Table of Contents

1 INTRODUCTION ............................................................................................................................................... 5
  1.1 PURPOSE .................................................................................................................................................. 5
  1.2 REFERENCES ........................................................................................................................................... 5

2 HP ENTERPRISE SECURE KEY MANAGER ............................................................................................... 6
  2.1 OVERVIEW .............................................................................................................................................. 6
  2.2 CRYPTOGRAPHIC MODULE SPECIFICATION ..................................................................................... 6
  2.3 MODULE INTERFACES ........................................................................................................................... 8
  2.4 ROLES, SERVICES, AND AUTHENTICATION ........................................................................................... 11
    2.4.1 Crypto-Officer Role .......................................................................................................................... 11
    2.4.2 User Role ........................................................................................................................................ 13
    2.4.3 HP User Role .................................................................................................................................. 14
    2.4.4 Cluster Member Role ....................................................................................................................... 14
    2.4.5 Authentication ................................................................................................................................. 14
    2.4.6 Unauthenticated Services ................................................................................................................ 15
  2.5 PHYSICAL SECURITY .............................................................................................................................. 15
  2.6 OPERATIONAL ENVIRONMENT ............................................................................................................... 16
  2.7 CRYPTOGRAPHIC KEY MANAGEMENT ............................................................................................... 16
    2.7.1 Keys and CSPs ................................................................................................................................. 16
    2.7.2 Key Generation ............................................................................................................................... 20
    2.7.3 Key/CSP Zeroization ....................................................................................................................... 20
  2.8 SELF-TESTS ............................................................................................................................................. 20
  2.9 MITIGATION OF OTHER ATTACKS ......................................................................................................... 21

3 SECURE OPERATION .................................................................................................................................... 22
  3.1 INITIAL SETUP ....................................................................................................................................... 22
  3.2 INITIALIZATION AND CONFIGURATION .............................................................................................. 22
    3.2.1 First-Time Initialization .................................................................................................................. 22
    3.2.2 FIPS Mode Configuration .............................................................................................................. 22
  3.3 PHYSICAL SECURITY ASSURANCE ....................................................................................................... 23
  3.4 KEY AND CSP ZEROIZATION ................................................................................................................ 25
  3.5 ERROR STATE ......................................................................................................................................... 25

ACRONYMS .............................................................................................................................................................. 26
# Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIGURE 1</td>
<td>DEPLOYMENT ARCHITECTURE OF THE HP ENTERPRISE SECURE KEY MANAGER</td>
<td>6</td>
</tr>
<tr>
<td>FIGURE 2</td>
<td>BLOCK DIAGRAM OF ESKM</td>
<td>7</td>
</tr>
<tr>
<td>FIGURE 3</td>
<td>FRONT PANEL LEDS</td>
<td>9</td>
</tr>
<tr>
<td>FIGURE 4</td>
<td>REAR PANEL COMPONENTS</td>
<td>9</td>
</tr>
<tr>
<td>FIGURE 5</td>
<td>REAR PANEL LEDS</td>
<td>10</td>
</tr>
<tr>
<td>FIGURE 6</td>
<td>FIPS COMPLIANCE IN CLI</td>
<td>23</td>
</tr>
<tr>
<td>FIGURE 7</td>
<td>FIPS COMPLIANCE IN WEB ADMINISTRATION INTERFACE</td>
<td>23</td>
</tr>
<tr>
<td>FIGURE 8</td>
<td>TAMPER-EVIDENCE LABELS ON ESKM</td>
<td>24</td>
</tr>
<tr>
<td>FIGURE 9</td>
<td>TAMPER-EVIDENCE LABEL ON TOP OF ESKM</td>
<td>24</td>
</tr>
<tr>
<td>FIGURE 10</td>
<td>TAMPER-EVIDENCE LABELS ON SIDE OF ESKM</td>
<td>24</td>
</tr>
<tr>
<td>FIGURE 11</td>
<td>TAMPER-EVIDENCE LABELS ON REAR OF ESKM</td>
<td>25</td>
</tr>
</tbody>
</table>
Table of Tables

<table>
<thead>
<tr>
<th>TABLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SECURITY LEVEL PER FIPS 140-2 SECTION</td>
</tr>
<tr>
<td>2</td>
<td>LOGICAL INTERFACE AND PHYSICAL PORTS MAPPING</td>
</tr>
<tr>
<td>3</td>
<td>FRONT PANEL LED DEFINITIONS</td>
</tr>
<tr>
<td>4</td>
<td>REAR PANEL COMPONENTS DESCRIPTIONS</td>
</tr>
<tr>
<td>5</td>
<td>REAR PANEL LED DEFINITIONS</td>
</tr>
<tr>
<td>6</td>
<td>CRYPTO OFFICER SERVICES</td>
</tr>
<tr>
<td>7</td>
<td>USER SERVICES</td>
</tr>
<tr>
<td>8</td>
<td>HP USER SERVICES</td>
</tr>
<tr>
<td>9</td>
<td>CLUSTER MEMBER SERVICES</td>
</tr>
<tr>
<td>10</td>
<td>ROLES AND AUTHENTICATIONS</td>
</tr>
<tr>
<td>11</td>
<td>LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS FOR SSH</td>
</tr>
<tr>
<td>12</td>
<td>LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS FOR TLS</td>
</tr>
<tr>
<td>13</td>
<td>CIPHER SUITES SUPPORTED BY THE MODULE’S TLS IMPLEMENTATION IN FIPS MODE</td>
</tr>
<tr>
<td>14</td>
<td>OTHER CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS</td>
</tr>
<tr>
<td>15</td>
<td>ACRONYMS</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Purpose

This document is a non-proprietary Cryptographic Module Security Policy for the HP Enterprise Secure Key Manager (ESKM) from Hewlett-Packard Company. Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules, specifies the U.S. and Canadian Governments’ requirements for cryptographic modules. The following pages describe how HP’s ESKM meets these requirements and how to use the ESKM in a mode of operation compliant with FIPS 140-2. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the HP ESKM 3.0 (Hardware P/N AJ585A, Version 3.0; Firmware Version: 5.0.0) and ESKM 3.1 (Hardware P/N C8Z51AA, Version 3.1; Firmware Version: 5.1.0).

More information about FIPS 140-2 and the Cryptographic Module Validation Program (CMVP) is available at the website of the National Institute of Standards and Technology (NIST): http://csrc.nist.gov/groups/STM/cmvp/index.html.

In this document, the HP Enterprise Secure Key Manager is referred to as the ESKM, the module, or the device.

1.2 References

This document deals only with the operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The HP website (http://www.hp.com) contains information on the full line of products from HP.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the module.
2 HP Enterprise Secure Key Manager

2.1 Overview

HP provides a range of security products for banking, the Internet, and enterprise security applications. These products use encryption technology—often embedded in hardware—to safeguard sensitive data, such as financial transactions over private and public networks and to offload security processing from the server.

The HP Enterprise Secure Key Manager is a hardened server that provides security policy and key management services to encrypting client devices and applications. After enrollment, clients, such as storage systems, application servers and databases, make requests to the ESKM for creation and management of cryptographic keys and related metadata.

Client applications can access the ESKM via its Key Management Service (KMS) server. Configuration and management can be performed via web administration, Secure Shell (SSH), or serial console. Status-monitoring interfaces include a dedicated FIPS status interface, a health check interface, and Simple Network Management Protocol (SNMP).

The deployment architecture of the HP Enterprise Secure Key Manager is shown in Figure 1 below.

2.2 Cryptographic Module Specification

The HP Enterprise Secure Key Manager is validated at FIPS 140-2 section levels shown in Table 1.

<table>
<thead>
<tr>
<th>Section</th>
<th>Section Title</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cryptographic Module Specification</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Cryptographic Module Ports and Interfaces</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Roles, Services, and Authentication</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Finite State Model</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>Physical Security</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>Operational Environment</td>
<td>N/A</td>
</tr>
<tr>
<td>7</td>
<td>Cryptographic Key Management</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>EMI/EMC</td>
<td>2</td>
</tr>
</tbody>
</table>
The block diagram of the module is given in Figure 2. The cryptographic boundary is clearly shown in the figure. Notice that the power supplies are not included in the boundary.

The block diagram of the module is given in Figure 2. The cryptographic boundary is clearly shown in the figure. Notice that the power supplies are not included in the boundary.

In the FIPS mode of operation, the module implements the following Approved algorithms:

- Advanced Encryption Standard (AES) encryption and decryption: 128, 192, and 256 bits, in Electronic Codebook (ECB) and Cipher Block Chaining (CBC) modes (Certificate #2069)
- Triple Data Encryption Standard (Triple-DES or TDES) encryption and decryption: 168 bits (3-key), in ECB and CBC modes (Certificate #1328)
- Secure Hash Algorithm (SHA)-1, SHA-256, SHA-384, SHA-512 (Certificate #1802)
• Keyed-Hash Message Authentication Code (HMAC)-SHA-1 and HMAC-SHA-256 (Certificate #1254)
• Rivest, Shamir, and Adleman (RSA) American National Standard Institute (ANSI) X9.31 key generation, signature generation, and signature verification: 1024 (signature verification only) and 2048 bits (Certificate #1073)
• Deterministic Random Bit Generator (DRBG) using AES in CTR mode (Certificate #207)
• Diffie-Hellman key agreement (CVL Certificate #23)
• Digital Signature Algorithm (DSA) key generation (required for Diffie-Hellman KAS): 1024 bits (Certificate #653)

In the FIPS mode of operation, the module implements the following non-Approved algorithms:

• A non-Approved Non-Deterministic Random Number Generator (NDRNG) to seed the DRBG
• The following commercially-available protocols for key establishment:
  - Transport Layer Security (TLS) 1.0/Secure Socket Layer (SSL) 3.1 protocol using RSA 2048 bits for key transport (key wrapping: key establishment methodology provides 112 bits of encryption strength)

In the non-FIPS mode of operation, the module also implements the non-Approved algorithms DES, MD5, RC4, and RSA-512, RSA-768, and RSA-1024 for signature generation and verification, and key establishment as well as the above listed protocols for key establishment.

2.3 Module Interfaces

FIPS 140-2 defines four logical interfaces:

• Data Input
• Data Output
• Control Input
• Status Output

The module features the following physical ports and LEDs:

• Serial port (RS232 DB9)
• Ethernet 10/100/1000 RJ-45 ports (Network Interface Card [NIC], quantity: 2)
• Monitor port (VGA DB15)
• Power input (100-240VAC)
• LEDs (four on the front panel and three on the rear panel)

The logical interfaces and their physical port mappings are described in Table 2.

<table>
<thead>
<tr>
<th>Logical Interface</th>
<th>Physical Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Input</td>
<td>Serial, Ethernet</td>
</tr>
<tr>
<td>Data Output</td>
<td>Monitor, serial, Ethernet</td>
</tr>
<tr>
<td>Control Input</td>
<td>Serial, Ethernet</td>
</tr>
<tr>
<td>Status Output</td>
<td>Monitor, serial, Ethernet, LEDs</td>
</tr>
</tbody>
</table>
There are no ports on the front panel. There are four LEDs on the front panel. See Figure 3.

![Figure 3 – Front Panel LEDs](image1)

Descriptions of the LEDs are given in Table 3.

### Table 3 – Front Panel LED Definitions

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unit Identifier (UID) LED/button</td>
<td>Blue = Identification is activated. Off = Identification is deactivated.</td>
</tr>
<tr>
<td>2</td>
<td>Power/Standby LED</td>
<td>Green = System is on. Amber = System is in standby, but power is still applied. Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed, facility power is not available.</td>
</tr>
<tr>
<td>3</td>
<td>Aggregate Network LED</td>
<td>Solid green = Link to network. Flashing green = Network activity. Off = No network connection</td>
</tr>
<tr>
<td>4</td>
<td>System Health LED</td>
<td>Green = System health is normal. Amber = System health is degraded. Red = System health is critical. Off = System health is normal (when in standby mode).</td>
</tr>
</tbody>
</table>

The components on the rear panel are illustrated in Figure 4.

![Figure 4 – Rear Panel Components](image2)
Descriptions of components on the rear panel are given in Table 4.

**Table 4 – Rear Panel Components Descriptions**

<table>
<thead>
<tr>
<th>Item</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Slot 2 PCIe 3.0 x 16 (Blocked)</td>
</tr>
<tr>
<td>2</td>
<td>NIC 4 connector (Disabled)</td>
</tr>
<tr>
<td></td>
<td>NIC 3 connector (Disabled)</td>
</tr>
<tr>
<td></td>
<td>NIC 2 connector</td>
</tr>
<tr>
<td></td>
<td>NIC 1 connector</td>
</tr>
<tr>
<td>3</td>
<td>Video connector</td>
</tr>
<tr>
<td>4</td>
<td>Serial connector</td>
</tr>
<tr>
<td>5</td>
<td>Slot 1 PCIe 3.0 x 8 (Blocked)</td>
</tr>
<tr>
<td>6</td>
<td>iLO 3/NIC connector (Blocked)</td>
</tr>
<tr>
<td>7</td>
<td>USB connectors (4) (Blocked)</td>
</tr>
<tr>
<td>8</td>
<td>Power supply bay 2</td>
</tr>
<tr>
<td>9</td>
<td>Power supply bay 1</td>
</tr>
</tbody>
</table>

The three LEDs on the rear panel are illustrated in Figure 5.

![Figure 5 – Rear Panel LEDs](image)

Descriptions of LEDs on the rear panel are given in Table 5.

**Table 5 – Rear Panel LED Definitions**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Standard NIC activity LED for NIC 1 and NIC 2</td>
<td>Green = Activity exists.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flashing green = Activity exists.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off = No activity exists.</td>
</tr>
<tr>
<td>2</td>
<td>Standard NIC link LED for NIC 1 and NIC 2</td>
<td>Green = Link exists.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off = No link exists.</td>
</tr>
<tr>
<td>3</td>
<td>UID LED/button</td>
<td>Solid blue = Identification is activated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off = Identification is deactivated.</td>
</tr>
</tbody>
</table>
2.4 Roles, Services, and Authentication

The module supports four authorized roles:

- Crypto-Officer
- User
- HP User
- Cluster Member

All roles require identity-based authentication.

2.4.1 Crypto-Officer Role

The Crypto-Officer accesses the module via the Web Management Console and/or the Command Line Interface (CLI). This role provides all services that are necessary for the secure management of the module. Table 6 shows the services for the Crypto-Officer role under the FIPS mode of operation. The purpose of each service is shown in the first column (“Service”), and the corresponding function is described in the second column (“Description”). The keys and Critical Security Parameters (CSPs) in the rightmost column correspond to the keys and CSPs introduced in Section 2.7.1.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Keys/CSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate to ESKM</td>
<td>Authenticate to ESKM with a username and the associated password</td>
<td>Crypto-Officer passwords – read;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TLS/SSH keys – read</td>
</tr>
<tr>
<td>Perform first-time</td>
<td>Configure the module when it is used for the first time</td>
<td>Crypto-Officer (admin) password – write;</td>
</tr>
<tr>
<td>initialization</td>
<td></td>
<td>Krsa private – write;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Krsa private – write;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log signing RSA key – write;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log signature verification RSA key – write;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KRsaPub – write;</td>
</tr>
<tr>
<td>Upgrade firmware</td>
<td>Upgrade firmware (firmware must be FIPS-validated)</td>
<td>Firmware upgrade key – read</td>
</tr>
<tr>
<td>Configure FIPS mode</td>
<td>Enable/disable FIPS mode</td>
<td>None</td>
</tr>
<tr>
<td>Manage keys</td>
<td>Manage all client keys that are stored within the module. This includes the</td>
<td>Client keys – write, read, delete;</td>
</tr>
<tr>
<td></td>
<td>generation, storage, export (only public keys), import, and zeroization of</td>
<td>PKEK – write, read, delete.</td>
</tr>
<tr>
<td></td>
<td>keys.</td>
<td></td>
</tr>
<tr>
<td>Manage clusters</td>
<td>Manage all clusters that are defined within the module. This includes the</td>
<td>Cluster Member passwords – write, delete</td>
</tr>
<tr>
<td></td>
<td>creation, joining, and removal of a cluster from the module.</td>
<td>Cluster key – write, read, delete</td>
</tr>
<tr>
<td>Manage services</td>
<td>Manage all services supported by the module. This includes the starting and</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>stopping of all services.</td>
<td></td>
</tr>
<tr>
<td>Manage operators</td>
<td>Create, modify, or delete module operators (Crypto-Officers and Users).</td>
<td>Crypto-Officer passwords – write, delete; User passwords – write, delete</td>
</tr>
<tr>
<td>Service</td>
<td>Description</td>
<td>Keys/CSPs</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>Manage certificates</td>
<td>Create/import/revoke certificates</td>
<td>KRsaPub – write, read, delete;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KRsaPriv – write, read, delete;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARsaPub – write, read, delete;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARsaPriv – write, read, delete;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Client RSA public keys – read.</td>
</tr>
<tr>
<td>Reset factory settings</td>
<td>Rollback to the default firmware shipped with</td>
<td>All RSA keys/CSPs – delete</td>
</tr>
<tr>
<td></td>
<td>the module</td>
<td></td>
</tr>
<tr>
<td>Restore default</td>
<td>Delete the current configuration file and</td>
<td>None</td>
</tr>
<tr>
<td>configuration</td>
<td>restores the default configuration settings</td>
<td></td>
</tr>
<tr>
<td>Restore configuration</td>
<td>Restore a previously backed up configuration file</td>
<td>None</td>
</tr>
<tr>
<td>file</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup configuration</td>
<td>Back up a configuration file</td>
<td>None</td>
</tr>
<tr>
<td>file</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zeroize all keys/CSPs</td>
<td>Zeroize all keys and CSPs in the module</td>
<td>All RSA keys and CSPs – delete</td>
</tr>
</tbody>
</table>
2.4.2 User Role

The User role is associated with external applications or clients that connect to the KMS via its XML interface. Users in this role may exercise services—such as key generation and management—based on configured or predefined permissions. See Table 7 for details. The keys and CSPs in the rightmost column correspond to the keys and CSPs introduced in Section 2.7.1.

Table 7 – User Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Keys/CSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate to ESKM</td>
<td>Authenticate to ESKM with a username and the associated password</td>
<td>User passwords – read</td>
</tr>
<tr>
<td>Generate key</td>
<td>Generate a cryptographic key</td>
<td>Client keys – write;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PKEK – write.</td>
</tr>
<tr>
<td>Modify key meta data</td>
<td>Change the key owner or update/add/delete the custom attributes</td>
<td>None</td>
</tr>
<tr>
<td>Delete key</td>
<td>Delete a cryptographic key</td>
<td>Client keys – delete;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PKEK – delete.</td>
</tr>
<tr>
<td>Query key meta data</td>
<td>Output key names and meta data that the User is allowed to access</td>
<td>Client keys – read;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PKEK – read.</td>
</tr>
<tr>
<td>Import key</td>
<td>Import key</td>
<td>Client keys – write;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PKEK – write.</td>
</tr>
<tr>
<td>Export key</td>
<td>Export a cryptographic key</td>
<td>Client keys – read;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PKEK – read.</td>
</tr>
<tr>
<td>Export certificate</td>
<td>Export a certificate</td>
<td>Client certificate – read</td>
</tr>
<tr>
<td>Get certificate info</td>
<td>Return a list of local CAs including the certificate status</td>
<td>None</td>
</tr>
<tr>
<td>Clone key</td>
<td>Clone an existing key under a different key name</td>
<td>Client keys – write,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>read; PKEK – write, read.</td>
</tr>
<tr>
<td>Generate random number</td>
<td>Generate a random number</td>
<td>DRBG seed – write, read, delete</td>
</tr>
<tr>
<td>Manage operators</td>
<td>Only users with administration permission can create, modify, or delete</td>
<td>User passwords – write, delete</td>
</tr>
<tr>
<td></td>
<td>module operators</td>
<td></td>
</tr>
<tr>
<td>Sign certificate request</td>
<td>Only users with administration permission can sign certificate requests</td>
<td>Client RSA public key;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARsaPub – read;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARsaPriv – read.</td>
</tr>
</tbody>
</table>
2.4.3 HP User Role

The HP User role can reset the module to an uninitialized state in the event that all Crypto-Officer passwords are lost, or when a self-test permanently fails. See Table 8. The keys and CSPs in the rightmost column correspond to the keys and CSPs introduced in Section 2.7.1.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Keys/CSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate to the module</td>
<td>Authenticate to ESKM with a signed token</td>
<td>HP User RSA public key – read</td>
</tr>
<tr>
<td>Reset factory settings</td>
<td>Rollback to the default firmware shipped with the module</td>
<td>All keys/CSPs – delete</td>
</tr>
<tr>
<td>Restore default configuration</td>
<td>Delete the current configuration file and restores the default configuration settings</td>
<td>None</td>
</tr>
<tr>
<td>Zeroize all keys/CSPs</td>
<td>Zeroize all keys/CSPs in the module</td>
<td>All keys/CSPs – delete</td>
</tr>
</tbody>
</table>

2.4.4 Cluster Member Role

The Cluster Member role is associated with other ESKMs that can connect to this ESKM and access cluster services. See Table 9. The keys and CSPs in the rightmost column correspond to the keys and CSPs introduced in Section 2.7.1.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Keys/CSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate Cluster Member</td>
<td>Authenticate to ESKM via TLS</td>
<td>Cluster Member passwords – read; Cluster key – read; Cluster Member RsaPub – read</td>
</tr>
<tr>
<td>Receive Configuration File</td>
<td>Update the module’s configuration settings</td>
<td>None</td>
</tr>
<tr>
<td>Zeroize Key</td>
<td>Delete a specific key</td>
<td>Cluster key – delete</td>
</tr>
<tr>
<td>Backup Configuration File</td>
<td>Back up a configuration file</td>
<td>None</td>
</tr>
</tbody>
</table>

2.4.5 Authentication

The module performs identity-based authentication for the four roles. Two authentication schemes are used: authentication with certificate in TLS and authentication with password. See Table 10 for a detailed description.

<table>
<thead>
<tr>
<th>Role</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto-Officer</td>
<td>Username and password with optional digital certificate</td>
</tr>
<tr>
<td>User</td>
<td>Username and password and/or digital certificate</td>
</tr>
<tr>
<td>HP User</td>
<td>Digital certificate</td>
</tr>
<tr>
<td>Cluster Member</td>
<td>Digital certificate</td>
</tr>
</tbody>
</table>
The 1024-bit RSA signature on a digital certificate provides 80-bits of security. There are $2^{80}$ possibilities. The probability of a successful random guess is $2^{-80}$. Since $10^{-6} \gg 2^{-80}$, a random attempt is very unlikely to succeed. At least 80 bits of data must be transmitted for one attempt. (The actual number of bits that need to be transmitted for one attempt is much greater than 80. We are considering the worst case scenario. Note also that the 1024-bit signature verification option is only available to the User role; all other roles require 2048-bit digital certificates.) The processor used by the module has a working frequency of 2.5 gigabytes, hence, at most $60 \times 2.5 \times 10^9$ bits of data can be transmitted in 60 seconds. Since 80 bits are necessary for one attempt, at most $(60 \times 2.5 \times 10^9)/80 = 1.875 \times 10^9$ attempts are possible in 60 seconds. However, there exist $2^{80}$ possibilities. $(1.875 \times 10^9)/2^{80} = 1.55 \times 10^{-15} \ll 10^{-5}$. The probability of a successful certificate attempt in 60 seconds is considerably less than $10^{-5}$.

Passwords in the module must consist of eight or more characters from the set of 90 human-readable numeric, alphabetic (upper and lower case), and special character symbols. Excluding those combinations that do not meet password constraints (see Section 2.7.1 – Keys and CSPs), the size of the password space is about $60^8$. The probability of a successful random guess is $60^{-8}$. Since $10^{-6} \gg 5 \times 60^{-8}$, the probability of a successful password attempt in 60 seconds is considerably less than $10^{-6}$.

2.4.6 Unauthenticated Services

The following services do not require authentication:

- SNMP statistics
- FIPS status services
- Health check services
- Network Time Protocol (NTP) services
- Initiation of self-tests by rebooting the ESKM
- Negotiation of the XML protocol version for communications with the KMS

SNMP is used only for sending statistical information (SNMP traps). FIPS status and health check are status-report services, unrelated to security or cryptography. NTP is a date/time synchronization service that does not involve keys or CSPs. Initiation of self-tests and negotiation of the XML protocol version do not involve keys or CSPs.

The services listed above for each role comprise the entire set of services available in non-FIPS mode.

2.5 Physical Security

The module was tested and found conformant to the EMI/EMC requirements specified by Title 47 of the Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (that is, for business use).

The HP Enterprise Secure Key Manager is a multi-chip standalone cryptographic module. The entire contents of the module, including all hardware, software, firmware, and data, are enclosed in a metal case. The case is opaque and must be sealed using tamper-evident labels in order to prevent the case cover from being removed without signs of tampering. Two pick-resistant locks are installed on the module’s front bezel to protect the front interfaces, including the power switch, from unauthorized access. All circuits in the module are coated with commercial standard passivation. Once the bezel is locked and the module has been configured to meet FIPS 140-2 Level 2 requirements, the module cannot be accessed without signs of tampering. See Section 3.3 – Physical Security Assurance of this document for more information.
2.6 Operational Environment

The operational environment requirements do not apply to the HP Enterprise Secure Key Manager—the module does not provide a general purpose operating system and only allows the updating of image components after checking an RSA signature on the new firmware image. Crypto-Officers can install a new firmware image on the ESKM by downloading the image to the ESKM. This image is signed by an RSA private key (which never enters the module). The ESKM verifies the signature on the new firmware image using the public key stored in the module. If the verification passes, the upgrade is allowed. Otherwise the upgrade process fails and the old image is reused.

2.7 Cryptographic Key Management

2.7.1 Keys and CSPs

The SSH and TLS protocols employed by the FIPS mode of the module are security-related. Table 11 and
Table 12 introduce cryptographic keys, key components, and CSPs involved in the two protocols, respectively.

### Table 11 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs for SSH

<table>
<thead>
<tr>
<th>Key</th>
<th>Key Type</th>
<th>Generation / Input</th>
<th>Output</th>
<th>Storage</th>
<th>Zeroization</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>DH public</td>
<td>2048-bit Diffie-Hellman public parameters</td>
<td>Generated by DRBG during session initialization</td>
<td>In plaintext</td>
<td>In volatile memory</td>
<td>Upon session termination</td>
<td>Negotiate SSH Ks and SSH Khmac</td>
</tr>
<tr>
<td>DH private</td>
<td>256-bit Diffie-Hellman private parameters</td>
<td>Generated by DRBG during session initialization</td>
<td>Never</td>
<td>In volatile memory</td>
<td>Upon session termination</td>
<td>Negotiate SSH Ks and SSH Khmac</td>
</tr>
<tr>
<td>Krsa public</td>
<td>2048-bit RSA public keys</td>
<td>Generated by DRBG during first-time initialization</td>
<td>In plaintext</td>
<td>In non-volatile memory</td>
<td>At operator delete or zeroize request</td>
<td>Verify the signature of the server’s message.</td>
</tr>
<tr>
<td>Krsa private</td>
<td>2048-bit RSA private keys</td>
<td>Generated by DRBG during first-time initialization</td>
<td>Never</td>
<td>In non-volatile memory</td>
<td>At operator delete or zeroize request</td>
<td>Sign the server’s message.</td>
</tr>
<tr>
<td>SSH Ks</td>
<td>SSH session 168-bit TDES key, 128-, 192-, 256-bit AES key</td>
<td>Diffie-Hellman key agreement</td>
<td>Never</td>
<td>In volatile memory</td>
<td>Upon session termination or when a new Ks is generated (after a certain timeout)</td>
<td>Encrypt and decrypt data</td>
</tr>
<tr>
<td>SSH Khmac</td>
<td>SSH session 512-bit HMAC key</td>
<td>Diffie-Hellman key agreement</td>
<td>Never</td>
<td>In volatile memory</td>
<td>Upon session termination or when a new Khmac is generated (after a certain timeout)</td>
<td>Authenticate data</td>
</tr>
</tbody>
</table>

Notice that SSH version 2 is explicitly accepted for use in FIPS mode, according to section 7.1 of the NIST FIPS 140-2 Implementation Guidance.
### Table 12 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs for TLS

<table>
<thead>
<tr>
<th>Key</th>
<th>Key Type</th>
<th>Generation / Input</th>
<th>Output</th>
<th>Storage</th>
<th>Zeroization</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-MS TLS pre-master secret</td>
<td>Input in encrypted form from client</td>
<td>Never</td>
<td>In volatile memory</td>
<td>Upon session termination</td>
<td>Derive MS</td>
<td></td>
</tr>
<tr>
<td>MS TLS master secret</td>
<td>Derived from Pre-MS using FIPS Approved key derivation function</td>
<td>Never</td>
<td>In volatile memory</td>
<td>Upon session termination</td>
<td>Derive TLS Ks and TLS Khmac</td>
<td></td>
</tr>
<tr>
<td>KRsaPub Server RSA public key (2048-bit)</td>
<td>Generated by DRBG during first-time initialization</td>
<td>In plaintext</td>
<td>In non-volatile memory</td>
<td>At operator delete request</td>
<td>Client encrypts Pre-MS. Client verifies server signatures</td>
<td></td>
</tr>
<tr>
<td>KRsaPriv Server RSA private key (2048-bit)</td>
<td>Generated by DRBG during first-time initialization</td>
<td>Never</td>
<td>In non-volatile memory</td>
<td>At operator delete or zeroize request</td>
<td>Server decrypts Pre-MS. Server generates signatures</td>
<td></td>
</tr>
<tr>
<td>CARsaPub Certificate Authority (CA) RSA public key (2048-bit)</td>
<td>Generated by DRBG during first-time initialization</td>
<td>In plaintext</td>
<td>In non-volatile memory</td>
<td>At operator delete request</td>
<td>Verify CA signatures</td>
<td></td>
</tr>
<tr>
<td>CARsaPriv CA RSA private key (2048-bit)</td>
<td>Generated by DRBG during first-time initialization</td>
<td>Never</td>
<td>In non-volatile memory</td>
<td>At operator delete or zeroize request</td>
<td>Sign server certificates</td>
<td></td>
</tr>
<tr>
<td>Cluster Member RsaPub Cluster Member RSA public key (2048-bit)</td>
<td>Input in plaintext</td>
<td>Never</td>
<td>In volatile memory</td>
<td>Upon session termination</td>
<td>Verify Cluster Member signatures</td>
<td></td>
</tr>
<tr>
<td>TLS Ks TLS session AES or TDES symmetric key(s)</td>
<td>Derived from MS</td>
<td>Never</td>
<td>In volatile memory</td>
<td>Upon session termination</td>
<td>Encrypt and decrypt data</td>
<td></td>
</tr>
<tr>
<td>TLS Khmac TLS session HMAC key</td>
<td>Derived from MS</td>
<td>Never</td>
<td>In volatile memory</td>
<td>Upon session termination</td>
<td>Authenticate data</td>
<td></td>
</tr>
</tbody>
</table>

Table 13 details all cipher suites supported by the TLS protocol implemented by the module. The suite names in the first column match the definitions in RFC 2246 and RFC 4346.

### Table 13 – Cipher Suites Supported by the Module’s TLS Implementation in FIPS Mode

<table>
<thead>
<tr>
<th>Suite Name</th>
<th>Authentication</th>
<th>Key Transport</th>
<th>Symmetric Cryptography</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA</td>
<td>RSA</td>
<td>RSA</td>
<td>AES (256-bit)</td>
<td>SHA-1</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>RSA</td>
<td>RSA</td>
<td>AES (128-bit)</td>
<td>SHA-1</td>
</tr>
<tr>
<td>TLS_RSA_WITH_TDES_EDE_CBC_SHA</td>
<td>RSA</td>
<td>RSA</td>
<td>TDES (168-bit)</td>
<td>SHA-1</td>
</tr>
</tbody>
</table>
Other CSPs are tabulated in Table 14.

<table>
<thead>
<tr>
<th>Key</th>
<th>Key Type</th>
<th>Generation / Input</th>
<th>Output</th>
<th>Storage</th>
<th>Zeroization</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client AES key</td>
<td>128, 192 or 256-bit AES key</td>
<td>Generated by DRBG</td>
<td>Via TLS in encrypted form (encrypted with TLS Ks) per client's request</td>
<td>Encrypted in non-volatile memory</td>
<td>Per client's request or zeroize request</td>
<td>Encrypt plaintexts/decrypt ciphertexts</td>
</tr>
<tr>
<td>Client TDES key</td>
<td>TDES key</td>
<td>Generated by DRBG</td>
<td>Via TLS in encrypted form (encrypted with TLS Ks) per client's request</td>
<td>Encrypted in non-volatile memory</td>
<td>Per client's request or zeroize request</td>
<td>Encrypt plaintexts/decrypt ciphertexts</td>
</tr>
<tr>
<td>Client RSA public keys</td>
<td>RSA public key</td>
<td>Generated by DRBG</td>
<td>Via TLS in encrypted form (encrypted with TLS Ks) per client's request</td>
<td>Encrypted in non-volatile memory</td>
<td>At operator delete</td>
<td>Sign messages/verify signatures</td>
</tr>
<tr>
<td>Client RSA keys</td>
<td>RSA private keys</td>
<td>Generated by DRBG</td>
<td>Via TLS in encrypted form (encrypted with TLS Ks) per client's request</td>
<td>Encrypted in non-volatile memory</td>
<td>Per client's request or zeroize request</td>
<td>Sign messages/verify signatures</td>
</tr>
<tr>
<td>Client HMAC keys</td>
<td>HMAC keys</td>
<td>Generated by DRBG</td>
<td>Via TLS in encrypted form (encrypted with TLS Ks) per client's request</td>
<td>Encrypted in non-volatile memory</td>
<td>Per client's request or zeroize request</td>
<td>Compute keyed-MACs</td>
</tr>
<tr>
<td>Client certificate</td>
<td>X.509 certificate</td>
<td>Input in ciphertext over TLS</td>
<td>Via TLS in encrypted form (encrypted with TLS Ks) per client's request</td>
<td>In non-volatile memory</td>
<td>Per client's request or by zeroize request</td>
<td>Encrypt data/verify signatures</td>
</tr>
<tr>
<td>Crypto-Officer passwords</td>
<td>Character string</td>
<td>Input in ciphertext over TLS</td>
<td>Never</td>
<td>In non-volatile memory</td>
<td>At operator delete or by zeroize request</td>
<td>Authenticate Crypto-Officer</td>
</tr>
<tr>
<td>User passwords</td>
<td>Character string</td>
<td>Input in ciphertext over TLS</td>
<td>Never</td>
<td>In non-volatile memory</td>
<td>At operator delete or by zeroize request</td>
<td>Authenticate User</td>
</tr>
<tr>
<td>Cluster Member password</td>
<td>Character string</td>
<td>Input in ciphertext over TLS</td>
<td>Never</td>
<td>In non-volatile memory</td>
<td>At operator delete or by zeroize request</td>
<td>When a device attempts to become a Cluster Member</td>
</tr>
<tr>
<td>HP User RSA public key</td>
<td>2048-bit RSA public key</td>
<td>Input in plaintext at factory</td>
<td>Never</td>
<td>In non-volatile memory</td>
<td>At installation of a patch or new firmware</td>
<td>Authenticate HP User</td>
</tr>
<tr>
<td>Cluster key</td>
<td>Character string</td>
<td>Input in ciphertext over TLS</td>
<td>Via TLS in encrypted form</td>
<td>In non-volatile memory</td>
<td>At operator delete or by zeroize request</td>
<td>Authenticate Cluster Member</td>
</tr>
</tbody>
</table>
### Key Generation

The module uses the DRBG (AES in CTR mode) as specified in SP 800-90A to generate cryptographic keys. This DRBG is a FIPS 140-2 Approved RNG as specified in Annex C to FIPS 140-2.

### Key/CSP Zeroization

All ephemeral keys are stored in volatile memory in plaintext. Ephemeral keys are zeroized when they are no longer used. Other keys and CSPs are stored in non-volatile memory with client keys being stored in encrypted form.

To zeroize all keys and CSPs in the module, the Crypto-Officer should execute the reset factory settings zeroize command at the serial console interface. For security reasons, this command is available only through the serial console.

### Self-Tests

The device implements two types of self-tests: power-up self-tests and conditional self-tests.

Power-up self-tests include the following tests:

- Firmware integrity tests (CRC-16 and RSA 2048-bit signature verification)
- Known Answer Test (KAT) on TDES
- KAT on AES
- KAT on SHA-1
- KAT on SHA-256
- KAT on SHA-384
- KAT on SHA-512
- KAT on HMAC SHA-1
- KAT on HMAC SHA-256
- KAT on DRBG
- KAT on Diffie-Hellman
- KAT on SSH Key Derivation Function
- KAT on RSA signature generation and verification
Conditional self-tests include the following tests:

- Pairwise consistency test for new RSA keys
- Continuous random number generator test on DRBG
- Continuous random number generator test on non-Approved RNG
- Firmware load test (RSA 2048-bit signature verification)
- Diffie-Hellman primitive test

The module has two error states: a Soft Error state and a Fatal Error state. When one or more power-up self-tests fail, the module may enter either the Fatal Error state or the Soft Error State. When a conditional self-test fails, the module enters the Soft Error state. See Section 3 of this document for more information.

2.9 Mitigation of Other Attacks

This section is not applicable. No claim is made that the module mitigates against any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.
3 Secure Operation

The HP Enterprise Secure Key Manager meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in the FIPS mode of operation.

3.1 Initial Setup

The device should be unpacked and inspected according to the Installation Guide. The Installation Guide also contains installation and configuration instructions, maintenance information, safety tips, and other information.

3.2 Initialization and Configuration

3.2.1 First-Time Initialization

When the module is turned on for the first time, it will prompt the operator for a password for a default Crypto-Officer. The module cannot proceed to the next state until the operator provides a password that conforms to the password policy described in Section 2.7.1. The default username associated with the entered password is “admin”.

During the first-time initialization, the operator must configure minimum settings for the module to operate correctly. The operator will be prompted to configure the following settings via the serial interface:

- Date, Time, Time zone
- IP Address/Netmask
- Hostname
- Gateway
- Management Port

3.2.2 FIPS Mode Configuration

In order to comply with FIPS 140-2 Level 2 requirements, the following functionality must be disabled on the ESKM:

- Global keys
- File Transfer Protocol (FTP) for importing certificates and downloading and restoring backup files
- Lightweight Directory Access Protocol (LDAP) authentication
- Use of the following algorithms: RC4, MD5, DES, RSA-512, RSA-768, RSA-1024 (signature generation)
- SSL 3.0
- RSA encryption and decryption operations (note, however, that RSA encryption and decryption associated with TLS handshakes and Sign and Sign Verify are permitted)

These functions need not be disabled individually. There are two approaches to configuring the module such that it works in the Approved FIPS mode of operation:

Through a command line interface, such as SSH or serial console, the Crypto-Officer should use the fips compliant command to enable the FIPS mode of operation. This will alter various server settings as described above. See Figure 6. The fips server command is used for the FIPS status server configuration. The show fips status command returns the current FIPS mode configuration.
In the web administration interface, the Crypto-Officer should use the “High Security Configuration” page to enable and disable FIPS compliance. To enable the Approved FIPS mode of operation, click on the “Set FIPS Compliant” button. See Figure 7. This will alter various server settings as described above.

```
labhp (config)# fips compliant
This device is now FIPS compliant.
labhp (config)# fips server
Enable FIPS Status Server [y]:
Available IP addresses:
  1. All
  2. 192.168.0.202
Local IP (1-2) [1]:
Local Port [5004]:
labhp (config)# show fips status
FIPS Compliant: Yes
```

**Figure 6 – FIPS Compliance in CLI**

In the web administration interface, the User can review the FIPS mode configuration by reading the “High Security Configuration” page.

The Crypto-Officer must zeroize all keys when switching from the Approved FIPS mode of operation to the non-FIPS mode and vice versa.

### 3.3 Physical Security Assurance

Five (5) serialized tamper-evidence labels have been applied during manufacturing on the metal casing. See Figure 8. The tamper-evidence labels have a special adhesive backing to adhere to the module’s surface and have an individual, unique serial number. They should be inspected periodically and compared to the previously-recorded serial number to verify that fresh labels have not been applied to a tampered module. If the labels show evidence of tamper, the Crypto-Officer should assume that the module has been compromised and contact HP Customer Support.
Figure 8 – Tamper-Evidence Labels (Qty. 5) on ESKM

Figure 9 – Tamper-Evidence Label on top of ESKM

Figure 10 – Tamper-Evidence Labels on Side of ESKM
3.4 Key and CSP Zeroization

To zeroize all keys and CSPs in the module, the Crypto-Officer should execute reset factory settings zeroize command in the serial console interface. Notice that, for security reasons, the command cannot be initiated from the SSH interface.

When switching between different modes of operations (FIPS and non-FIPS), the Crypto-Officer must zeroize all CSPs.

3.5 Error State

The module has two error states: a Soft Error state and a Fatal Error state.

When a power-up self-test fails, the module may enter either the Fatal Error state or the Soft Error State. When a conditional self-test fails, the module will enter the Soft Error state. The module can recover from the Fatal Error state if power is cycled or if the ESKM is rebooted. An HP User can reset the module when it is in the Fatal Error State. No other services are available in the Fatal Error state. The module can recover from the Soft Error state if power is cycled. With the exception of the firmware load test and Diffie-Hellman primitive test, the only service that is available in the Soft Error state is the FIPS status output via port 9081 (default). A User can connect to port 9081 and find the error message indicating the failure of FIPS self-tests. Access to port 9081 does not require authentication.
## Acronyms

### Table 15 – Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standard Institute</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input/Output System</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CBC</td>
<td>Cipher Block Chaining</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>CMVP</td>
<td>Cryptographic Module Validation Program</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>CSP</td>
<td>Critical Security Parameter</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DRBG</td>
<td>Deterministic Random Bit Generator</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
</tr>
<tr>
<td>ECB</td>
<td>Electronic Codebook</td>
</tr>
<tr>
<td>EMC</td>
<td>Electromagnetic Compatibility</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
</tr>
<tr>
<td>ESKM</td>
<td>Enterprise Secure Key Manager</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Drive</td>
</tr>
<tr>
<td>HMAC</td>
<td>Keyed-Hash Message Authentication Code</td>
</tr>
<tr>
<td>HP</td>
<td>Hewlett-Packard</td>
</tr>
<tr>
<td>IDE</td>
<td>Integrated Drive Electronics</td>
</tr>
<tr>
<td>iLO</td>
<td>Integrated Lights-Out</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISA</td>
<td>Instruction Set Architecture</td>
</tr>
<tr>
<td>KAT</td>
<td>Known Answer Test</td>
</tr>
<tr>
<td>KMS</td>
<td>Key Management Service</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>N/A</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>PCI</td>
<td>Peripheral Component Interconnect</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments</td>
</tr>
<tr>
<td>RNG</td>
<td>Random Number Generator</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, and Adleman</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TDES</td>
<td>Triple Data Encryption Standard</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>UID</td>
<td>Unit Identifier</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>VGA</td>
<td>Video Graphics Array</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>