SmartGate®

FIPS 140-1 Non-Proprietary Security Policy

Level 1 Validation

February 2002

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for version 4.3 of V-ONE's SmartGate(R). This security policy describes how the SmartGate 4.3 meets the security requirements of FIPS 140-1, and how to operate SmartGate in a secure FIPS 140-1 mode. This policy was prepared as part of the level 1 FIPS 140-1 certification of SmartGate.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-1 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

1.2 References

This document deals only with operations and capabilities of SmartGate in the technical terms of a FIPS 140-1 Cryptographic Module Security Policy. More information is available on SmartGate and the complete suite of V-ONE networking solutions from http://www.v-one.com/.

1.3 Terminology

In this document, version 4.3 of the SmartGate Server will be referred to as the SmartGate, the module, the server, or the SmartGate server.

1.4 Document Organization

The Security Policy document is one document in complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

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

This document provides an overview of the SmartGate server software and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the SmartGate server. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

Corsec Security, Inc. produced this Security Policy and other Certification Submission Documentation under contract to V-ONE Corporation. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Certification Submission Documentation is V-ONE Corporation-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact V-ONE Corporation.

2 The SmartGate Server

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's strong user authentication, authorization, management, accounting, encryption, key distribution, and proxy capabilities provides organizations 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.

2.1 Module Interfaces

SmartGate server is classified as a multi-chip standalone module for FIPS 140-1 purposes. As such, the module includes a computer running an operating system (OS) with physical interfaces including a computer keyboard, mouse, screen, floppy drives, CD-ROM drives, speakers, microphone inputs, serial ports, parallel ports, and power plug.

The logical interfaces of SmartGate server consist of a set of logical network interfaces and Application Programming Interfaces (APIs). The following is a list of the logical interfaces implemented by the module as required by FIPS 140-1:

- Data input – data received via the SmartGate Single Port Proxy (sgproxy) and data received as variables passed to the module's API
- Data output – data output via the SmartGate Single Port Proxy (sgproxy) and data returned from the module's API
- Control input – 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
- Status output – data output to log files, command line interface, and the SmartAdmin Web Adminstration tool

The SmartGate Single Port Proxy's primary purpose is to provide the various SmartGate services with a single-port presence on the perimeter of the network. This means that all client-to-SmartGate connectivity will pass through the Single Port Proxy and be forwarded to the correct destination SmartGate service.

2.2 Roles and Services

As required by FIPS 140-1, there are two main roles an operator can assume when working with the SmartGate server: the Crypto Officer (CO) role and the User role. The local administrator of the module assumes the Crypto Officer role and can configure the SmartGate server via console administration (command line or screen) and manually editing configuration files. An operator assuming the role of User has some administrator privileges but is limited to accessing SmartGate remotely through the SmartAdmin Web Tool. Although not required by FIPS 140-1 at level 1, both roles require identity-based authentication.

There is no factory default login ID and password, which allows access to the CO role. Instead, SmartGate allows an user with administrative privileges on the host OS to completely manage the SmartGate and its users.

2.2.1 Crypto Officer Services

A Crypto Officer (CO) is expected in install and configuration the SmartGate. Once, the SmartGate is running, the CO can perform all management, configuration and administration of the SmartGate server. The CO can locally manage the SmartGate server thru console administration (command line or screen) and manually editing configuration files.

At the highest level, the Crypto Officer services include:

- Installing the SmartGate product
- Creating SmartGate RSA public/private key pair
- Managing Users and Groups
- Defining Access Permissions
- Setting Up On-Line Registration (OLR)
- Defining Authentication Settings
- Configuring Logging
- Rebooting the server

It should be noted that Crypto Officers can be assigned varying levels (or degrees) of administrative control. For a complete explanation of the Crypto Officer services see the SmartGate Administrator’s Guide.

2.2.2 User Services

The User 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.

At the highest level, the User services include:

- Managing Users and Groups
- Defining Access Permissions
- Setting Up On-Line Registration (OLR)
- Defining Authentication Settings
- Configuring Logging

It should be noted that Users can be assigned varying levels (or degrees) of administrative control. For a complete explanation of the User services see the SmartGate Administrator’s Guide.

2.3 Finite State Machine Model

The SmartGate is designed around a Finite State Machine (FSM) which is detailed in a V-ONE-proprietary document (*FIPS 140-1 Proprietary Finite State Machine*). Parties interested in reviewing this document should contact V-ONE thorough the sources listed in Section 1.2.

2.4 Physical Security

The SmartGate server is a software module evaluated for use with the RedHat Linux and Solaris operating systems but will also operate under Microsoft Windows NT/2000/XP, and other Linux distributions. The module was tested against FIPS 140-1 requirements on a standard Intel platform Personal Computer (PC) that meets all FIPS 140-1 level 1 physical requirements. This platform provides production grade equipment, industry-standard passivation, and a strong enclosure.

Although SmartGate consists entirely of software, the FIPS 140-1 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 Cryptographic Key Management

SmartGate server securely administers all its cryptographic keys. This includes the server's public/private key pair, user shared secret keys, a database encryption key, and ephemeral session keys. SmartGate server 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.

2.6 Cryptographic Algorithms

SmartGate provides support for the following FIPS approved algorithms:

- DES ECB
- DES CBC
- DES CFB
- 3-Key Triple DES CBC
- 3-Key Triple DES CFB
- SHA-1
- RSA (public/private key generation)
- Diffie-Hellman (key agreement)

Additionally, support is provided for the following non-FIPS-approved algorithms:

- RC4
- MD5

Only FIPS-approved algorithms may be used when operating the SmartGate in a FIPS 140-1 compliant manner.

2.7 Self-Tests

As required by FIPS 140-1, SmartGate performs a number of startup and conditional self-tests to ensure proper operation. Self-tests include integrity checks over each binary component, cryptographic algorithm tests, and a continuous random number generator test that monitors output from the module's FIPS-approved random number generator.

3 Secure Operation of SmartGate Server

The V-ONE SmartGate server meets all the level 1 requirements for FIPS 140-1. Follow the setting instructions provided below to place the module in FIPS compliant mode of operation. Operating SmartGate without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 System Initialization and Configuration

SmartGate server provides numerous configuration options to ensure its versatility. FIPS 140-1 compliance demands the following options be configured as specified. For guidance on configuring these options, see the *Using SmartAdmin Web Administration* and/or *Console Administration* sections of the SmartGate Administrator's Guide.

1. The Authentication Encryption Method (AuthEncryptMethod) must be set to 3DES or DES (SmartGate default is 3DES).
2. The SmartGate Encryption Methods (SGEncryptMethod) must be set to 3DES or DES (SmartGate default is 3DES).
3. The Proxy Encryption Methods (ProxyEncryptMethod) must be set to 3DES or DES (SmartGate default is 3DES).
4. RSA key pair for OLR must be set to use 1024 bytes (SmartGate default is 1024).
5. The Hash Method (HashMethod) must be set to SHA-1 only (SmartGate default is SHA-1 and MD5).
6. The SmartGate Java Client must not be installed or must be disabled.
7. The operating system must be configured to limit use of the module to a single user at a time. These procedures are described below.

3.2 Configuring Linux or Solaris for "single-user mode"

FIPS 140-1 mandates that a cryptographic module be limited to a single user at a time. To ensure that Linux or Solaris meets this requirement the administrator 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). Services that only allow local access connections (e.g., the SmartGate proxies) or client applications that perform outgoing connections (e.g., telnet client, ftp client, web browser, etc.) are allowed. The root account will be used for installing/uninstalling software and creating/administrating SmartGate.

4 Acronym List

3DES	Triple DES (see DES)
API	Application Programming Interface
CD-ROM	Compact Disk – Read Only Memory
CO	Crypto Officer
DES	Data Encryption Standard
FIPS	Federal Information Processing Standard
FSM	Finite State Machine
MD5	Message Digest Algorithm
OLR	On-Line Registration
OS	Operating System
PC	Personal Computer
SHA-1	Secure Hash Algorithm
V-ONE	Virtual Open Network Environment
VPN	Virtual Private Network