	Non-volatile memory (hard drive - plaintext)	Zeroized by uninstalling the module and then overwriting all addressable locations with a single character and reformatting the module's hard drive	Key transport from client to SmartGate during OLR
DES-MAC key	DES (56 bits)	Externally generated predetermined value.	Non-volatile memory (hard drive – plaintext) in module binaries	Zeroized by uninstalling the module and then overwriting all addressable locations with a single character and reformatting the module's hard drive	Software integrity check
Authentication & Proxy communication Key	Triple-DES (112 bits)	Internally generated during OLR by ANSI X9.31 PRNG	Non-volatile memory (hard drive – plaintext)	Zeroized by uninstalling the module and then overwriting all addressable locations with a single character and	Authentication server and Proxy server use shared secret keys to exchange user data.

				reformatting the module's hard drive	
Random data value (RDV)	256 bits random data	Externally generated by the client and sent to the SmartGate encrypted with the Shared Secret Key when the client initiates a session.	Volatile memory only (plaintext)	Zeroized when not needed or the module reboots	For seeding the FIPS 186-2 PRNG
RDV encryption key	AES (256 bits)	Externally generated predetermined value.	Non-volatile memory (hard drive – plaintext)	Zeroized by uninstalling the module and then overwriting all addressable locations with a single character and reformatting the module's hard drive	For encrypting the RDV
UID encryption key	AES (128 bits)	Externally generated predetermined value.	Non-volatile memory (hard drive – plaintext)	Zeroized by uninstalling the module and then overwriting all addressable locations with a single character and reformatting the module's hard drive	For encrypting the user ID
FIPS 186-2 PRNG Seed Key	Seed-Key (160 bits)	Internally generated by whitening RDV using DES with the shared secret key	Volatile memory only (plaintext)	Zeroized when not needed or the module reboots	Used by FIPS 186-2 PRNG
FIPS 186-2 PRNG Seed	Seed (96 bits)	Internally generated by whitening RDV using DES with the shared secret key	Volatile memory only (plaintext)	Zeroized when not needed or the module reboots	Used by FIPS 186-2 PRNG
Ticket Encrypting Key	DES (56 bits), Triple-DES (168 bits), AES (128, 192, 256 bits)	Internally generated by the FIPS 186-2 PRNG	Volatile memory only (plaintext)	Zeroized when not needed or the module reboots	For encrypting the handshake session messages

Table 7 – Listing of Key and Critical Security Parameters

SmartGate securely administers all of its cryptographic keys, which include the server's public/private key pair; user shared secret keys, and ephemeral session keys. SmartGate stores and transmits all sensitive data in encrypted form. All session keys are ephemeral and are discarded immediately after use. Shared secret keys that are electronically distributed during the optional database backup process are done so in encrypted form.

2.7 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The SmartGate includes an array of self-tests.

Power-up self-tests:

- Software integrity check: Verifying the integrity of the software binaries of the module using a DES-MAC.
- AES Known Answer Test (KAT): Verifying the correct operation of the AES algorithm implementation
- DES KAT: Verifying the correct operation of the DES algorithm implementation
- Triple-DES KAT: Verifying the correct operation of the Triple-DES algorithm implementation
- RSA encrypt/decrypt pair-wise consistency check: Verifying the correct operation of the RSA implementation
- RSA sign/verify pair-wise consistency check: Verifying the correct operation of the RSA implementation
- SHA-1 KAT: Verifying the correct operation of the SHA-1 algorithm implementation
- ANSI X9.31 RNG KAT: Verifying the correct operation of the ANSI X9.31 RNG implementation
- FIPS 186-2 RNG KAT: Verifying the correct operation of the FIPS 186-2 RNG implementation.

Conditional self-tests:

- RSA encrypt/decrypt pair-wise consistency check: Verifying that a newly generated or stored RSA key pair works properly
- RSA sign/verify pair-wise consistency check: Verifying that a newly generated or stored RSA key pair works properly

- ANSI X9.31 Continuous RNG: Verifying the RNG has not failed to a constant value
- FIPS 186-2 Continuous RNG: Verifying the RNG has not failed to a constant value

The SmartGate will start its services only after all the self tests are passed. If the self tests are not passed, it enters an error state and logs the failure. All error conditions can be cleared by cycling the module's power.

2.8 Design Assurance

AEP utilizes Microsoft Visual Source Safe (VSS) version 6.0 for its version control system. This software provides access control, versioning, and logging.

2.9 Mitigation of Other Attacks

This section is not applicable. The SmartGate v4.5 does not claim to mitigate any attacks beyond the FIPS 140-2 level 1 requirements for this validation.

3. Secure Operation

The SmartGate meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS Approved mode of operation. Operating the SmartGate without maintaining the following settings will remove the module from the FIPS Approved mode of operation.

3.1 Crypto Officer Guidance

The Local Crypto Officer is responsible for installation and initialization of the module, configuration and management of the module, and removal of the module. More details on how to use the module can be found in the SmartGate Administrator's Guide.

3.1.1 Initial Setup

There is no access control provided by the module until it has been installed and initialized. Therefore, the Crypto Officer must maintain control of the installation media.

FIPS 140-2 mandates that a cryptographic module be limited to a single user at a time. Before the module can be installed, the Local Crypto Officer must have a standard PC running RedHat Linux or Sun Solaris, and these Operating Systems must be configured for single user mode.

To ensure that RedHat Linux or Sun Solaris is running in single user mode, the Local Crypto Officer must delete or disable all accounts except for the root account. Additionally, to ensure only one user can be logged in at a time, the root account must be configured to only allow console access logins and all remote server services must be disabled (e.g., telnet or rlogin server daemon).

The specific procedure to configure RedHat Linux System for single user is described below.

a) Log in as the "root" user.
b) Edit the system files /etc/passwd and /etc/shadow and remove all the users except "root" and the pseudo-users. Make sure the password fields in /etc/shadow for the pseudo-users are either a star (*) or double exclamation mark (!!). This prevents login as the pseudo-users.
c) Edit the system file /etc/nsswitch.conf and make "files" the only option for "passwd", "group", and "shadow". This disables NIS and other name services for users and groups.
d) In the /etc/xinetd.d directory, edit the files "rexec", "rlogin", "rsh", "rsync", "telnet", and "wu-ftpd", and set the value of "disable" to "yes".
e) Reboot the system for the changes to take effect.

- More information can be found at: http://csrc.nist.gov/cryptval/140-1/CMVPFAQ.pdf

The specific procedure to configure Solaris System for single user is described below.

a) Login as the "root" user.

b) Edit the system files /etc/passwd and /etc/shadow and remove all the users except "root" and the pseudo-users (daemon users). Make sure the password fields in /etc/shadow for the pseudo-users are either a star (*) or double exclamation mark (!!). This prevents login as the pseudo-users.
Also make sure the shell for daemon users is /dev/null, or something else unexploitable.

c) Edit the system file /etc/nsswitch.conf and make "files" the only option for "passwd", "group", and "shadow". This disables NIS and other name services for users and groups.

d) Edit the system file /etc/inet/inetd.conf, and comment out all unnecessary services (by prepending a hash '#' to the beginning of each unnecessary service line).
(generally) Unnecessary services:
sadmind - Solstice network administration agent server
rpc.ttdbserverd - Sun tool-talk server
kcms_server - Kodak Color Management System server
fs.auto - Sun font server
cachefsd - NFS cache service
rquotad - remote disk quota server
rpc.metad - Disksuite remote metaset service
rpc.metamhd - Disksuite remote multihost service
rpc.metamedd - Disksuite component service
ocfserv - Smartcard service
dtspcd - Part of the CDE package
rpc.cmsd - remote calendar server
in.comsat - biff, mail notification server
in.talkd - talk server
gssd - RPC application authentication
in.tnamed - deprecated name server
rpc.smserverd - removable media device sensor service (disabling requires manual CD mounting)
dcs - remote dynamic configuration server
ftpd - ye olde FTP server
ktkt_warnd - Kerberos warning server
chargen - deprecated network service
daytime - deprecated network time
time - legacy time service

discard - deprecated network service
echo - network 'echo' service
ufsd - part of RPC
in.uucpd - unix-to-unix copy server
In short, you should be able to disable all services, so long as the Solaris machine is not part of any cluster environment.

e) Disable service startup scripts within /etc/rc2.d. Many additional services (not bound to inetd) are started by default. To disable startup scripts, you may rename the files, just to be sure they don't begin with a cap-S (which denotes Startup). Disable startup scripts that are not pertinent to your setup. Suggestions:
nscd - NIS-related
snmpdx - SNMP services
cachefs.daemon - NFS-caching
rpc - Remote Procedure Call services
sendmail - Sendmail
lp - line printer daemon
pppd - Point-to-point Protocol services
uucp - Unix-to-Unix copy daemon
ldap - LDAP services

f) Reboot the system for the changes to take effect.

The Local Crypto Officer password for the module is the default of the host Operating System after installation. It is recommended that this is changed immediately upon logging into the module after installation.

Once the Operating System has been properly configured, the Local Crypto Officer ("root" account) can be used for installing/uninstalling software and creating/administrating SmartGate. For Server installing instructions refer to the *SmartGate Administrator's Guide – Server Installation on UNIX Operating Systems*.

3.1.2 Management

The SmartGate provides numerous configuration options to ensure its versatility. FIPS 140-2 compliance demands the following options be configured as specified in the following:

1. The Authentication Encryption Method (AuthEncryptMethod) must be set to AES, 3DES or DES (SmartGate default is 3DES).
2. The SmartGate Encryption Methods (SGEncryptMethod) must be set to AES, 3DES or DES (SmartGate default is 3DES).
3. The Proxy Encryption Methods (ProxyEncryptMethod) must be set to AES, 3DES or DES (SmartGate default is 3DES).
4. RSA key pair for OLR must be set to use 1024 bytes or greater (SmartGate default is 1024).

5. The Hash Method (HashMethod) must be set to SHA-1 (SmartGate default is SHA-1 and MD5).
6. The SmartGate Java Client must not be installed or must be disabled.

Note: DES can only be used for legacy systems.

For guidance on configuring these options, see the *Console Administration* sections of the SmartGate Administrator's Guide.

The Local Crypto Officer should monitor the module's status by regularly checking the log information. If strange activity is indicated or the module is consistently having errors, then AEP customer support should be contacted.

3.1.3 Zeroization

At the end of the life cycle of the module, the Local Crypto Officer must uninstall the module's software and then overwrite all addressable locations with a single character and reformat the hard drive which contained the software. This will zeroize all keys and other CSP's.

3.2 Remote Crypto Officer Guidance

The Remote Crypto Officer can perform most of the SmartGate's management, configuration and administration operations. More details on how to use the module can be found in the SmartGate Administrator's Guide.

3.2.1 Management

The SmartGate provides numerous configuration options to ensure its versatility. FIPS 140-2 compliance demands the following options be configured as specified in the following:

1. The Authentication Encryption Method (AuthEncryptMethod) must be set to AES, 3DES or DES (SmartGate default is 3DES).
2. The SmartGate Encryption Methods (SGEncryptMethod) must be set to AES, 3DES or DES (SmartGate default is 3DES).
3. The Proxy Encryption Methods (ProxyEncryptMethod) must be set to AES, 3DES or DES (SmartGate default is 3DES).
4. RSA key pair for OLR must be set to use 1024 bytes or greater (SmartGate default is 1024).
5. The Hash Method (HashMethod) must be set to SHA-1 (SmartGate default is SHA-1 and MD5).

Note: DES can only be used for legacy systems.

For guidance on configuring these options, see the *Using SmartAdmin Web Administration* of the SmartGate Administrator's Guide.

3.3 User Guidance

The User access the module's VPN functionality as a client. Although the User does not have any ability to modify the configuration of the module care should be taken not to provide authentication information and access codes to other parties.

4. ACRONYMS

3DES	Triple DES
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining mode of operation
CFB	Cipher FeedBack mode of operation
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
DES	Digital Encryption Standard
ECB	Electronic CodeBook mode of operation
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OFB	Output FeedBack mode of operation
OLR	On-Line Registration
OS	Operating System
PC	Personal Computer
RNG	Random Number Generator
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SP	Secure Platform
TCP	Transmission Control Protocol
VSS	Visual Source Safe
VPN	Virtual Private Network