Lenel OnGuard Access Control

Communication Server

Security Policy

Document *Version 1.6*

Lenel Systems International, Inc.
www.lenel.com

October 1, 2013

Revision History

Revision History			
Version	***Date***	***Author***	***Notes***
1.1	8-15-2011	R Pethick	Updates from initial revision 1.0 adding newer versions of OnGuard.
1.2	12-30-2011	R Pethick	Updated 6.1 Roles and Services and Table 4 in Section 6.2
1.3	01-09-2013	R. Martinez	Updated OG versions (TITAN & COBRA), corrected pg # for 6.4; cert # for WIN 2008, pg 4
1.4	07-09-2013	R. Martinez	General updates after input from NIST during listing of COBRA.
1.5	7/31/13	R .Martinez	Input from NIST. Added “encrypt & decrypt” to 8.4.A.a.i
1.6	10/01/13	R. Martinez	Added Dell Models per NIST request to Table 1

TABLE OF CONTENTS

1. Module Overview

The Lenel OnGuard Access Control "Communication Server" cryptographic module is a software only multi-chip standalone cryptographic module. The Communication Server module's primary purpose is to provide secure communications with external access control devices. 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 is defined as the outer perimeter of the general purpose computing platform (GPC) running Windows Server 2008 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. #1330 and #1010)
- Mercury SCPD_NET.DLL

The FIPS 140-2 Configurations tested:

Operating Environment	Communication Server	RSAENH.dll	Mercury scpd_net.dll
Dell OptiPlex 755 Windows 7 Intel Core2 Q6600	Software Version: • 6.5.624 • 6.6.287	Reference: CMVP Cert. #1330	Version: 4.5.1.103
Dell OptiPlex 760 Windows Server 2008 Intel Core2 E8400		Reference: CMVP Cert. #1010	

Table 1 - Module Configurations

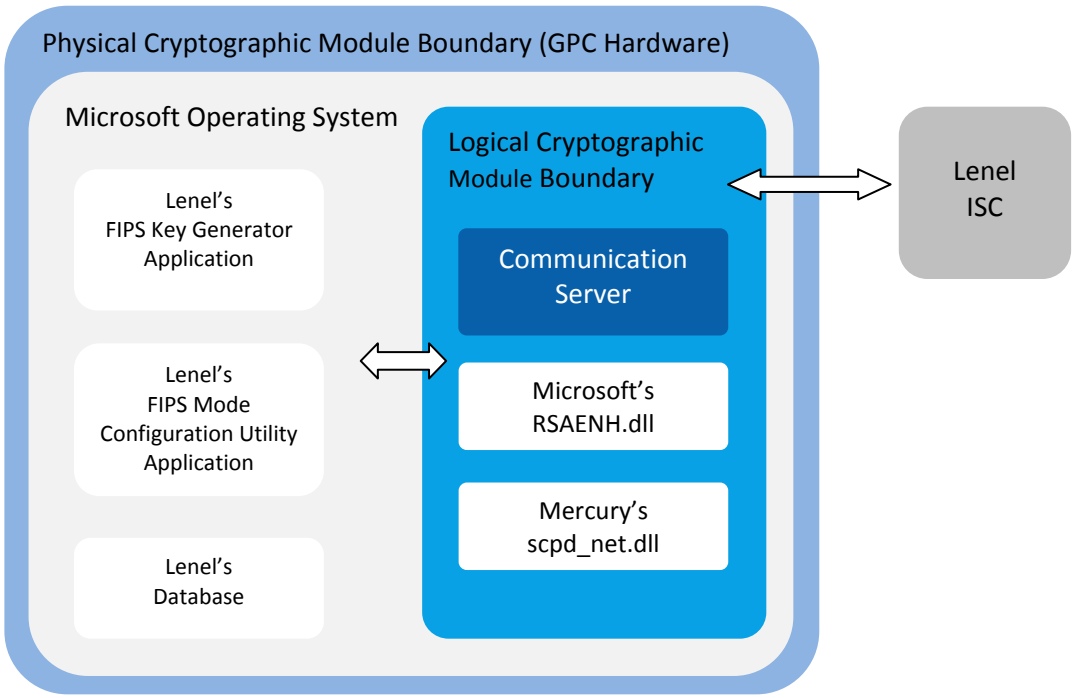

Figure 1 – Cryptographic Module Diagram

2. Security Level

The Lenel OnGuard Access Control cryptographic module meets the 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

In FIPS mode, the cryptographic module supports or uses the following algorithms:

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

The following algorithms are provided by RSAENH.DLL validated to FIPS 140-2 under Cert. #1330 or #1010.

- FIPS 140-2 Cert. #1330
  - RSA Cert. #557
  - SHA Cert. #1081
  - RNG (SP 800-90, vendor affirmed)

- FIPS 140-2 Cert. #1010
  - RSA Cert. #355
  - SHA Cert. #753

The cryptographic module may be configured for FIPS mode via execution of the "FIPS Mode Configuration Utility" and turning its "Enable FIPS Mode" checkbox ON. The operator can determine if the cryptographic module is running in FIPS vs. non-FIPS mode via execution of the "FIPS Mode Configuration Utility". When running this utility it will indicate if FIPS mode is enabled or disabled. If it is disabled you can invoke FIPS mode by selecting Modify and turning on FIPS Mode. You will also need to select which key is the active key as well as provide the master key. Once this is done the Lenel Communication Server service will need to be restarted to use the new settings.

3.2 Non-Approved Algorithms

The Lenel Communication Server uses the RC2 algorithm for encrypting and decrypting data from the database. This data is treated as plain text as far as this module is concerned.

4. Ports and Interfaces

The logical and physical ports and interfaces are summarized in the following table:

Table 3 – Ports and Interfaces

Interface	Logical	Physical
Data Input	Data that is received from the Intelligent System Controller by the Lenel Communication Server. Configuration information received via remote procedure calls (RPC). COM interface calls from non Lenel ISCs. Data read from the database by the Communication Server.	Ethernet, serial port, modem, Remote Procedure Calls, COM interfaces, Reading from Database
Data Output	Data that is sent from the Lenel Communication Server to the Intelligent System Controller. Data returned via remote procedure calls (RPC). Data sent to non Lenel ISCs via COM interfaces. Data written to the database.	Ethernet, serial port, modem, Remote Procedure Calls, COM interfaces, Writing to database
Control Input	Data entered into the FIPS Mode Configuration Utility	Keyboard, mouse
Status Output	All messages either logged to error logs or displayed in the Alarm Monitoring Interface. Events and status messages sent to client applications.	Hard disk, Monitor, Socket connection to client applications
Power Input	N/A	PC power supply

5. Identification and Authentication Policy

5.1 Assumption of Roles

No authentication is required. Assumption of roles is implied by the selection of service.

- Crypto Officer (CO) Role: This role is assumed to provide the operator key management and alternating bypass control as well as key generation. The CO role is assumed by the selection of a CO allocated service.

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

The module does not support a maintenance role.

6. Access Control Policy

6.1 Roles and Services

The cryptographic module supports the following services:

Crypto Officer Role Services:

- **Module Master Key Management**: This service allows the master keys to be entered as well as to indicate which key is the active key.
- **Alternating Bypass Enable/Disable**: This service allows encryption of data to be enabled or disabled to a particular ISC.
- **Zeroize**: This service provides a means to overwrite all temporary copies of cryptographic modules plaintext critical security parameters
- **Configure FIPS mode of Operation**: sets the parameter for the FIPS mode of Operation.

User Role services:

- **Secure Data Transmission**: This service provides AES encryption/decryption operations for secure transmission of data. (NOTE: During each session a fresh session key is generated by the CM via an Approved RNG and is electronically output to the ISC encrypted with AES).
- **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.
- **Remote Procedure Call Service:** This service provides a means for client applications to communicate with the Communication Server.
- **COM Interface Method Service:** This service provides a means for the Communication Server to interact with device translators via COM method interfaces.
- **Database Interaction Service:** This service provides interaction with the database from the Communication Server.

6.2 Service Inputs and Outputs

Table 4 - Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
Module Master Key Management	Header info.	None	None	Success/Fail

Alternating Bypass Enable/Disable	Header info.	None	None	Success/Fail
Secure Data Transmission (Encryption)	Header info.	Plaintext data	Ciphertext data	Success/Fail
Secure Data Transmission (Decryption)		Ciphertext data	Plaintext data	Success/Fail
Show Status	Service Selection	None	Status	Success/Fail
Self-tests		None	None	Success/Fail
Zeroize	Service Selection	None	None	Success/Fail
Remote Procedure Call		None	Plaintext	Plaintext
COM Interface Method		None	Plaintext	Plaintext
Database Interaction		None	Plaintext	Plaintext

6.3 Definition of Critical Security Parameters (CSPs)

- Master Key 1 – This key is used to provide encryption of session keys.
- Master Key 2 – This key is used to provide encryption of session keys.
- Session Key – This key is used to encrypt data communication between the module and the ISC.
- Seed Key for Mercury RNG within the Mercury SCPD_NET.DLL – This seed key is used for generating random numbers.
- Seed Value for Mercury RNG within the Mercury SCPD_NET.DLL – This seed value is used for generating random numbers.

Definition of Public Keys:

The following are the public keys contained in the module:

- RSA Software Public Key - 1024 bits: This key is the RSA public key that is used to validate the software integrity.

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:

- Generate: the parameter is generated.
- Enter: the parameter is input into the cryptographic boundary.
- Output: the parameter is output from the cryptographic boundary.
- Read: the parameter is used within its corresponding security function.
- Zeroize: the parameter is actively overwritten.

Role		Service	Cryptographic Keys and CSPs Access Operation Enter = E, Generate = G, Output= O, Read = R, Zeroize = Z				
CO	User		Master Key1	Master Key 2	Session Key	Seed Key (M)	Seed Value (M)
X		Module Master Key Management	E,O,R, Z	E,O,R, Z			
X		Alternating Bypass Enable/Disable					
	X	Secure Data Transmission	R	R	G,O,R	G	G
	X	Show Status					
	X	Self-Tests	R	R			
X		Zeroize	Z	Z	Z	Z	Z
	X	Remote Procedure Call					
	X	COM Interface Method					
	X	Database Interaction					

Table 5 – CSP Access Rights within Roles & Services

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 2008
- Windows 7

8. Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules for the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module shall provide two distinct operator roles. These are the User role, and the Cryptographic-Officer role.
2. The module does not support operator authentication.
3. The cryptographic module shall encrypt message traffic using the AES algorithm.
4. The cryptographic module shall perform FIPS 140-2 required self-tests
    A. Power up Self-Tests:
        a. Cryptographic Algorithm Tests:
            i. AES (encrypt and decrypt) Known Answer Tests (KATs).
            ii. ANSI x9.31 RNG Known Answer Test.
        b. Software Integrity Test
            i. RSA 1024 with SHA-1 signature verification.
        c. Critical Functions Tests: Configuration Parameter Integrity test
    B. Conditional Self-Tests:
        a. Continuous Random Number Generator (RNG) test:
            i. ANSI x9.31 RNG
        b. Alternating bypass test
5. At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-tests, this is done by restarting the individual application.
6. Data output shall be inhibited during self-tests and error states. The module is logically disconnected from data output during key zeroization and key generation processes.
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 a single user configuration of the operating system specified on the validation certificate, or another compatible single user operating system.

9. Physical Security Policy

9.1 Physical Security Mechanisms

The 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 cryptographic module has 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

11. References

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

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

Windows 7 Enhanced Cryptographic Provider (RSAENH) Security Policy

Windows Server 2008 Enhanced Cryptographic Provider (RSAENH) Security Policy

12. Definitions and Acronyms

AES – Advanced Encryption Standard.

ISC – Intelligent System Controller.

CBC – Cipher Block Chaining.

CSP – Critical Security Parameters.

RNG –Random Number Generator.

EMI – Electromagnetic Interference.

FIPS – Federal Information Processing Standards.

GPC – General Purpose Computer.

NIST – National Institute of Standards and Technology.

SHA – Secure Hash Algorithm