Lenel OnGuard Access Control Cryptographic Module

Non-Proprietary Security Policy

Document *Version 4.2*

UTC Fire & Security Americas Corporation, Inc.

www.lenel.com

November 14, 2019

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
1.7	05/02/2014	M. Obrien	Added OnGuard Version 7.0.8xx for Windows 8 and Windows Server 2012
1.8	8/14/2014	R. Pethick	Updated version, Company Logo and boundaries diagram
1.9	10/31/2014	M. Obrien	Added certs for new Operating Environments.
2.0	08/11/2015	M. Obrien	Changed legal entity name from Lenel to UTC Fire & Security Americas Corporation, Inc.
2.1	08/12/2015	M. Obrien	Added OnGuard 7.1.481
2.2	02/02/2016	M Obrien	Added OnGuard 7.2.269
2.3	05/16/2016	M Obrien	Revised Mercury SCPD version.
2.4	06/28/2016	M Obrien	Updated references to DRBG.
2.5	10/11/2016	R. Cortese	Updates sections 1, 3.1, 8 and 11 to indicate changes to use Microsoft BCRYPTPRIMITIVES.DLL.

			Added comments from Brandon in the 9/14 review doc
2.6	10/21/2016	R. Cortese	Accepted comments and changes from previous revisions. Updated section 1 to indicate the CMVP certs we will be using regarding BCRYPT Updated section 3.1 regarding FIPS mode of operation and supported algorithm certs Responded to comment in section 3.2 Updated section 6.4 – removed seed key and responded to comment from Brandon Updated section 7 with the desired operational environments Updated section 8 with comments and updates from Brandon Updated section 11 with comment from Brandon
2.7	10/28/2016	R. Cortese	Accepted all previous tracked changes. Removed signature generation from section 8 power up self-tests
2.8	11/2/2016	R. Cortese	Renamed document to indicate more general Lenel crypto module Updated file format to be .docx Updated Module Overview to indicate additional modules included in the logical boundary Updated Figure 1 Module Diagram Added section 3.3 Non-Approved but Allowed Algorithms Added several comments and responses in section 8
2.9	02/03/2017	M. OBrien	Updated to note use of SHA-256. Version of OnGuard updated to 7.3.345.100
3.0	3/27/2019	K. Kolakowski L. Zawlocki	Version of OnGuard updated to 7.4 Update 1 Release. Adding TLS protocol related information.
4.0	9/20/2019	K. Kolakowski	Version of OnGuard updated to 7.5 Release.

		L. Zawlocki	
4.1	10/29/2019	M. O'Brien	Minor updates in Section 3.3
4.2	11/xx/2019	M. O'Brien	Minor updates to Table 1 and Section 7

TABLE OF CONTENTS

REVISION HISTORY **2**

1. MODULE OVERVIEW **5**

2. SECURITY LEVEL **6**

3. MODES OF OPERATION **7**

3.1 FIPS APPROVED MODE OF OPERATION 7
3.2 NON-APPROVED ALGORITHMS ONLY USED IN THE NON-APPROVED MODE 10
3.3 NON-APPROVED BUT ALLOWED ALGORITHMS 10

4. PORTS AND INTERFACES **11**

5. IDENTIFICATION AND AUTHENTICATION POLICY **12**

6. ACCESS CONTROL POLICY **12**

6.1 ROLES AND SERVICES 12
6.2 SERVICE INPUTS AND OUTPUTS 13
6.3 DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) 15
6.4 DEFINITION OF CSPS MODES OF ACCESS 15

7. OPERATIONAL ENVIRONMENT **16**

8. SECURITY RULES **17**

9. PHYSICAL SECURITY POLICY **18**

9.1 PHYSICAL SECURITY MECHANISMS 18
9.2 OPERATOR REQUIRED ACTIONS 18

10. MITIGATION OF OTHER ATTACKS POLICY **19**

11. MULTIPLE APPROVED MODES **19**

12. REFERENCES **21**

13. DEFINITIONS AND ACRONYMS **21**

1. Module Overview

The Lenel OnGuard Access Control Cryptographic Module is a software only multi-chip standalone cryptographic module. The components of the module include the Lenel "Communication Server", "FIPS Mode Configuration Utility" and the "FIPS Key Generator". 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 Microsoft Windows 10 or Microsoft Windows Server 2016 on which the software only module executes.

The logical cryptographic module encompasses the following runtime components:

- Lenel Communication Server
- FIPS Mode Configuration Utility
- FIPS Key Generator
- Microsoft Cryptographic Primitives Library BCRYPTPRIMITIVES.DLL, configured into FIPS Mode. These are previously validated FIPS 140-2 modules (CMVP Certs. #2606 and #2937)
- Mercury SCPD_NET.DLL

The FIPS 140-2 Configurations tested:

Table 1 - Module Configurations

Operational Environment	Lenel OnGuard	BCRYPTPRIMITIVES.dll	Mercury scpd_net.dll
Microsoft Windows 10 64-bit running on Precision Workstation T3500 with an Intel Xeon W3670	7.4.457.69 with Critical On-Demand Hot Fix for DE40714[1] or 7.5.375.1	**CMVP Cert #2606**	**4.6.1.244** **DLL_AES_VER =1.0.0.1**
Microsoft Windows Server 2016 64-bit running on Precision Workstation T3500 with an Intel Xeon W3530	7.4.457.69 with Critical On-Demand Hot Fix for DE40714[1] or 7.5.375.1	**CMVP Cert. #2937**	**4.6.1.244** **DLL_AES_VER =1.0.0.1**

[1] DE40714 is reference to a defect "TLS encryption cannot be used when FIPS Mode encryption is enabled."

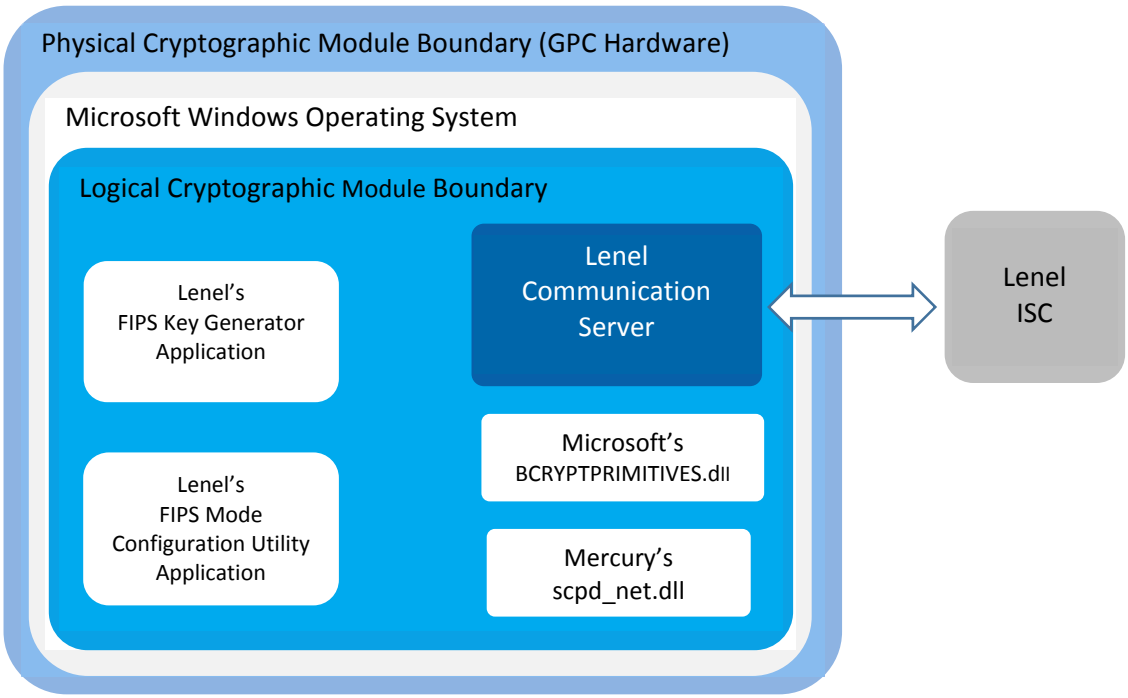

Figure 1 – Cryptographic Module Diagram

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	1
Self-Tests	1

Security Requirements Section	Level
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, CBC and KW with 128-bit keys for encryption using Scpd_net.dll (AES Cert. #C500).

In addition to the above, the cryptographic module also uses algorithms provided by BCRYPTPRIMITIVES.DLL validated to FIPS 140-2 under CMVP Certs. #2606 and #2937, as shown in the following table. Note that BCRYPTPRIMITIVES.DLL is a library in which several algorithms and algorithm modes of operation have been tested, but are not utilized in this module. Only algorithms and modes of operation that are utilized are listed below.

Table 3 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
Algorithms Used by SCPD_NET.DLL		
AES	[FIPS 197, SP 800-38A] Functions: encrypt, decrypt Modes: ECB, CBC Key sizes: 128 bits	C500
AES	[SP 800-38F] Functions: encrypt, decrypt Modes: KW Key sizes: 128 bits	C500
KTS	[SP 800-38F] Functions: authenticated encrypt, authenticated decrypt Mode: KW Key sizes: 128 bits	C500
Algorithms Used by BCRYPTPRIMITIVES.DLL		
AES	[FIPS 197, SP 800-38A] Mode: CBC Key sizes: 128, 256 bits	3497 or 4064

Algorithm	Description	Cert #
CKG	[SP 800-133] Section 7.1: direct symmetric key generation using unmodified DRBG output	Vendor Affirmed
CVL: TLS KDF	[SP 800-135] Mode: TLS	575 or 886
DRBG	[SP 800-90A] Function: generation Mode: CTR DRBG Security Strength: 256 bits	868 or 1217
HMAC	[SP 800-38D] Function: message authentication SHA sizes: SHA-1, SHA-256, SHA-384, SHA-512 *Note: SHA-512 is only implemented to self-test SHA-384	2233 or 2651
RSA	[FIPS 186-4, PKCS1 v1.5] Function: signature verification with SHA-256, SHA-384 file hash Key sizes: 2048, 3072	1783 or 2193
RSA	[FIPS 186-4, PKCS1 v1.5] Function: signature verification with SHA-256, SHA-384 file hash Key sizes: 4096	Approved per IG A.14 1783 or 2193
SHS	[FIPS 180-4] SHA Sizes: SHA-1, SHA-256, SHA-384, SHA-512 *Note: SHA-512 is only implemented to self-test SHA-384	2886 or 3347

The cryptographic module may be configured to FIPS mode by turning the “Enable FIPS Mode” checkbox to ON** in the FIPS Mode Configuration Utility and ensuring an appropriate FW version is running on the connected ISC(s). An appropriate FW version would be-1.20.5 (442) or higher for LNL-4420, LNL-X2210, LNL-X2220, LNL-X3300, LNL-X4420 ISCs. Also note that LNL-X2210, LNL-X2220, LNL-X3300 and LNL-X4420 are not supported on OnGuard version 7.4.457.69, only 7.5.375.1. No other ISCs are supported for use in the FIPS Approved mode.

The FIPS Mode Configuration Utility will indicate if it has been configured for FIPS mode. You can change the module’s configuration to an Approved or non-Approved Mode by selecting “Modify” in the FIPS Mode Configuration Utility and changing the FIPS Mode checkbox selection; once this is done the Lenel Communication Server service will need to be restarted to use the new settings. Whenever switching modes, an operator must first ensure all keys/ CSPs are zeroized and/ or replaced.

When configuring TLS mode both the Mercury panel and its OnGuard setting have to match. The panel needs to expect TLS connection. Otherwise, it will connect via AES without TLS. The

TLS option is set on the panel; it's the only way to connect to it. The OnGuard settings must match that – thus the Panel options need to have their checkbox "TLS Encryption" set in order for the FIPS mode with TLS to work.

There are multiple Approved Modes. The FIPS Key Generator, FIPS Mode Configuration Utility and Communication Server are independent applications that each run their own set of self-tests. When configured as described above and the security rules described in Section 8 of this Security Policy are adhered to, the FIPS Approved Mode shall exist whenever any combination of the FIPS Key Generator, FIPS Mode Configuration Utility and/or the Communication Server applications are running.

** Note: If the panel is configured to expect "TLS mode" – OnGuard will not establish a connection if the settings in OnGuard don't match the settings in the panel. In order to work in TLS mode, both the panel and OnGuard panel need to have TLS options enabled.

3.2 Non-Approved Algorithms Only Used in the Non-Approved Mode

When connected to ISCs with legacy FW versions loaded into them (older than what has been specified in Section 3.1 above), the module will utilize AES key wrapping for key transport. If the module is connected to an EP series ISC other than the LNL-4420, LNL-X2210, LNL-X2220, LNL-X3300 or LNL-X4420 RSA-1024 signature verification and key encapsulation is used.

3.3 Non-Approved but Allowed Algorithms

- The Lenel Communication Server uses the RC2 (no security claimed) algorithm for encrypting and decrypting data from the database. This data is treated as plain text as far as this module is concerned. Per IG 1.23, no security is claimed.
- RSA key encapsulation non-compliant with SP 800-56B, allowed per IG D.9. Provides between 112 and 150 bits of encryption strength.
- NDRNG; implemented by CNG.SYS, a BRCRYPTPRIMITIVES.dll dependency available in the Approved mode configuration; provides at least 256 bits of entropy.

Table 4 – Security Relevant Protocols* Used in FIPS Mode

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
TLS [IG D.8 and SP 800-135	TLS_RSA_WITH_AES_128_CBC_SHA			TLS v1.1, v1.2**
	RSA	RSA	AES-CBC-128	HMAC-SHA-1
	TLS_RSA_WITH_AES_128_CBC_SHA256			TLS v1.2**
	RSA	RSA	AES-CBC-128	HMAC-SHA-256
	TLS_RSA_WITH_AES_128_CBC_SHA384			TLS v1.2**
	RSA	RSA	AES-CBC-128	HMAC-SHA-384
	TLS_RSA_WITH_AES_256_CBC_SHA			TLS v1.1, v1.2**
	RSA	RSA	AES-CBC-256	HMAC-SHA-1
	TLS_RSA_WITH_AES_256_CBC_SHA256			TLS v1.2**

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
	RSA	RSA	AES-CBC-256	HMAC-SHA-256
	TLS_RSA_WITH_AES_256_CBC_SHA384			TLS v1.2**
	RSA	RSA	AES-CBC-256	HMAC-SHA-384

* No parts of these protocols, other than the KDFs, have been tested by the CAVP and CMVP

** EP series controllers will support only TLS v1.1, except for LNL-4420 and X series controllers - LNL-X2210, LNL-X2220, LNL-X3300, LNL-X4420 which support TLS 1.2.

4. Ports and Interfaces

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

Table 5 – 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. This service is applicable both for AES and TLS encryption.
- **Zeroize**: This service provides a means to overwrite all temporary copies of cryptographic modules plaintext critical security parameters. This operation is performed both in RAM as well as in the registry of the workstation where the CSPs are stored.
- **Configure FIPS Mode of Operation**: This sets the parameter for the FIPS mode of Operation.
- **Key Generation**: This service allows for encryption keys to be generated using a FIPS Approved SP 800-90A DRBG. The keys can be exported to a file or visually copied from the computer display after two independent, internal actions are performed.
- **TLS Certificate Installation**: This role provides proper certificate installation & registration on the OnGuard machines. These certificates correspond with the Master CA mercury certificates already present on the Access Panels.
- **Setting TLS mode**: The Crypto-Officer will toggle if the TLS connection option is either set “on” or “off” for a single Panel. If the panel is configured to TLS but the option is set to “no” – communication will not be established.

User Role services:

- **Secure Data Transmission**: This service provides AES encryption/decryption operations for secure transmission of data. During each session, a fresh Session Key is generated by the cryptographic module via an Approved DRBG and is electronically output to the ISC encrypted with AES.

  NOTE: KTS (AES-KW mode) will be used in the Approved mode, however non-Approved AES key wrapping may be used in the non-Approved mode.

- **TLS Data Transmission**: When TLS is enabled, data is transmitted over a TLS session in place of the Secure Data Transmission service described above.

  NOTE: RSA-2048 or greater is used in the Approved mode, however RSA-1024 is used in the non-Approved mode.

- **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 6 – 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
Zeroize	Service Selection	None	None	Success/Fail
Configure FIPS Mode of	Service Selection	None	None	Success/Fail

Service	Control Input	Data Input	Data Output	Status Output
Operation				
Key Generation	Service Selection	None	Plaintext data	Success/Fail
TLS Certificate Installation	None	Plaintext data	None	Success/Fail
Setting TLS Mode	Service Selection	None	None	Success/Fail
Secure Data Transmission (Encryption)	Header info.	Plaintext data	Ciphertext data	Success/Fail
Secure Data Transmission (Decryption)	None	Ciphertext data	Plaintext data	Success/Fail
TLS Data Transmission (Encryption)	Header info.	Plaintext data	Ciphertext data	Success/Fail
TLS Data Transmission (Decryption)	None	Ciphertext data	Plaintext data	Success/Fail
Show Status	Service Selection	None	Status	Success/Fail
Self-tests	None	None	None	Success/Fail
Remote Procedure Call	None	None	Plaintext	Plaintext
COM Interface Method	None	None	Plaintext	Plaintext
Database Interaction	None	None	Plaintext	Plaintext

6.3 Definition of Critical Security Parameters (CSPs)

- **Master Key 1** – This AES-KW 128 bit key is used to provide encryption of session keys.
- **Master Key 2** – This AES-KW 128 bit key is used to provide encryption of session keys.
- **Session Key** – This AES-128 bit key is used to encrypt data communication between the module and the ISC.
- **DRBG Seed** – This seed value (384 bits) is used for generating random numbers.
- **DRBG State** – Key (256 bits) and V (128 bits) values of the SP 800-90A DRBG
- **TLS Pre-Master Secret** – 384 bit secret key material
- **TLS Master Secret** – 384 bit secret key material
- **TLS Session Encryption Key** – AES-128/ 256 CBC session encryption keys
- **TLS HMAC Key** – HMAC SHA-1 (160 bit), HMAC SHA-256 (256-bit) or HMAC SHA-384 (384-bit) TLS session authentication keys

Definition of Public Keys:

The following are the public keys contained in the module:

- **RSA Software Public Key** – RSA 2048 bit public key that is embedded in the module and used to validate the software integrity.
- **TLS CA-Pub** – RSA 4096 bit public key owned by the Mercury CA.
- **TLS Host-Pub** – RSA 2048/ 3072/ 4096 bit public key owned by controllers the OnGuard communicates with.

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.

Table 7 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation Enter = E, Generate = G, Output= O, Read = R, Zeroize = Z											
CO	User		Master Key 1	Master Key 2	Session Key	DRBG SeedDRSeed	DRBG StateDRBG State	TLS Pre-Master Secret	TLS Master Secret	TLS Session Encryption Key	TLS HMAC Key	RSA Software Signing Public Key	TLS CA-Pub	TLS Host-Pub
X		Module Master Key Management	E,O, R, Z	E,O, R, Z	-	-	-	-	-	-	-	-	-	-
X		Alternating Bypass Enable/Disable	-	-	-	-	-	-	-	-	-	-	-	-
X		Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	-	Z	Z
X		Configure FIPS Mode of Operation	-	-	-	-	-	-	-	-	-	-	-	-
X		TLS Certificate Installation	-	-	-	-	-	-	-	-	-	-	E	-
X		Setting TLS Mode	-	-	-	-	-	-	-	-	-	-	-	-
X		Key Generation	G	G	-	G	G	-	-	-	-	-	-	-
	X	Secure Data Transmission	R	R	G,O, R	-G	G	-	-	-	-	-	-	-
	X	TLS Data Transmission	-	-	-	G	G	G,O, R	G,R	G,R	G, R	-	R	E,R
	X	Show Status	-	-	-	-	-	-	-	-	-	-	-	-
	X	Self-Tests	R	R	-	-	-	-	-	-	-	R	-	-
	X	Remote Procedure Call	-	-	-	-	-	-	-	-	-	-	-	-
	X	COM Interface Method	-	-	-	-	-	-	-	-	-	-	-	-
	X	Database Interaction	-	-	-	-	-	-	-	-	-	-	-	-

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 operational environment configurations were used during the FIPS 140-2 operational testing:

- Microsoft Windows Server 2016 64-bit running on Precision Workstation T3500 with an Intel Xeon W3530
- Microsoft Windows 10 64-bit running on Precision Workstation T3500 with an Intel Xeon W3670

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. Encrypted communications between the Communication Server and the Lenel ISC will be performed using AES-KW-128 or TLS when in FIPS Mode
4. The cryptographic module shall perform FIPS 140-2 required self-tests. Self-tests marked with a '*' indicate that they are performed by BCRYPTPRIMITIVES.dll. Self-tests marked with '**' indicate they are performed by a dependency of BCRYPTPRIMITIVES.dll, available as a result of configuring it into the Approved mode.

    A. Power up Self-Tests:

        a. Cryptographic Algorithm Tests:

            i. AES ECB (encrypt and decrypt) Known Answer Test (Cert. C500)

            ii. AES CBC (encrypt and decrypt) Known Answer Test (Certs. #3497 and #4064)*

            iii. AES-256 CTR DRBG Known Answer Test with health checks (instantiate, generate and reseed) as defined in SP 800-90A section 11.3 (Certs. #868 and #1217)*

            iv. HMAC (SHA-1, SHA-256 and SHA-512) Known Answer Test (Certs. #2233 and #2651)*

            v. RSA w/ SHA-256 signature verification Known Answer Test (Certs. #1783 and #2193)*

        b. Software Integrity Test

            i. RSA 2048 with SHA-256 signature verification performed over all Lenel applications*, scpd_net.dll* and BCRYPTPRIMITIVES.dll**.

        c. Critical Functions Tests: Configuration Parameter Integrity test

B. Conditional Self-Tests:
    a. DRBG Continuous RNG test (Certs. #868 and #1217)*
    b. NDRNG Continuous RNG test**
    c. DRBG health test (Certs. #868 and #1217)*
    d. Manual key entry test
    e. 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. When switching between the Approved and non-Approved Modes of operation, master keys need to be re-generated and/or zeroized.
10. Only Lenel ISCs configured for FIPS communications shall communicate with the module while in FIPS Mode except those ISCs that have been selected for bypass.
11. If a cryptographic key is imported into the module, the key shall be generated from an SP 800-90A DRBG with a minimum of 128 bits of strength.

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.

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.

11. Multiple Approved Modes

Table 10 maps the algorithms, services and self-tests performed by each application. The certificate numbers used for the algorithms specified below are dependent on which BCRYPTPRIMITIVES.dll Cert. # is used (CMVP Certs. #2606 or #2937). Note that the one exception is that the Communication Server always uses Cert. #C500 for AES key transport.

Table 8 – Individual Application Functionality

Application	Algorithms	Services	Self-Tests
Communication Server	• AES • DRBG • SHS • RSA • KTS	• Secure Data Transmission • TLS Data Transmission • Remote Procedure Call Service • COM Interface Method Service • Database Interaction Service (non-compliant) • Zeroize • Show Status • Self-tests	**Cryptographic Algorithm Tests:** • AES encrypt/ decrypt KATs • DRBG KAT and SP 800-90A Health Checks* • SHA-256 KAT • RSA verification KAT* **Software Integrity Test:** • RSA verification with SHA-256 **Critical Functions Test:** • Configuration Parameter Integrity Test **Conditional Tests:** • DRBG CRNGT • Entropy Source CRNGT • Alternating Bypass Test
FIPS Key Generator	• DRBG • SHS	• Key Generation • Zeroize	**Cryptographic Algorithm Tests:** • DRBG KAT and SP 800-90A

Application	Algorithms	Services	Self-Tests
	• RSA	• Show Status • Self-tests	Health Checks* • SHA-256 KAT • RSA verification KAT* **<u>Software Integrity Test:</u>** • RSA verification with SHA-256 **<u>Conditional Tests:</u>** • DRBG CRNGT • Entropy Source CRNGT
FIPS Mode Configuration Utility	• SHS • RSA	• Module Master Key Management • TLS Certificate Installation • Setting TLS Mode • Alternating Bypass Enable/Disable • Configure FIPS Mode of Operation • Zeroize • Show Status • Self-tests	**<u>Cryptographic algorithm tests</u>** • SHA-256 KAT • RSA verification KAT* **<u>Software Integrity Test:</u>** • RSA verification with SHA-256 **<u>Conditional Tests:</u>** • Manual Key Entry Test

12. References

The UTC Fire & Security Americas Corporation, Inc. Lenel website: https://www.lenel.com

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

Non-proprietary Security Policy for FIPS 140-2 Validation Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows 10 for Surface Hub

Non-proprietary Security Policy for FIPS 140-2 Validation Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016

13. Definitions and Acronyms

AES – Advanced Encryption Standard.

CBC – Cipher Block Chaining.

CSP – Critical Security Parameters.

DRBG – Deterministic Random Bit Generator.

EMI – Electromagnetic Interference.

FIPS – Federal Information Processing Standards.

GPC – General Purpose Computer.

ISC – Intelligent System Controller.

NIST – National Institute of Standards and Technology.

RNG –Random Number Generator.

SHA – Secure Hash Algorithm.

TLS – Transport Layer Security