Lenel OnGuard Access Control Cryptographic Module

Non- Proprietary Security Policy

Document *Version 2.10*

UTC Fire & Security Americas Corporation, Inc.

www.lenel.com

July 12, 2017

Copyright 2017 UTC Fire & Security Americas Corporation, Inc.

May be reproduced only in its original entirety [without revision].

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
2.10	07/11/2017	M. OBrien	Reverted to OnGuard version 7.3.345.54 due to errors found in .100.

TABLE OF CONTENTS

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 Windows 10, Windows Server 2012, Windows Server 2012 R2, Windows 8.1 or Windows 8 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. This is a previously validated FIPS 140-2 module (CMVP Certs. #2606, #2357 & #1892)
- Mercury SCPD_NET.DLL

The operating systems listed in Table 1 below were tested using ESXi 6.0, but are vendor affirmed[1] to run without ESXi6.0. Both configurations are considered FIPS 140-2 compliant.

Table 1 – Module Configurations

Operating System	Lenel OnGuard	BCRYPTPRIMITIVES.dll	Mercury scpd_net.dll
Windows 10 64 bit	7.3.345.54	CMVP Cert #2606	4.6.1.180
Windows Server 2012 R2 64-bit	7.3.345.54	CMVP Cert. #2357	4.6.1.180
Windows Server 2012 64-bit	7.3.345.54	CMVP Cert. #1892	4.6.1.180
Windows 8.1 64-bit	7.3.345.54	CMVP Cert. #2357	4.6.1.180
Windows 8 64-bit	7.3.345.54	CMVP Cert. #1892	4.6.1.180

1 The CMVP does not guarantee the correct operation of vendor affirmed configurations, however these configurations are FIPS compliant per IG G.5 and assurance of the correct operation is guaranteed by Lenel.

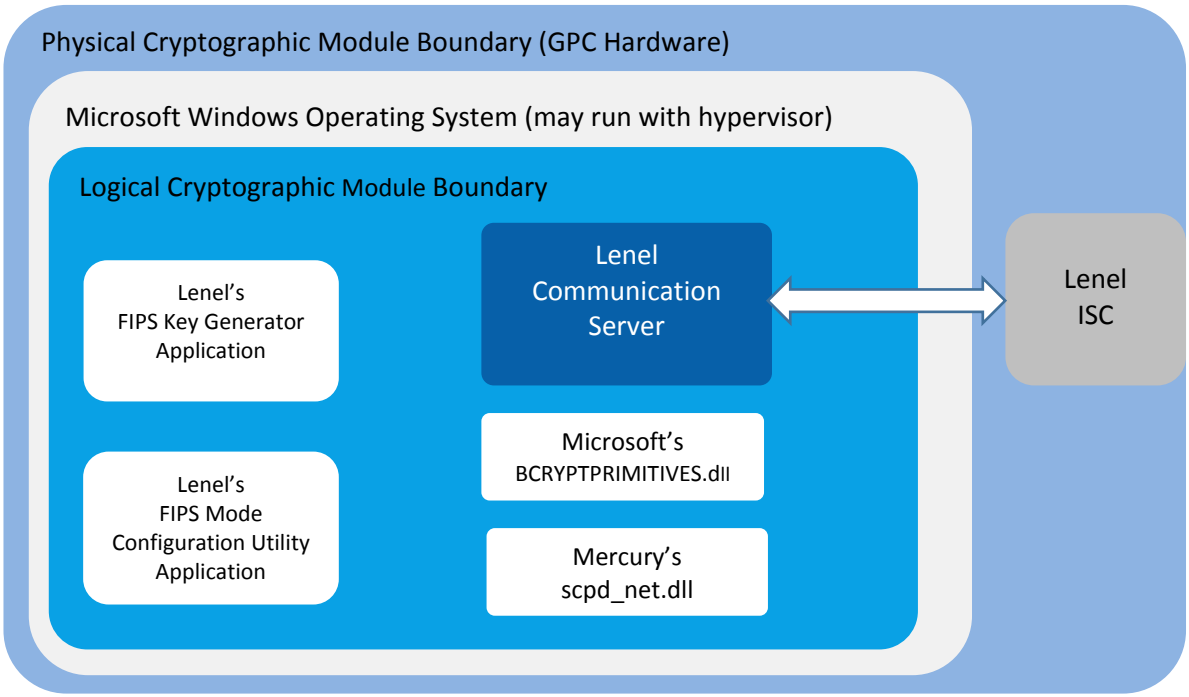

Figure 1 – Cryptographic Module Diagram

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

Security Requirements Section	Level
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 Cert. #4149).

In addition to the above, the cryptographic module also uses algorithms provided by BCRYPTPRIMITIVES.DLL validated to FIPS 140-2 under CMVP Certs. #2606, #2357 & #1892 as shown in the following table.

Table 3 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
Algorithms Used by SCPD_NET.DLL		
AES	[FIPS 197, SP 800-38A] Modes: ECB (Encrypt/Decrypt), CBC (Encrypt only) Key sizes: 128 bits	4149
Algorithms Used by BCRYPTPRIMITIVES.DLL		
AES	[FIPS 197, SP 800-38A] Modes: CTR (internal only) Key sizes: 256 bits *Note: this implementation is only used by the DRBG	2197, 2832 or 3497
DRBG	[SP 800-90A] Functions: Generation Modes: CTR DRBG Security Strength: 256 bits	258, 489 or868
RSA	[FIPS 186-4, PKCS1 v1.5] Functions: Signature Verification with SHA-256 file hash Key Sizes: 2048	1134, 1493 or 1783
SHA	[FIPS 180-4] SHA Sizes: SHA-256	1903, 2373 or 2886

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.

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. Please see Table 9 for a list of algorithms, services and self-tests performed by each individual application.

The services available in the FIPS mode of operation are covered in Section 6 below.

The critical security parameters that are used while in FIPS mode are covered in Section 6.3

The algorithms used and self-tests that are performed while in FIPS mode of operation are covered in Section 8.

3.2 Non-Approved Algorithms

The Lenel Communication Server uses the RC2 algorithm for encrypting and decrypting data as part of the Database Interaction Service (non-compliant). This data is treated as plain text as far as this module is concerned.

3.3 Non-Approved but Allowed Algorithms

The Lenel Communication Server implements AES Key Wrapping of session keys, not compliant with NIST key transport standards (provides 128 bits of encryption strength).

4. Ports and Interfaces

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

Table 4 – 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	Ethernet, serial port, modem, Remote

Interface	Logical	Physical
	via remote procedure calls (RPC). COM interface calls from non Lenel ISCs. Data read from the database by the Communication Server.	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. This operation is performed both in RAM as well as in the registry of the workstation where the CSP's are stored.
- **Configure FIPS Mode of Operation**: 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.

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 cryptographic module via an Approved DRBG 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 (non-compliant):** This service provides interaction with the database from the Communication Server. The module is considered to be in a non-Approved Mode while using this service.

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	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 Operation	Service Selection	None	None	Success/Fail
Key Generation	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
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 (non-compliant)	None	None	Plaintext	Plaintext

6.3 Definition of Critical Security Parameters (CSPs)

- **Master Key 1** – This AES-128 bit key is used to provide encryption of session keys.

- **Master Key 2** – This AES-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

6.4 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.

6.5 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	DRBG Seed	DRBG State	RSA Public Key
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	-
X		Configure FIPS Mode of Operation	-	-	-	-	-	-
X		Key Generation	G	G	-	G[1]	G	-

	X	Secure Data Transmission	R	R	G,O,R	G[1]	G	-
	X	Show Status	-	-	-	-	-	-
	X	Self-Tests	-	-	-		-	-
	X	Remote Procedure Call	-	-	-	-	-	-
	X	COM Interface Method	-	-	-	-	-	-
	X	Database Interaction (non-compliant)	-	-	-	-	-	-

Table 6 – CSP Access Rights within Roles & Services

1 Note that "G" is periodic; it does not occur on every service call

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 2012 64-bits
- Windows Server 2012 R2 64-bits
- Windows 8.1 64-bits
- Windows 8 64-bits
- Windows 10 64-bits

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 the AES algorithm using 128-bit keys 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.

   A. Power up Self-Tests:

      a. Cryptographic Algorithm Tests:

         i. AES ECB (encrypt and decrypt) Known Answer Test (Cert. #4149)

ii. AES-256 CTR DRBG Known Answer Test with health checks (instantiate, generate and reseed) as defined in SP 800-90A section 11.3 (Certs. #2197, #2832 and #3497)*

iii. RSA signature verification Known Answer Test*

iv. SHA-256 Known Answer Test.

b. Software Integrity Test

i. RSA 2048 with SHA-256 signature verification.

c. Critical Functions Tests: Configuration Parameter Integrity test

B. Conditional Self-Tests:

a. Microsoft Cryptographic Primitives Library performs a continuous RNG test (CRNGT) for the Deterministic Random Bit Generator (DRBG) of this cryptographic module. There is also a CRNGT for the entropy source of the DRBG.

b. Manual key entry test

c. 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 ISC's 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.

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. 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 8 – Mitigation of Other Attacks

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

11. Multiple Approved Modes

Table 9 maps the algorithms, services and self-tests performed by each application. The Cert. # used for the algorithms specified below are dependent on which BCRYPTPRIMITIVES.dll Cert. # is used (CMVP Certs. #2606, #2357 or #1892). Note that the one exception is that the Communication Server always uses Cert. #4149 for AES key transport.

Table 9 – Individual Application Functionality

Application	Algorithms	Services	Self-Tests
Communication Server	• AES • DRBG • SHA • RSA	• Secure Data Transmission • Remote Procedure Call Service • COM Interface Method Service • Database Interaction	**Cryptographic Algorithm Tests:** • AES encrypt/ decrypt KATs • DRBG KAT and SP 800-90A Health Checks* • SHA-256 KAT

Application	Algorithms	Services	Self-Tests
		Service (non-compliant) • Zeroize • Show Status • Self-tests	• 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	• AES • DRBG • SHA • RSA	• Key Generation • 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 **Conditional Tests:** • DRBG CRNGT • Entropy Source CRNGT
FIPS Mode Configuration Utility	• SHA • RSA	• Module Master Key Management • Alternating Bypass Enable/Disable • Configure FIPS Mode of Operation • Zeroize • Show Status • Self-tests	**Cryptographic algorithm tests** • SHA-256 KAT • RSA verification KAT* **Software Integrity Test:** • RSA verification with SHA-256 **Conditional Tests:** • Manual Key Entry Test

12. References

The UTC Fire & Security Americas Corporation, Inc. Lenel website: http://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 Microsoft Windows 8 Microsoft Windows Server 2012 Microsoft Windows RT Microsoft Surface Windows RT Microsoft Surface Windows 8 Pro Microsoft Windows Phone 8 Microsoft Windows Storage Server 2012 Cryptographic Primitives Library (BCRYPTPRIMITIVES.DLL)

Non-proprietary Security Policy for FIPS 140-2 Validation Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series

13. Definitions and Acronyms

AES – Advanced Encryption Standard.

ISC – Intelligent System Controller.

CBC – Cipher Block Chaining.

CSP – Critical Security Parameters.

RNG –Random Number Generator.

DRBG – Deterministic Random Bit Generator.

EMI – Electromagnetic Interference.

FIPS – Federal Information Processing Standards.

GPC – General Purpose Computer.

NIST – National Institute of Standards and Technology.

SHA – Secure Hash Algorithm.