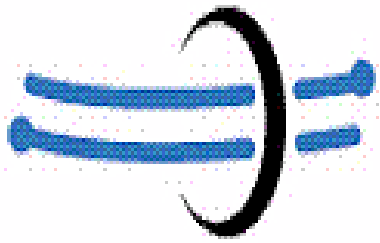


BLUE RIDGE
NETWORKS

BorderGuard X.509 VPN Client 4.0

FIPS 140-2 Security Policy

Version 1.0

1. Introduction

This non-proprietary cryptographic module security policy describes how version 4.0 of the BorderGuard X.509 VPN Client meets the security requirements of FIPS 140-2, and how to run the VPN Client in secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the VPN Client. The BorderGuard X.509 VPN Client is referred to in this document as the VPN Client, the software client, and 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 NIST web site at:

http://csrc.nist.gov/cryptval/

The security policy document is organized in the following sections.

Introduction

- References
- Document Organization

BorderGuard X.509 VPN Client

- Overview
- VPN Client Interfaces
- Roles and Services
- Physical Security
- Cryptographic Key Management
- Self-Tests
- Design Assurance
- Mitigation of Other Attacks

Secure Operation

1.1 References

This document describes the operations and capabilities of the BorderGuard X.509 VPN Client only in the technical terms of FIPS 140-2 cryptographic module security policy. More information is available on the VPN Client in the following documents:

The Blue Ridge Networks Inc. web site (http://www.blueridgenetworks.com) contains information on the full line of products from Blue Ridge Networks Inc.

The NIST Validated Modules web site (http://csrc.ncsl.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

BorderGuard X.509 VPN Client User Guide, Release 4.0 — explains how to install, configure, and use the VPN Client. The VPN Client lets a remote user securely establish and maintain a remote VPN session with a BorderGuard Network Appliance. There is additional documentation provided for troubleshooting as well.

1.2 Documentation Organization

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

- Vendor Evidence Document
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Blue Ridge Networks and is releasable only under appropriate non-disclosure agreements. For access to these documents, contact Blue Ridge Networks.

2. BorderGuard X.509 VPN Client

This section presents an overview of the BorderGuard X.509 VPN Client, its interfaces, roles and services, authentication mechanisms, cryptographic key management, design assurance, and mitigation of attacks.

2.1 Overview

The BorderGuard X.509 VPN Client is a set of software applications that runs on a Microsoft ® Windows ® based PC configured in a single-user mode. The VPN Client running on a remote PC and communicating with a BorderGuard Network Appliance at an enterprise or service provider creates a secure connection over the Internet using Data Privacy Facility (DPF), an IPSEC variant proprietary protocol that lets you access a private network as if you were an on-site user. This secure connection is a Virtual Private Network (VPN). Data Privacy Facility (DPF) uses the Diffie-Hellman cryptographic protocol for purposes of key establishment to support VPN connection creation.

Some of the features of the VPN Client are:

- Support for BorderGuard 6000 Series Network Appliance.
- Local LAN access — The ability to access resources on a local LAN while connected through a secure gateway to a central-site VPN server (if the central site grants permission)
- Automatic VPN Client configuration option — the ability to import a configuration file containing information for remote access set up.
- Log Viewing— the ability of collecting events associated with the remote access session for viewing and analysis.
- Smart Card Support — Support for the use of a smart card associated with a X.509 digital certificate.
- Secure Wireless Roaming — ability for a remote user to maintain VPN session connectivity, confidentiality, integrity while physically moving to a new wireless network.
- Automatic connection using Microsoft Dial-Up Networking or the use of some third-party remote access dialer.

For a complete list of features please reference the BorderGuard X.509 VPN Client User Guide, Release 4.0.

2.2 VPN Client Interfaces

The BorderGuard X.509 VPN Software Client is a software module that runs on the Windows platform. It runs and was tested on the following Operating Systems:

- Windows 2000
- Windows XP

The cryptographic boundary of the software client supports the physical interfaces of the standard PC. The physical interfaces include the computer keyboard port, CDROM drive, floppy disk, mouse, network port, monitor port and power plug. The PC network port includes the serial ports, parallel ports, Ethernet ports and NIC cards. The functional module interface exists in the software.

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

TABLE 1. ***VPN Client Physical Interfaces and Logical 140-2 Interfaces***

VPN Client Physical Interface	FIPS 140-2 Logical Interface
Standard PC ports	Data input interface
Standard PC ports	Data output interface
Standard PC ports	Control input interface
LEDs, PC monitor, PC network port	Status output interface
PC power interface	Power interface

The physical interfaces are mapped to the logical interfaces in the following way:

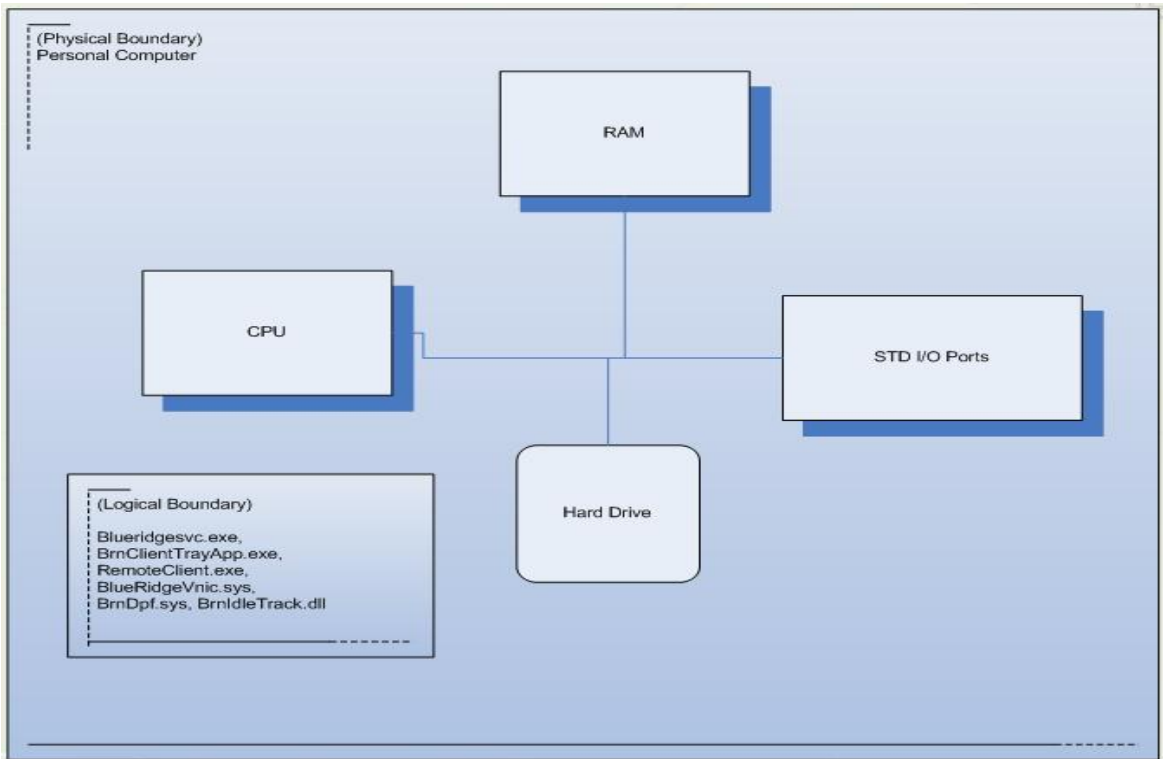
TABLE 2. ***FIPS 140-2 Logical Interfaces***

Logical Interface	Program Mapping
Control Input	A BorderGuard Network Appliance pushes security policies and parameters to a BorderGuard X.509 VPN Client. In addition, the following programs also control input: brnclienttrayapp.exe, remoteclient.exe, blueridgevnic.sys, brndpf.sys,
Data Input	The data input is all data coming into the network port. Programs providing this interface are: blueridgevnic.sys, brndpf.sys.
Data Output	The data output is any data sent through the network stack. This includes all application data (e-mail, web browser, telnet etc.).
Status Output	The status output comprises all messages either logged by the module or returned by the module. Error messages from DPF key exchange negotiations are also status output. Programs providing this interface are: brnclienttrayapp.exe, remoteclient.exe, blueridgevnic.sys, brndpf.sys, brnidletrack.dll,

The VPN Client provides programs with Graphical User Interfaces to configure and interact with the module. The following is a list of executables that the module uses.

TABLE 3. ***BorderGuard X.509 VPN Client executables***

Executable	Description
blueridgesvc.exe	VPN client service providing execution of user-defined commands.
brnclienttrayapp.exe	GUI for VPN client; connects/disconnects VPN tunnels, and creates remote access connection profiles.
remoteclient.exe	VPN client service; handles communication between all aspects of VPN client, initiates DPF key exchange on behalf of the User for given remote access connection
blueridgevnic.sys	VPN client virtual network interface device driver.
brndpf.sys	VPN client cryptographic device driver providing confidentiality and integrity for remote access sessions.
brnidletrack.dll	DLL supports the ability to track user in-activity during a remote access session.



2.3 Roles and Services

As required by FIPS 140-2, there are two main roles in the module that operators may assume: Crypto-Officer and User. These roles are logically separated. The BorderGuard X.509 VPN Client does not implement authentication mechanisms for any role. Also, the module does not allow concurrent operators.

The operators can access all keys and services in the module, because they are separated only logically.

2.3.1 Crypto-Officer Role

The Crypto-Officer can install/un-install the BorderGuard X.509 VPN Client. All the services available to the Users are also available to the Crypto-Officer. For descriptions of the services available to the Crypto-Officer and User roles, see Table 4.

Configuring, managing and monitoring the BorderGuard Network Appliance with which the client is working is also considered to be a Crypto-Officer role. The BorderGuard Network Appliance pushes the tunneling policy to the BorderGuard X.509 VPN Client software over a DPF tunnel and is responsible for assuring that only FIPS-Approved algorithms are used for DPF negotiations.

2.3.2 User Role

A user can access the VPN service provided by the module and create tunnels with the proper session establishment. Service descriptions and inputs/outputs are listed in the following table:

TABLE 4. Services that a Crypto-Officer and a User can perform

Service	Role	Action
Installing and Uninstalling the module	Crypto-Officer	Installs and uninstalls the VPN Client.
Configuring user/tunnel characteristics (X.509 Digital Certificates Usage, remote access connection attributes)	Crypto-Officer	Used in creating DPF tunnels. Remote access connection attributes such as dial-up requirements, multiple BorderGuard Network Appliance addresses, X.509 digital certificate assignment, user-defined commands.
Creating DPF tunnels (Encryption, Decryption, hashing, HMAC)	User, Crypto-Officer	Both Users and a Crypto-Officer can create tunnels.

Showing status; performing Self-Tests	Crypto-Officer	The Crypto-Officer can view the log files. The current status of the module including the self-test-output information can be seen in the log files.

2.4 Physical Security

BorderGuard X.509 VPN Client is a multi-chip, standalone cryptographic module. The module's physical boundary is the PC case in which it is running. The module is enclosed in a removable PC cover, which is an industry standard, production grade covering on all standard PCs.

2.5 Cryptographic Key Management

The module uses the following FIPS-approved algorithms.

- Symmetric Key Algorithms

Algorithm	Modes Implemented	Key Sizes
Triple DES (FIPS 46-3)	CBC	168 bits
AES (FIPS 197)	CBC	128, 196, 256 bits

- Hashing Algorithm
  - SHS (SHA-1) (FIPS 180-1)
- Message Authentication Algorithms
  - HMAC SHA-1 (FIPS-198)

The certificate numbers of the algorithms are as follows:

- SHS: Certs. #463 and #467
- Triple DES: Certs. #432 and #448
- AES: Certs. #386 and #418
- HMAC: Certs. #173 and #192

The module supports the following non-FIPS approved algorithms:

- MD5
- DES (Use by legacy systems)
- IDEA
- HMAC-MD5
- Diffie-Hellman (While not approved, it may be used in FIPS mode)
- RSA (While not approved, it may be used in FIPS mode)

- RNG (Not approved, only used to create keys for authentication purposes.)

The BorderGuard X.509 VPN Client supports only logical separation of users and operates in a single user mode. Hence the files (containing keys) in the module have read/write access permissions for all users. The operating system principles of file locking and open file access restriction (no other process can write/delete a file opened by another process) prevent unwanted modification or deletion of files. As an exception, operators do not have read and write access to the DPF session keys, which are stored in RAM, but can zeroize (Delete) them by closing the DPF tunnel.

Operators have no access to CSP's. The BorderGuard X.509 VPN Client supports the following critical security parameters:

TABLE 5. ***Security Parameters that the VPN Client Supports***

Cryptographic Key	Description	Key Type	Storage and Zeroization
HMAC Cryptographic Module Integrity Key	Used by the module for the "Strong" software integrity test at power-up. This CSP is hard-coded and embedded within the module binary.	HMAC (160 bit)	This CSP is hard-coded and embedded within the module binary. It is zeroized when the module is deleted from memory or by reformatting the hard drive.
Diffie-Hellman Keys	Used by the module in the establishment of DPF Session Keys and Packet Integrity Keys	Diffie-Hellman (512 bit, 1024 bit). Key establishment methodology provides 56 to 80 bits of encryption strength.	The volatile memory location that stores the key pair (in RAM) is obfuscated from visual inspection and cannot be accessed. It is zeroized after session establishment.
VPN Client RSA public/ private keys	Used by the module for DPF to authenticate communicating modules. This helps establish a security association with a BorderGuard Network Appliance. This is randomly generated by the VPN client at each user's request for remote access.	RSA public/private keys (512/1024 bits)	The volatile memory location that stores the key pair (in RAM) is obfuscated from visual inspection and cannot be accessed. It is zeroized when a DPF tunnel is terminated or can not complete a successful DPF negotiation process.
Packet Integrity Key	Generated in DPF transactions to perform packet integrity checks	HMAC (160 bit)	Stored only in volatile memory (RAM); zeroized once DPF tunnel is terminated.

BorderGuard Network Appliance RSA Public Key	Obtained by the module during X.509 digital certificate validation phase of authentication.	RSA public key (512/1024 bits)	The volatile memory location that stores the public key (in RAM) is obfuscated from visual inspection and can not be access. It is zeroized when a DPF tunnel is terminated or can not complete a successful DPF negotiation process.
DPF Session Keys	Generated in DPF transactions to encrypt tunnels; destroyed when the tunnel is destroyed	Either AES or 3DES keys depending on the negotiated algorithm	Stored only in volatile memory (RAM); zeroized once a DPF tunnel is terminated.

2.5.1 Diffie-Hellman and RSA Key Management

The BorderGuard X.509 VPN Client creates Diffie-Hellman key agreements and RSA keys for remote access identity to a BorderGuard Network Appliance providing VPN services. DPF session keys are established using Diffie-Hellman key agreement. The implemented RNG is not approved and only generates keys used for authentication purposes.

2.5.2 Key Storage

The BorderGuard X.509 VPN Client has two classes of key storage on a general purpose personal computer. Public/Private Keys for authentication and Traffic keys for cryptographic sessions (AES keys, for example) are always transient and are never placed in nonvolatile storage. They are stored in general purpose RAM; operating system controls make all access to memory regions inaccessible to other processes running. Areas in memory holding key material have been obfuscated as well to counter visual inspection. The second class is the HMAC module integrity key, which is hard-coded and embedded within the module binary.

2.5.3 Key Destruction

All keys can be zeroized by uninstalling the module. Restarting the module or rebooting the general purpose personal computer zeroizes all session keys.

2.6 Self-Tests

The BorderGuard X.509 VPN Client provides the following power-up self-tests:

- Software integrity test
- DES KAT
- Triple-DES KAT

- AES KAT
- SHS KAT
- HMAC-SHA1 KAT
- Statistical PRNG Tests

The BorderGuard X.509 VPN Client performs all power-up self-tests automatically each time it starts. All power-up self-tests must be passed before allowing any operator to perform any cryptographic services. The power-up self-tests are performed after the cryptographic systems are initialized, but prior to reading any security associations and creating network connections. This prevents the module from passing any data during a power-up self-test failure. In the unlikely event a power-up self-test fails, the VPN Client displays a message indicating the error and does not allow further use.

In addition, the VPN Client also provides the following conditional self-tests:

- Continuous Random Number Generator Test for the PRNG
- RSA Public/Private Key Pairwise Consistency Test

In the unlikely event a PRNG test or RSA pairwise consistency conditional self-test fails, the VPN Client displays an error message and logs a message into a session log file and requests that the user perform another remote access VPN connection attempt.

2.7 Design Assurance

Blue Ridge Networks uses the Microsoft Visual Source Safe Configuration Management System. Visual Source Safe is used for software and document version control, code sharing and build management.

The configuration management system is used for *software lifecycle modeling*. Software life-cycle modeling is the business of tracking source code as it goes through various stages throughout its life, from development, to testing, release, reuse, and retirement. Blue Ridge Networks also uses the best practices for configuration management to perform the following processes:

- Workspaces - where developers build, test, and debug
- Codelines - the canonical sets of source files
- Branches - variants of the codeline
- Change propagation - getting changes from one codeline to another
- Builds - turning source files into products

Blue Ridge Networks follows best software engineering principles in designing, developing, tracking and documenting software modules. The FIPS submission documentation is maintained and tracked using Visual Source Safe.

2.8 Mitigation of other attacks

The BorderGuard X.509 VPN Client does not claim to mitigate any attacks.

3. Secure Operation

The BorderGuard X.509 VPN Client meets Level 1 requirements for FIPS 140-2. The section below describes how to place and keep the module in FIPS-approved mode of operation.

3.1 Initial Setup

To ensure that the BorderGuard X.509 VPN Client operates in FIPS mode, the corresponding BorderGuard Network Appliance is configured in FIPS mode using only FIPS approved algorithms during DPF negotiations.