Lenel OnGuard Access Control Cryptographic Modules:

FIPS Key Generator
Communication Server

Security Policy

Document *Version 2.7*

Lenel Systems International, Inc.
www.lenel.com

January 23, 2009

Revision History

Revision History			
Version	***Date***	***Author***	***Notes***
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 Cryptographic Package (Versions 1.0 and 1.1) is comprised of two separate software only multi-chip standalone FIPS 140-2 cryptographic modules. The two separate FIPS 140-2 cryptographic modules are tightly coupled and always exist as a single bundled package.

The two separate Lenel FIPS 140-2 cryptographic modules of the Lenel OnGuard Access Control Cryptographic Package Version 1.0 are the Lenel:

- FIPS Key Generator (S/W Version 2.1)
- Communication Server (S/W Version 5.11.216 + Hot Fix 2.0.3)

The two separate Lenel FIPS 140-2 cryptographic modules of the Lenel OnGuard Access Control Cryptographic Package Version 1.1 are the Lenel:

- FIPS Key Generator (S/W Version 2.1)
- Communication Server (S/W Version 5.12.012 + Hot Fix 2.0.3)

At run-time the following modules dynamically link to the Microsoft Enhanced Cryptographic Provider RSAENH.DLL (FIPS 140-2 Cert. #382):

- FIPS Key Generator
- Communication Server

At run-time, the following modules dynamically link to the Mercury SCPD_NET.DLL (version 4.5.1.70). Mercury SCPD_NET.DLL source code has been reviewed and operationally tested as part of the following:

- FIPS Key Generator
- Communication Server

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 on which the software only modules execute.

The logical boundaries of the two cryptographic modules are as follows:

- FIPS Key Generator module:
  - FIPS Key Generator
  - Mercury SCPD_NET.DLL
- Communication Server module:
  - Communication Server
  - Mercury SCPD_NET.DLL

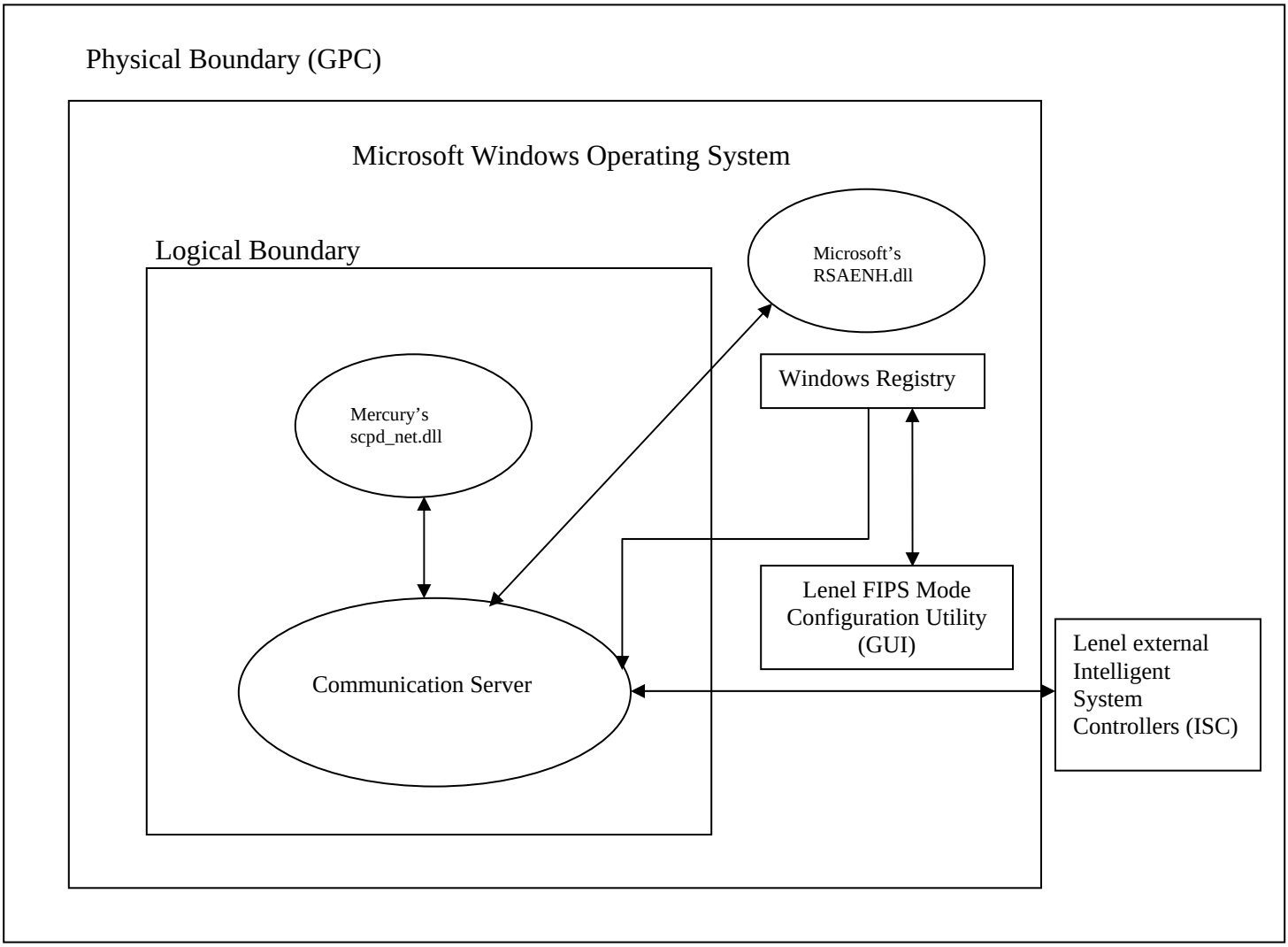
The two diagrams below define the physical and logical boundaries for each of the validated modules. Note:

- The Communication Server module is the only one of the two modules that

communicates with entities outside the physical boundary of the GPC.

- The Lenel FIPS Mode Configuration Utility, a graphical user interface application, is used to place the Communication Server module configuration data in the Windows Registry. The Lenel FIPS Mode Configuration Utility application is not a FIPS module.

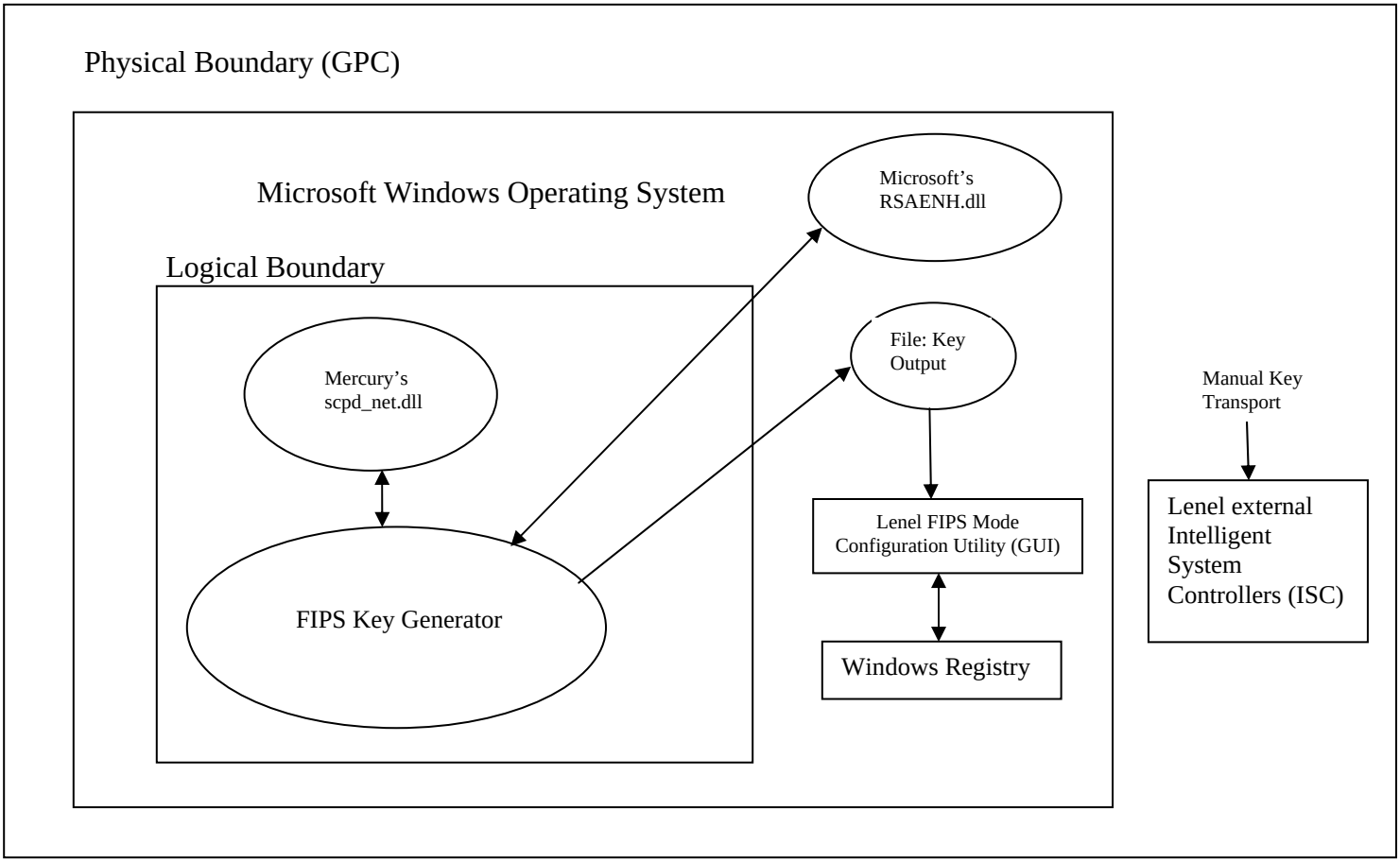
Figure 1 – Diagram of the Communication Server Module



Note:

- The FIPS Key Generator writes its output, a strong cryptographically generated key, to a file within the GPC's physical boundary. The Lenel FIPS Mode Configuration Utility application is used to place the key generated by the FIPS Key Generator into the Windows Registry where it will be read by the Communication Server module.

Figure 2 – Diagram of the FIPS Key Generator Module



2. Security Level

Each of the two separate Lenel FIPS 140-2 cryptographic modules (Communication Server, FIPS Key Generator) meet the same overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1 - 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 Lenel FIPS 140-2 validated cryptographic modules support the listed algorithms as follows:

FIPS Key Generator:

- AES CBC with 128-bit keys for encryption using Scpd_net.dll (AES Certificate #327).
- RNG based on ANSI X9.31 Appendix A.2.4 using the AES algorithm (RNG Certificate #149)
- RSA signatures with a SHA-1 file hash using RSAENH.DLL (RSA Certificate #81).
- SHA-1 using RSAENH.DLL (SHA Certificate #364).
- DRNG using RSAENH.DLL (FIPS 186-2 DRNG is vendor affirmed).

Communication Server:

- AES CBC with 128-bit keys for encryption using Scpd_net.dll (AES Certificate #327).
- RNG based on ANSI X9.31 Appendix A.2.4 using the AES algorithm (RNG Certificate #149)
- RSA signatures with a SHA-1 file hash using RSAENH.DLL (RSA Certificate #81).
- SHA-1 using RSAENH.DLL (SHA Certificate #364).
- DRNG using RSAENH.DLL (FIPS 186-2 DRNG is vendor affirmed).

The two separate Lenel FIPS 140-2 cryptographic modules may be configured for FIPS mode as follows:

FIPS Key Generator:

- Always in FIPS mode.

Communication Server:

- Execute the FIPS Mode Configuration Utility application (see section "13. Definitions and Acronyms" below):
    - Turn its [Enable FIPS Mode] checkbox ON.
    - Select which key is to be used as the active Master Key.
    - Save the above setting to the Windows Registry.
- Start/Restart the Communication Server module:
    - On its start up the Communication Server module will read the above settings from the Windows Registry which is within the physical boundary of the Communication Server module.
- The operator can determine if the Communication Server module is running in FIPS mode in two ways:
    - Dynamically (when started as an application on the GPC): The Communication Server module display window status line indicates "FIPS Mode".
    - Procedurally (when started as a service on the GPC):
        - Whenever the FIPS Mode Configuration Utility application is used to change the value of its [Enable FIPS Mode] on/off checkbox and save that new value in the Windows Registry, record this activity in a log noting the date and time the value was saved to the Registry.
        - Whenever the Communication Server module is started, record this activity in a log noting the date and time the Communication Server module was started.
        - Compare the two logs above. The currently running Communication Server module will be running in FIPS mode if the [Enable FIPS Mode] on/off checkbox value in the Windows Registry was "on" when the Communication Server module was started.

3.2 Non-Approved Algorithms

The two separate Lenel FIPS 140-2 validated cryptographic modules use non-Approved cryptographic algorithms as follows:

FIPS Key Generator:

- None used.

Communication Server:

- Uses the RC2 algorithm for encrypting and decrypting data sent to or received from the external OnGuard Access Control database. No security claim is made for the data encrypted with RC2 and for the purpose of FIPS is considered plaintext. This data does not contain any CSPs.

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:

Interface	**Logical**	**Physical**
Data Input	FIPS Key Generator: • GUI interface Communication Server: • Data read from the Windows Registry • Data received from an external Intelligent System Controller (ISC) • Configuration information received via remote procedure calls (RPC) • COM interface calls from non Lenel ISCs • Data read from the OnGuard Access Control database	FIPS Key Generator: • Keyboard & mouse Communication Server: • GPC Windows Registry file • Ethernet port • Serial port • Modem
Data Output	FIPS Key Generator: • GPC disk File Communication Server: • Data sent to Intelligent System Controllers • Data returned to remote procedure calls (RPC) • Data sent to non Lenel ISCs via COM interfaces • Data written to the OnGuard Access Control database	FIPS Key Generator: • GPC disk Communication Server: • Ethernet port • Serial port • Modem
Control Input	FIPS Key Generator:	FIPS Key Generator:

	• GUI interface Communication Server: • Data read from the Windows Registry • Remote procedure calls • COM interface calls from non Lenel ISCs	• Keyboard & mouse Communication Server: • GPC Windows Registry file • Ethernet port • Serial port • Modem
Status Output	FIPS Key Generator: • GUI interface Communication Server: • Error log files or Windows message boxes • Events and status messages sent to client applications via socket connections	FIPS Key Generator: • GPC Display Communication Server: • GPC Hard disk • GPC Display • Ethernet port • Serial port • Modem
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. (See Section 6.1, Roles and Services, for service definitions.)

FIPS Key Generator:

- 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.

Communication Server:

- Crypto-Officer Role: This role is assumed to provide the operator key management and alternating bypass control. The Crypto-Officer role is assumed by the selection of the following services:
  - Module Master Key Management (configuration data read from the Windows Registry)
  - Alternating Bypass Enable/Disable (configuration data read from the Windows Registry)
  - Key Generation (Session Key)
  - Key Output Service (Session Key wrapped with Master Key 1 or Master Key 2)
  - Zeroize

- User Role: This role is assumed to provide the operator access to cryptographic services, communication services, status information, self-tests and zeroization service. The user role is assumed by the selection of the following services:
  - Secure Data Transmission
  - Show Status
  - Self-Tests
  - Zeroize
  - Remote Procedure Call
  - COM Interface Method
  - Database Interaction

The Communication server module does not support a maintenance role.

6. Access Control Policy

6.1 Roles and Services

The cryptographic modules support the following services:

- **Module Master Key Management**: This service allows Master Key 1 and Master Key 2 to be read from the Windows Registry. Performed by:
  - Communication Server:
    - The active master key, Master Key 1 or Master Key 2, is read from the Windows Registry whenever the Communication Server is started. The Windows Registry contains another data item, read by the Communication Server module on start-up, that indicates which key, Master Key 1 or Master Key 2 is the active master key it is to use.
    - Note that Master Key 1 and Master Key 2 are placed in the Windows Registry by the FIPS Mode Configuration Utility application (a GUI which is not a FIPS module).
- **Alternating Bypass Enable/Disable**: This service allows encryption of data to be enabled or disabled during communication with external Intelligent System Controllers (ISCs). Performed by:
  - Communication Server:

        - Reads Bypass configuration parameters that were placed in the Windows Registry by the FIPS Mode Configuration Utility application.
        - Uses the Bypass parameters to control its form of communication with Intelligent System Controllers outside the module's physical boundary. Depending on the Windows Registry Bypass Parameter values, communication with different ISCs may alternate between plaintext and ciphertext.

- **Secure Data Transmission**: This service provides AES encryption/decryption operations for secure transmission of data. (NOTE: During each Communication Server session a fresh Session Key is generated by the Communication Server module via an Approved RNG and is electronically output to the ISC encrypted with the active AES Master Key). Performed by:
  - Communication Server
- **Show Status**: This service provides the current status of the cryptographic module. Performed by:
  - FIPS Key Generator
  - Communication Server
- **Self-tests**: This service executes the suite of self-tests required by FIPS 140-2. Performed by:
  - FIPS Key Generator
  - Communication Server
- **Zeroize**: This service zeroizes plaintext critical security parameters. Performed by:
  - FIPS Key Generator which zeroizes:
    - Master Key 1 and Master Key 2:
      - Zeroizes its own RAM working copy of Master Key 1 or Master Key 2 (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.
  - Communication Server which zeroizes:
    - Master Key 1 and Master Key 2:
      - Zeroizes its own RAM working copy of Master Key 1 or Master Key 2 (only one can be resident in the Communication Server module's RAM at any given moment).
    - Session Key:
      - Zeroizes its own RAM working copy of the Session Key (only one Session Key can be resident in the Communication Server module's RAM at any given moment). Note: The Communication Server is the "**owner**" of the Session Key.
    - 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 Key 1, Master Key 2, and Session Keys to be generated. Performed by:
  - FIPS Key Generator which generates:
    - Master Key 1
    - Master Key 2
  - Communication Server which generates:
    - Session Keys
- **Key Output Service**: This service provides a means for Master Key 1, Master Key 2, and Session Key(s) to be output. Performed by:
  - FIPS Key Generator:
    - Master Key 1: Generates Master Key 1 and then outputs it 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.
    - Master Key 2: Generates Master Key 2 and then outputs it to be distributed manually to external Lenel ISCs. Master Key 2 is output in plaintext which is allowed for Level 1, Manual Distribution/Manual Output as per FIPS 140-2 IG 7.7.
  - Communication Server:
    - Session Key: Generates Session Key and then outputs it (encrypted with either Master Key 1 or Master Key 2) to be distributed electronically to external Lenel ISCs.
- **Remote Procedure Call Service:** This service provides a means for external client applications to communicate with the Communication Server module. Performed by:
  - Communication Server
- **COM Interface Method Service:** This service provides a means for the Communication Server module to interact with device translators via COM method interfaces. Performed by:
  - Communication Server
- **Database Interaction Service:** This service provides a means for the Communication Server module to communicate with the Lenel OnGuard Access Control database. Performed by:
  - Communication Server

6.2 Service Inputs and Outputs

Table 5 - Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
Module Master Key Management	Command Header info.	Plaintext master key	N/A	Success/Fail

Service	Control Input	Data Input	Data Output	Status Output
Alternating Bypass Enable/Disable	Command Header info.	Bypass values read from Windows Registry	N/A	Success/Fail
Secure Data Transmission (Encryption)	Command Header info.	Plaintext data	Ciphertext data	Success/Fail
Secure Data Transmission (Decryption)	Command Header info.	Ciphertext data	Plaintext data	Success/Fail
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 (Documentation requires that the operator must select a secure location)	Key	Success/Fail
Remote Procedure Call	Command Header info.	Command/Request data	Plaintext response	Success/Fail
COM Interface Method	Command Header info.	N/A	Command/Request data sent to ISC device translators	Success/Fail
Database Interaction	Command Header info.	Data received from the Database	Data written to the Database	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 Key 1 – This key can be used by the Communication Server module to encrypt Session Keys it sends to external Intelligent System Controllers:
    - As it starts up, the Communication Server module can read the Master Key 1 value from the Windows Registry.
- Master Key 2 – This key can be used by the Communication Server module to encrypt Session Keys it sends to external Intelligent System Controllers :
    - As it starts up, the Communication Server module can read the Master Key 2 value from the Windows Registry.

  (*Note on differences between Master Key 1 and Master Key 2 above:*
  The Windows registry can contain values for two Lenel OnGuard Access Control master keys, Master Key 1 and Master Key 2. Both values are written to the Registry by the Lenel FIPS Mode Configuration Utility application. There is another Windows registry value, also placed there by the FIPS Mode Configuration Utility application, indicating which Master Key the Communication Server module is to use when it starts up (Master Key 1 or Master Key 2). Only one of these master keys is used during each Communication Server module instantiation.)
- Session Key – This key is used by the Communication Server module to encrypt data communications with ISCs:
    - The Communication Server is the "**owner**" of the Session Key. The FIPS Key Generator never uses the Session Key.
- Seed Key for Mercury DRNG within the Mercury SCPD_NET.DLL. This seed value is used for generating random numbers:
    - The Communication Server module has its own Seed Key. It is the "**owner**" of that Seed Key.
- Seed Value for Mercury DRNG within the Mercury SCPD_NET.DLL. This seed value is used for generating random numbers:
    - The Communication Server module has its own Seed Value. It is the "**owner**" of that Seed Value.

Definition of Public Keys:

The following public key is contained in each of the two separate Lenel FIPS 140-2 cryptographic modules (FIPS Key Generator, Communication Server).

- 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:

- **G**enerate: the CSP is generated.
- **E**nter: the CSP is input into the cryptographic module.
- **O**utput: the CSP is output from the cryptographic module.
- **R**ead: the CSP is used within its corresponding security function.

- **Z**eroize: the CSP is zeroized.

The two separate Lenel FIPS 140-2 cryptographic modules will be represented with the following acronyms in Table 6 immediately below:

- FIPS Key Generator module KeyGen
- Communication Server module ComServer

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

Table 6 – CSP Access Rights within Roles & Services

7. Operational Environment

FIPS 140-2 Area 6 Operational Environment requirements are applicable because the two Lenel OnGuard Access Control Cryptographic modules run in a modifiable operational environment. The following operating systems were used during the FIPS 140-2 operational testing:

- Windows Server 2003 SP1

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

b. the GPC uses the specified single user operating system/mode specified on the validation certificate, or the specified single user operating system/mode specified for Windows 2000 SP4 or Windows XP SP2.

8. Security Rules

The design of the two cryptographic modules corresponds to the following security rules. This section documents the security rules enforced by the two cryptographic modules 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:
    - FIPS Key Generator
    - Communication Server
2. The modules do not support operator authentication. Applies to:
    - FIPS Key Generator
    - Communication Server
3. The cryptographic modules shall encrypt message traffic using the AES algorithm. Applies to:
    - Communication Server
4. Self-tests:

    <u>FIPS Key Generator (KeyGenerator.exe):</u>

    A. Power up Self-Tests:

        a. Cryptographic algorithm 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 Cert. #382) which is dynamically linked in by the FIPS Key Generator:

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

b. Software Integrity Test:

i. A strong integrity test is performed over the FIPS Key Generator module as required by FIPS 140-2.

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

c. Critical Functions Tests: Not Applicable

B. Conditional Self-Tests

a. Continuous Random Number Generator (RNG) tests:

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

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

ii. Microsoft DLL (RSAENH.DLL) DRNG:

- Inferred – test performed inside the Microsoft Enhanced Cryptographic Provider DLL (RSAENH.DLL with FIPS 140-2 Cert. #382).

<u>Communication Server (lnlcomsrvr.exe):</u>

A. Power up Self-Tests:

a. Cryptographic Algorithm Tests:

i. AES Known Answer Test (KAT). Performed inside the Mercury DLL (scpd_net.dll) which is dynamically linked in by the Communication Server.

ii. ANSI x9.31 RNG Known Answer Test. Performed inside the Mercury DLL (scpd_net.dll) which is dynamically linked in by the Communication Server.

iii. The following power up Cryptographic algorithm tests are performed inside the Microsoft Enhanced Cryptographic Provider DLL (RSAENH.DLL with FIPS 140-2 Cert. #382) which is dynamically

linked in by the Communication Server:

- RSA Sign/Verify with SHA-1
- DRNG

b. Software Integrity Test:

i. A strong integrity test is performed over the Communication Server module as required by FIPS 140-2.

ii. Using the Microsoft Enhanced Cryptographic Provider (RSAENH with FIPS 140-2 Cert. #382), verify RSA signatures with SHA-1 file hashes on all executable files within the Communication Server's logical boundary.

c. Critical Functions Tests: Not Applicable

B. Conditional Self-Tests:

a. Continuous Random Number Generator (RNG) tests:

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

- Test performed inside the Communication Server (lnlcomsrvr.exe) after it receives a random number from the Mercury DLL.

ii. Microsoft DLL (RSAENH.DLL) DRNG:

- Inferred – test performed inside the Microsoft Enhanced Cryptographic Provider DLL (RSAENH.DLL with FIPS 140-2 Cert. #382).

b. Bypass Tests:

i. For each ISC communication channel that is not being bypassed, the Communication Server will always perform an encryption verification test before sending an encrypted packet on that channel. This insures that plaintext information is never output on a channel that is not being bypassed.

ii. Alternating bypass, corruption of Windows Registry configuration hash mechanism.

5. 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. At start-up, each of these modules automatically run their power-up self-tests (as listed in security rule #4). Applies to:
   - FIPS Key Generator
   - Communication Server
6. Prior to each use random number output shall be tested using the conditional test specified in FIPS 140-2 section 4.9.2:
   - Microsoft Enhanced Cryptographic Provider RSAENH.DLL (FIPS 140-2 Cert.

#382) is responsible for testing its own RNG output.

- Mercury SPD_NET.DLL RNG output is tested by the Lenel modules that request the output. Applies to:
  - FIPS Key Generator
  - Communication Server

7. Data output shall be inhibited during self-tests and error states. Applies to:
   - FIPS Key Generator
   - Communication Server
8. Logical disconnection of the output data path is implemented as follows:
   - FIPS Key Generator. Implemented during:
     - Key zeroization
     - Key generation
   - Communication Server. Implemented during:
     - Key zeroization
     - Key generation
9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module. Applies to:
   - FIPS Key Generator
   - Communication Server
10. The two modules 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. Applies to:
    - FIPS Key Generator
    - Communication Server
11. 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 modules are software only cryptographic modules, 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 7 – 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. Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)

Each of the two separate Lenel FIPS 140-2 cryptographic modules (Communication Server, FIPS Key Generator) meet Level 3 security for FIPS 140-2 EMI/EMC requirements. Testing of the module, a software only module, was performed on a GPC platform (DELL Optiplex GX260 with Intel Pentium 4 Mobile 1.80 GHz). The DELL Optiplex GX260 contains an FFC label that provides evidence that it conforms to EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

11. 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 8 – 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

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 (it does not directly implement any FIPS Approved cryptographic algorithm – it relies on the Microsoft RSAENH.DLL for FIPS Approved algorithm functionality).

NIST – National Institute of Standards and Technology.

SHA-1 – Secure Hash Algorithm revision 1.