Lenel OnGuard Access Control Cryptographic Module

FIPS Key Generator Security Policy

Document *Version 2.8*

Lenel Systems International, Inc.
www.lenel.com

February 22, 2012

Revision History

Revision History			
Version	***Date***	***Author***	***Notes***
2.8	2/22/2012	Robert Pethick	Updated to discuss Key Generator module only and added additional tested operating systems.
2.7	01/23/2009	David Weinbach	Response to CMVP review comments.
2.6	12/17/2008	David Weinbach	Response to CMVP review comments: FIPS Mode Configuration Utility does not implement an Approved crypto algorithm by itself.
2.5	10/21/2008	David Weinbach	Response to CMVP review comments.
2.4	10/7/2008	David Weinbach	Response to CMVP review comments.
2.3	09/16/2008	David Weinbach	Response to CMVP review comments.
2.2	05/09/2008	David Weinbach	Clarifications added to meet requirements for splitting the Validation Report package into three Validation Report packages, one each for the Lenel: • FIPS Key Generator • FIPS Mode Configuration Utility • Communication Server Each of these components will receive their own FIPS 140-2 module validations with the caveat that they operate as a bundled package.
2.1	07/09/2007	Michael Serafin	Minor updates based on CMVP comments.
2.0	11/28/2006	Michael Serafin	Minor updates on additional review by InfoGard.
1.9	11/13/2006	Michael Serafin	Updates based on review done by InfoGard.
1.8	11/09/2006	Michael Serafin	Updated security rule #6 in section 8.

1.7	10/12/2006	Michael Serafin	Updated Lenel logo. Updated software version information. Update to 8.4.B.3 to indicate that the bypass test is performed by the FIPS Mode Configuration Utility.
1.6	09/25/2006	Michael Serafin	Updates to Figure 1 to include Mercury's DLL (scpd_net.dll). Update to Section 3.1 to include information on seed material. Updated table in Section 4 to include additional ports and interfaces for RPC calls, COM calls, database interaction.
1.5	04/17/2006	Michael Serafin	Added information on conditional bypass test to section 8.
1.4	02/22/2006	Michael Serafin	Updates based on feedback from InfoGard: • The date on revision 1.3 indicated 2005 instead of 2006. • Updated Figure 1 to include Microsoft's RSAENH.dll. • Section 1 was updated to include a statement that lists the various components. • The SHA-1 algorithm has been added to section 3.1. • Section 3.1 updated to clarify that the certificates are for the Mercury Scpd_net.dll. • Key Generation service added to Section 6. • Numerous updates to section 8.
1.3	01/09/2006	Michael Serafin	• Added Lenel logo to document. • Updated validation numbers for Mercury

			for Windows Server 2003 SP 1. • Updated the information on the intended Windows operating system. • Updated section 5.1 • Added section 3.2.
1.2	11/09/2005	Michael Serafin	Updated based on feedback from InfoGard.
1.1	09/28/2005	Michael Serafin	Revised to reflect changes made to the module.
1.0	06/06/2005	InfoGard	Initial template from InfoGard.

Table of Contents

1. Module Overview

The Lenel OnGuard Access Control "Key Generation" Cryptographic Module is a software only multi-chip standalone cryptographic module. The module's primary purpose is to provide key generation. The module is part of the Lenel advanced access control and alarm monitoring system. The Lenel advanced access control and alarm monitoring system is built on an open architecture platform, offers unlimited scalability, database segmentation, fault tolerance, and biometrics and smart card support. The Lenel advanced access control and alarm monitoring system is fully customizable, and can be seamlessly integrated into the OnGuard total security solution.

The physical cryptographic boundary of the two validated modules is defined as the outer perimeter of the general purpose computing platform (GPC) running Windows Server 2003 SP 1 Windows Server 2008 R2 or Windows 7 on which the software only module executes.

The logical cryptographic module encompasses the following runtime components:

- Microsoft Enhanced Cryptographic Provider RSAENH.DLL. This is a previously validated FIPS 140-2 module (Cert. #382, 1330 and #1337)
- Mercury SCPD_NET.DLL

The FIPS 140-2 Configurations tested:

Operating Environment	Communication Server	RSAENH.dll	Mercury scpd_net.dll
Windows Server 2003 SP 1	SW: v2.1	Reference: CMVP Cert. #382	Version: 4.5.1.70
Windows 7		Reference: CMVP Cert. #1330	
Windows Server 2008 R2		Reference: CMVP Cert. #1337	

Table 1 - Module Configurations

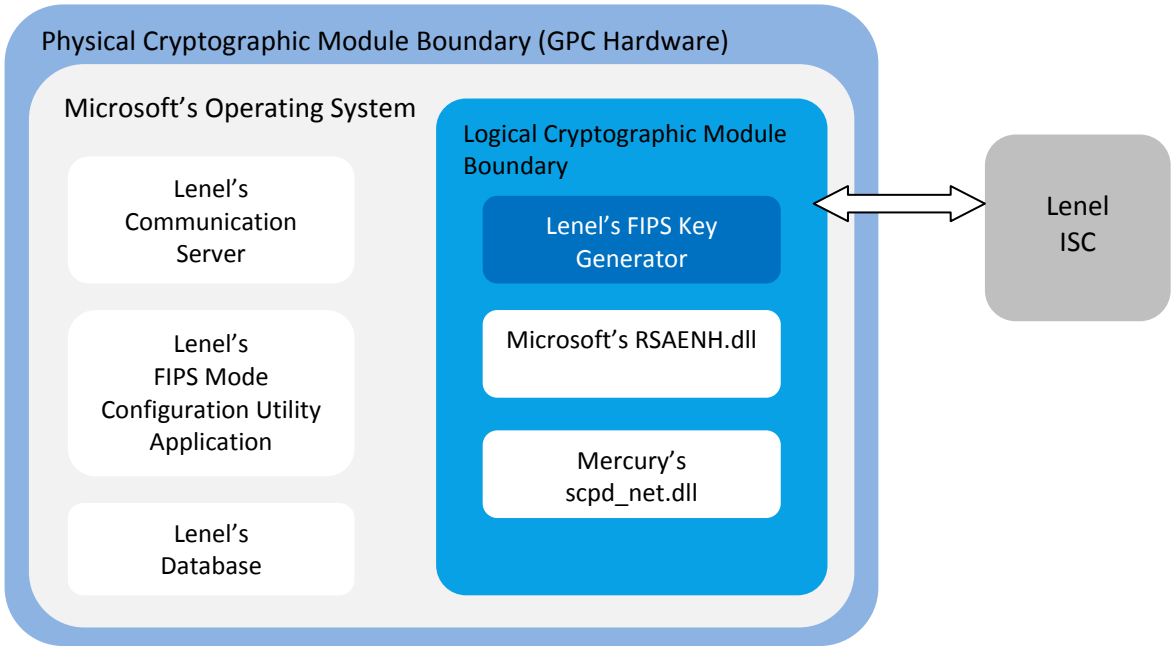

Figure 1 – Cryptographic Module Diagram

2. Security Level

The cryptographic module meets the same overall requirements applicable to Level 1 security of FIPS 140-2.

Table 2 - Module Security Level Specification

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

3. Modes of Operation

3.1 FIPS Approved Mode of Operation

The Lenel FIPS Key Generator always operates in the Approved mode of operation. The cryptographic module supports the following algorithms:

- AES CBC with 128-bit keys for encryption using Scpd_net.dll (AES Certificate #327 or #1650).
- RNG based on ANSI X9.31 Appendix A.2.4 using the AES algorithm (RNG Certificate #149 or #882)

The following algorithms are provided by RSAENH.DLL validated to FIPS 140-2 under Cert. #382, #1330 or #1337.

- RSA
- SHA-1
- RNG

3.2 Non-Approved Algorithms

The cryptographic module does not implement non-Approved cryptographic algorithms.

4. Ports and Interfaces

The logical and physical ports and interfaces of the two separate Lenel FIPS 140-2 validated cryptographic modules are summarized in the following table:

Table 3 – Ports and Interfaces

Interface	Logical	Physical
Data Input	GUI interface	Keyboard & mouse
Data Output	GPC disk	GPC disk
Control Input	GUI interface	Keyboard & mouse
Status Output	GUI interface	GPC Display
Power Input	N/A	PC power supply

5. Identification and Authentication Policy

5.1 Assumption of Roles

No authentication of identity is required in Level 1 cryptographic modules. Assumption of roles is implied by the selection of services.

Services provided by the two separate Lenel FIPS 140-2 validated cryptographic modules are as

follows.

Crypto-Officer Role: This role is assumed to provide the operator key management capabilities. The Crypto-Officer role is assumed by the selection of the following services:

- Key Generation
- Key Output Service
- Zeroize

User Role: This role is assumed to provide the operator access to status information, self-tests and zeroization service. The user role is assumed by the selection of the following services:

- Show Status
- Self-Tests
- Zeroize

The FIPS Key Generator module does not support a maintenance role.

6. Access Control Policy

6.1 Roles and Services

The cryptographic modules support the following services:

- **Show Status**: This service provides the current status of the cryptographic module.
- **Self-tests**: This service executes the suite of self-tests required by FIPS 140-2.
- **Zeroize**: This service zeroizes plaintext critical security parameters.
  - Master Keys:
    - Zeroizes its own RAM working copy of master keys (only one can be resident in the FIPS Key Generator module's RAM at any given time).
  - Seed Key and Seed Value:
    - Zeroizes its own RAM working copy of its own Seed Key and Seed Value.
- **Key Generation**: This service provides a means for master keys to be generated.
- **Key Output Service**: This service provides a means for master keys to be output.
  - Master Keys: Generates master keys and then outputs key to be distributed manually to external Lenel ISCs. Master Key 1 is output in plaintext which is allowed for Level 1, Manual Distribution/Manual Output as per FIPS 140-2 IG 7.7.

6.2 Service Inputs and Outputs

Table 4 - Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output

Service	Control Input	Data Input	Data Output	Status Output
Show Status	N/A	N/A	Status	Status
Self-tests	N/A	N/A	N/A	Success/Fail
Zeroize	Command Header info.	N/A	N/A	Success/Fail
Key Generation	Command Header info.	N/A	N/A	Success/Fail
Key Output	Command Header info.	Name of Destination file	Key	Success/Fail

6.3 Definition of Critical Security Parameters (CSPs)

Note that "*Table 6 – CSP Access Rights within Roles & Services*" below will identify which of the two separate Lenel FIPS 140-2 cryptographic modules (FIPS Key Generator, Communication Server) uses each of the following CSPs:

- Master Keys – Keys generated by the module.
- Seed Key for Mercury DRNG within the Mercury SCPD_NET.DLL. This seed value is used for generating random numbers:
- Seed Value for Mercury DRNG within the Mercury SCPD_NET.DLL. This seed value is used for generating random numbers:

Definition of Public Keys:

The following public key is contained in the cryptographic module.

- RSA Software Signing Public Key 1024 bits: This key is the RSA public key that the modules use to validate software integrity during their individual power-on self-tests.

6.4 Definition of CSPs Modes of Access

Table 6 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

Table 5 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation Generate = G, Output= O, Read = R, Zeroize = Z		
Crypto-Officer	User		Master Keys	Seed Key	Seed Value
	X	Show Status			

Role		Service	Cryptographic Keys and CSPs Access Operation Generate = G, Output= O, Read = R, Zeroize = Z		
Crypto-Officer	**User**		**Master Keys**	**Seed Key**	**Seed Value**
	X	Self-Tests			
X	X	Zeroize	Z (RAM)	Z (RAM)	Z (RAM)
X		Key Generation	G	R	R
X		Key Output Service	O		

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are applicable because the cryptographic module contains a modifiable operational environment. The following operating systems were used during the FIPS 140-2 operational testing:

- Windows Server 2003 SP1
- Windows Server 2008 R2
- Windows 7

In addition, per FIPS 140-2 Implementation Guidance G.5,

a. the source code of the two software cryptographic modules does not require modification prior to recompilation to allow porting to the following compatible single user operating systems: Windows 2000 SP4, and Windows XP SP2, and

8. Security Rules

The design of the cryptographic module corresponds to the following security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of FIPS 140-2 Level 1.

1. The cryptographic modules provide two distinct operator roles. These are the User role and the Cryptographic-Officer role. Applies to:
2. The modules do not support operator authentication. Applies to:
3. Self-tests:
    a. Power up Self-Tests:
        i. AES Known Answer Test (KAT). Performed inside the Mercury DLL (scpd_net.dll) which is dynamically linked in by the FIPS Key Generator.

ii. ANSI x9.31 RNG Known Answer Test. Performed inside the Mercury DLL (scpd_neet.dll) which is dynamically linked in by the FIPS Key Generator.

iii. The following power up Cryptographic algorithm tests are performed inside the Microsoft Enhanced Cryptographic Provider DLL (RSAENH.DLL with FIPS 140-2 Certs. #382, #1330, and #1337) which is dynamically linked in by the FIPS Key Generator:

1. RSA Sign/Verify with SHA-1.
2. DRNG

iv. Software Integrity Test:

1. Using the Microsoft Enhanced Cryptographic Provider (RSAENH with FIPS 140-2 Certs. #382, #1330, and #1337), verify RSA signatures with SHA-1 file hashes on all executable files within the FIPS Key Generator's logical boundary.

b. Critical Functions Tests: Not Applicable

c. Conditional Self-Tests

i. Continuous Random Number Generator (RNG) tests:

1. Mercury DLL (scpd_net.dll) ANSI x9.31 RNG:

a. Test performed inside the FIPS Key Generator (KeyGenerator.exe) after it receives a random number from the Mercury DLL.

b. Microsoft DLL (RSAENH.DLL) DRNG test performed inside the Microsoft Enhanced Cryptographic Provider DLL.

4. At any time the two separate cryptographic modules are in an idle state, the operator shall be capable of commanding the modules to perform their power-up self-tests, this is done by restarting the modules.
5. Data output shall be inhibited during self-tests and error states.
6. Logical disconnection of the output data path is implemented as follows:
7. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. The module shall operate on a GPC using the specified single user mode of the operating system specified on the validation certificate, or another compatible single user operating system.
9. Secure Delivery: Module software is shipped on CD via reputable courier services. The Cryptographic Officer must inspect the courier delivery to make sure the delivered package has not been tampered with or damaged.

9. Physical Security Policy

9.1 Physical Security Mechanisms

The two cryptographic module is a software only cryptographic module, and as such the physical security requirements of FIPS 140-2 are not applicable.

9.2 Operator Required Actions

The operator is not required to perform any special actions for inspection, since the physical security requirements are not applicable.

Table 6 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
N/A	N/A	N/A

10. Mitigation of Other Attacks Policy

The two cryptographic modules have not been designed to mitigate specific attacks outside of the scope of FIPS 140-2.

Table 7 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

12. References

The Lenel Systems International, Inc. website: http://www.lenel.com

FIPS PUB 140-2, Security Requirements for Cryptographic Modules.

FIPS PUB 197, Advanced Encryption Standard (AES)

Windows Server 2003 Enhanced Cryptographic Provider (RSAENH) Security Policy

Windows 7 Enhanced Cryptographic Provider (RSAENH) Security Policy

Windows Server 2008 R2 Enhanced Cryptographic Provider (RSAENH) Security Policy

13. Definitions and Acronyms

AES – Advanced Encryption Standard.

ISC – Intelligent System Controller.

CBC – Cipher Block Chaining.

CSP – Critical Security Parameters.

DRNG – Deterministic Random Number Generator.

EMI – Electromagnetic Interference.

FIPS – Federal Information Processing Standards.

Lenel FIPS Mode Configuration Utility Application – A Lenel GUI application used to place the Communication Server module configuration data in the Windows Registry. Note that the Lenel FIPS Mode Configuration Utility is not a FIPS module

NIST – National Institute of Standards and Technology.

SHA-1 – Secure Hash Algorithm revision 1.