Digi Passport™

FIPS 140-2 Non-Proprietary

Security Policy

Hardware version : **Digi Passport 4 FIPS rev. 1.1**
Digi Passport 8 FIPS rev. 1.1
Digi Passport 16 2AC FIPS rev. 1.1
Digi Passport 32 2 AC FIPS rev. 1.1
Digi Passport 48 2AC FIPS rev. 1.1

Firmware version : **1.2.0F**

Document rev. 1.3

Digi International

Revision History

Revision	Name	Date	Section	Changes
1.0	Brian O'rourke	Aug. 25, 2008	All	Initial Release
1.1	Brian O'rourke	Jan. 20, 2009		Reflected comments from CMVP.
1.2	Brian O'rourke	June 4, 2009		Reflected comments from CMVP.
1.3	Brian O'rourke	June 24, 2009		Reflected comments from CMVP.

Contents

1. Introduction

This document describes the Security Policy for the following Digi Passport console servers.

- Digi Passport 4 FIPS (Part number : 70002373)
- Digi Passport 8 FIPS (Part number : 70002374)
- Digi Passport 16 2 AC FIPS (Part number : 70002375)
- Digi Passport 32 2 AC FIPS (Part number : 70002376)
- Digi Passport 48 2 AC FIPS (Part number : 70002377)

With the Digi Passport unit, administrators can securely monitor and control servers, routers, switches, and other network devices from anywhere on the corporate TCP/IP network, over the Internet, or through dial-up modem connections even when the server is unavailable through the network. These capabilities combined with FIPS 140-2 Level 2 compliance make the Digi Passport an ideal choice for providing secure in-band and out-of-band remote access solution in a variety of environments.

1.1. Purpose

This document is intended for describing the Security Policy for the Digi Passport console servers. The Digi Passport provides secure remote access to the console ports of computer systems and network equipment over Ethernet or dial-up connections. This Security Policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

1.2. References

For more information on the full line of products from Digi International, please visit http://www.digi.com. For more information on NIST and the cryptographic module validation program, please visit http://csrc.nist.gov/groups/STM/cmvp/index.html.

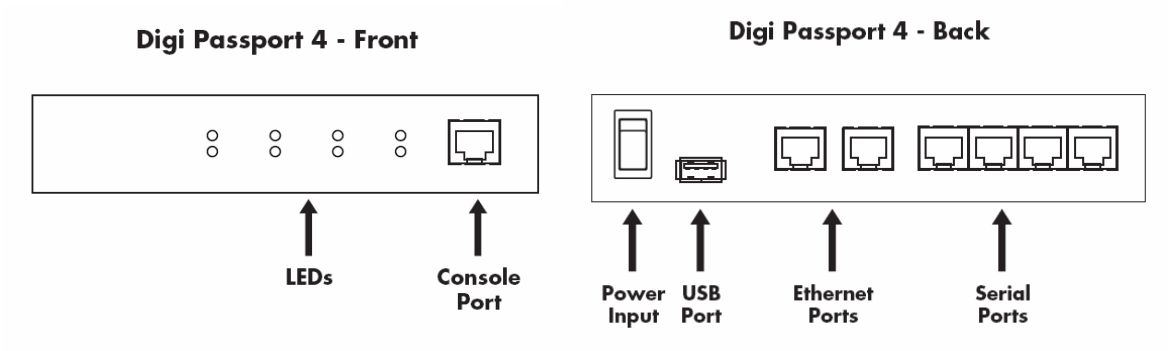
2. Ports and Interfaces

2.1. Physical ports and interfaces

The Digi Passport is a multi-chip standalone module and the cryptographic boundary of the module is defined by the outer case of module. The module provides a number of physical ports and interfaces to the device. The module conforms to the EMI/EMC standards specified by FCC Part 15, Subpart B, Class A.

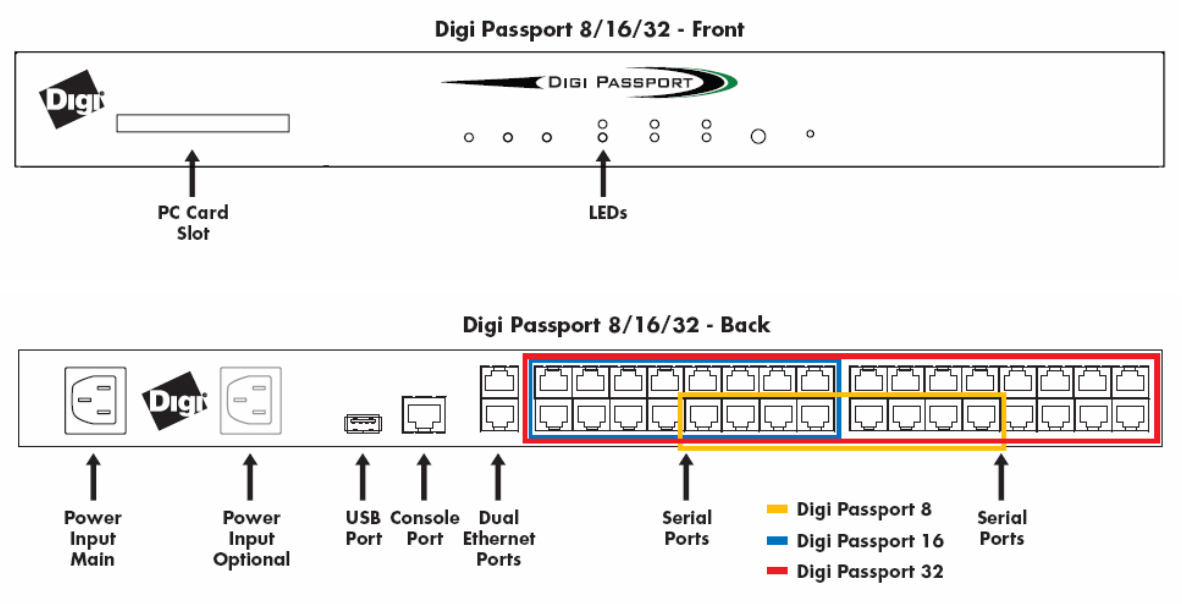
2.1.1. Digi Passport 4 FIPS

- Single DC input from external 5V/4A adapter
- 4 RJ45 RS-232 serial ports
- 1 RJ45 RS232 console port
- 2 RJ45 10/100 Mbps Ethernet ports
- 1 USB 2.0 port



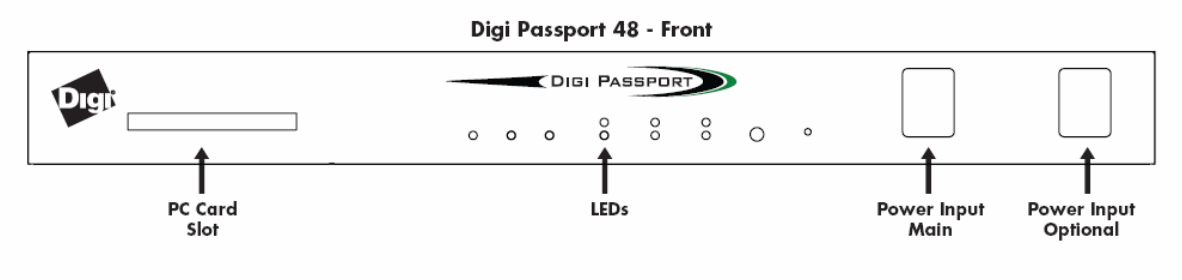
2.1.2. Digi Passport 8 FIPS/16 2AC FIPS/32 2AC FIPS

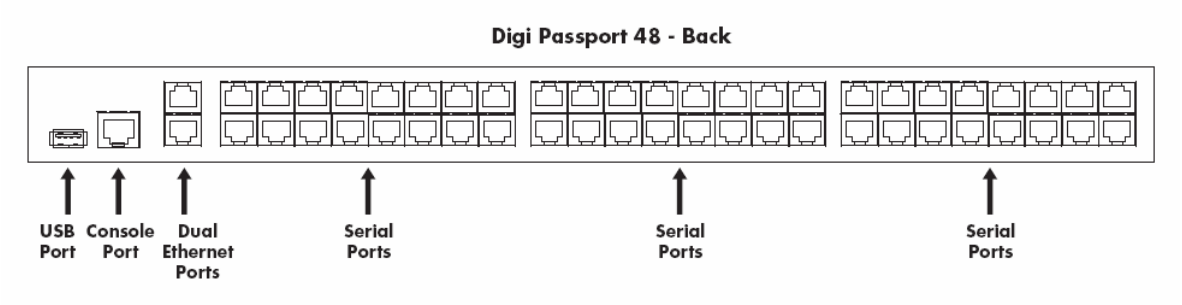
- Single AC input for the Digi Passport 8 and Dual AC inputs for the Digi Passport 16 2AC/32 2AC
- (8/16/32) RJ45 RS-232 serial ports
- 1 RJ45 RS232 console port
- 2 RJ45 10/100 Mbps Ethernet ports
- 1 USB 2.0 port
- 1 PC Card slot (not available in FIPS mode because function is disabled in FIPS mode and tamper evidence seal will be attached to the card slot)



2.1.3. Digi Passport 48 2AC FIPS

- Dual AC inputs
- 48 RJ45 RS-232 serial ports
- 1 RJ45 RS232 console port
- 2 RJ45 10/100 Mbps Ethernet ports
- 1 USB 2.0 port
- 1 PC Card slot (not available in FIPS mode because function is disabled in FIPS mode and tamper evidence seal will be attached to the card slot)





2.2. Ports and Interfaces mapping

The physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their module mapping are described in the following table.

FIPS 1402-2 Logical Interface	Digi Passport Physical Interface
Data Input Interface	2 10/100BASE-TX LAN Ports, 4/8/16/48 RS232 RJ45 Ports Console Port, USB Port
Data Output Interface	2 10/100BASE-TX LAN Ports, 4/8/16/48 RS232 RJ45 Ports Console Port, USB Port
Control Input Interface	Factory Reset Button 2 10/100BASE-TX LAN Ports, 4/8/16/48 RS232 RJ45 Ports, Console Port
Status Output Interface	LEDs, 4/8/16/48 RS232 RJ45 Ports 2 10/100BASE-TX LAN Ports, Console Port
Power Interface	Single DC Power Input / (Dual) AC Power Input

Each status output interface shows the information as follows,

- LEDs : Ready LED is used for indicating the status of module. If it is turned on steadily, it means the module is working properly. And if it is blinking, it means the module is performing power-on self tests or has some problems. If the module performs power-on self tests, Ready LED will blink with 1 second interval. And if any tests (power-on self tests or conditional self tests) are failed, Ready LED will blink with 2 second interval. USB, PC Card and Find LEDs will also blink with 2 second interval if the module fails any self tests.
- 4/8/16/48 RS232 RJ45 Ports : If the module is working properly, system admin user can access the module through modem connection to RS232 RJ45 ports and check the status of the module using system log or

statistics menu.

But if any tests (power-on self tests or conditional self tests) are failed, accessing the module through RS232 RJ45 ports will be blocked.

- LAN Ports : If the module is working properly, system admin user can access the module through SSH or HTTPS connection and check the status of the module using system log or statistics menu. But if any tests (power-on self tests or conditional self tests) are failed, accessing the module through LAN ports will be blocked.
- Console Port : If the module is working properly, system admin user can access the module through serial console port to check the status of the module using system log or statistics menu. But if any tests (power-on self tests or conditional self tests) are failed, user can only see the error message through serial console port and reboot the module.

3. Roles, Services and Authentication

3.1. Roles

The Digi Passport supports five different roles and each role has a specific set of services. A user is required to enter a password or to provide a certificate and to be authenticated to the system, and then explicitly to be assigned one either Crypto-Officer or User role as required by FIPS 140-2.
In general, the module can be accessed in one of the following ways,

- Serial console port
- HTTP
- HTTPS
- Telnet
- SSH
- SNMP v1/v2c/v3

But in a FIPS approved mode of operation, only the interfaces through the serial console port, HTTPS, SSH and SNMPv3 are enabled.

There are five main roles in the module classified by the services that operators can perform,

System admin user, Port admin user, User, Bios user, SNMP user.

These roles can be mapped to the FIPS140-2 authorized roles, Crypto-Officer role and User role, as shown below:

Role	FIPS 140-2 Mapping
System Admin user	Crypto-Officer
Bios user	Crypto-Officer
Port Admin user	Crypto-Officer
User	User
SNMP user	User

Each of these roles is described below,

3.1.1. System Admin User Role

The System Admin user is responsible for configuring the module properly. The System Admin user can access all the services available via the management interfaces. The System Admin user role can be accessed after supplying the correct username/password combination and passing the current authentication policy configured in the module. All System Admin users are responsible for ensuring that the module is configured properly to meet all FIPS 140-2 requirements.
Descriptions of the services available to the System Admin user are provided below,

- Changing general system configurations including authentication policy for the module, key generation, key enrollment, account management and configuration management.
- Changing serial port configurations including authentication policy for serial ports, access list for the serial ports and other serial ports related services.
- Monitoring system status
- Access serial ports
- Running self tests
- Performing firmware upgrade
- Performing zeroization

3.1.2. Bios User Role

The Bios user is responsible for enabling or disabling FIPS 140-2 mode. The Bios user role can be accessed only through the serial console port and accessing it through an Ethernet port is not allowed.
Descriptions of the services available to the Bios user are provided below,

- Enabling or disabling FIPS 140-2 mode.
- Managing the bios menu for testing hardware functionalities or setting the system clock.

3.1.3. Port Admin User Role

At some permission levels, an administrator can access only the configuration and

monitoring functions that the administrator with the highest level of permissions selects. It is possible to give other administrators the highest-level privileges.
The module implements a role called the Port Admin user. This role has limited rights on the system and is configured by the System Admin user. This role is disabled by default and the System Admin user has to enable them if needed.
The Port Admin user is responsible for configuring the serial port properly. The Port Admin user can access all the services for serial ports via the management interfaces.
Descriptions of the services available to the Port Admin user are provided below,

- Monitoring general system configurations
- Changing serial port configurations including authentication policy for serial ports, access list for the serial ports and other serial ports related services.
- Monitoring system status
- Access serial ports

3.1.4. User Role

User performs very limited set of services such as sending data through the serial ports and monitoring the serial port log data. All user roles are also assumed by supplying the correct authentication information. Users are authenticated to the module based on the authentication policy established by the System Admin user or the Port Admin.

3.1.5. SNMP User Role

Another special role defined in the module is the SNMP user. Although SNMPv3 traffic, which is the only SNMP protocol permitted in the FIPS mode of the module, is transmitted encrypted (using AES), for FIPS purposes, it is considered to be plaintext. (The reason being, encryption keys are derived from a pass phrase, which is not allowed in FIPS mode.) So SNMP user in the Digi Passport module cannot use the service that handles any sensitive data defined in Section 3.4.5.
Descriptions of the services available to the SNMP user are provided below,

- Changing general system configuration that does not handle any sensitive data.
- Changing serial port configuration that does not handle any sensitive data.
- Monitoring system status

3.2. Services

The services provided by the Digi Passport are listed in the following table. Some services may be performed only by Crypto Officer role.

In the table, the types of access are also identified per the explanation below,

R - The item is read or referenced by the service.

W - The item is written or updated by the service.

E - The item is executed by the service. (The item is used as part of a cryptographic function.)

Services	Roles	Keys or CSP used [**Types of Access**]
Accessing Module through Web UI	System Admin user Port Admin User	HTTPS(TLS) Web certificate [**R,E**] User Password (local authentication) [**R,E**] RADIUS/TACACS+ secret (remote authentication) [**R,E**]
Accessing module through SSH connection	System Admin user Port Admin User	SSH host keys[**R,E**] SSH Diffie-Hellman private key[**R,W,E**] SSH Session key [**R,W,E**] User Password (local authentication) [**R,E**] SSH user public key (public key authentication) [**R,E**] RADIUS/TACACS+ secret (remote authentication) [**R,E**]
Accessing module through serial console	System Admin user Port Admin	User Password (local authentication) [**R,E**] RADIUS/TACACS+ secret (remote authentication) [**R,E**]
Accessing module through SNMPv3 connection	SNMP User	SNMP v3 privacy/authentication password [**R,E**]
Accessing module through PPP connection	System Admin user Port Admin User	Incoming PAP/CHAP Secret [**R,E**] User Password (local authentication) [**R,E**] RADIUS/TACACS+ secret (remote authentication) [**R,E**]
Configuring module through clustering mode	System Admin user	Triple-DES static 192 bit key (2) [**R,E**]
Changing mode of operation	Bios User	Bios User Password [**R,W,E**]

Accessing bios menu of module	Bios User	Bios User Password [**R,W,E**]
Upgrading Firmware	System Admin user	HMAC-SHA-1 key [**R,W,E**]
Importing keys	System Admin user	HTTPS(TLS) Web certificate [**W**] SSH user public key [**W**] User Password[**W**] RADIUS/TACACS+ secret [**W**] Incoming PAP/CHAP Secret [**W**] Triple-DES static 192 bit key (1) [**W**] Triple-DES static 192 bit key (2) [**W**] SNMP v3 privacy/authentication password[**W**]
Exporting keys	System Admin user	RADIUS/TACACS+ secret [**R**] Triple-DES static 192 bit key (1) [**R**] Triple-DES static 192 bit key (2) [**R**]
Importing or exporting system configuration	System Admin user	Triple-DES static 192 bit key (1) [**R,E**] User Password[**R**/**W**] RADIUS/TACACS+ secret [**R**/**W**] Incoming PAP/CHAP Secret [**R**/**W**] Triple-DES static 192 bit key (2) [**R**/**W**] SSH host key[**R**/**W**] HTTPS(TLS) Web certificate [**R**/**W**] SSH user public key [**R**/**W**] SNMP v3 privacy/authentication password[**R**/**W**]
Changing system configuration	System Admin user	User Password[**W**] RADIUS/TACACS+ secret [**W**] Incoming PAP/CHAP Secret [**W**] Triple-DES static 192 bit key (1) [**W**] Triple-DES static 192 bit key (2) [**W**]
Changing serial port configuration	System Admin user Port Admin	None
SSH host key generation	System Admin user	SSH host keys[**W**]
Running self-tests	System Admin user	None

Performing zeroization	System Admin user	None

3.3. Authentication Mechanism

The module supports either a username password authentication or certificate based authentication. To access the Digi Passport, an operator (Crypto-Officer or User) must connect through Serial Port, SSH, or HTTPS. Except the case of using public key on SSH, an operator must provide a username and password.

Authentication Type	Strength
Username Password authentication	In FIPS mode, the passwords must be a minimum of 8 characters and they can consist of alphanumeric values (a-z, A-Z, 0-9) and non-alphabetic characters (more than 32 characters such as !,@,#,$). This yields 26+26+10+32 = 94 choices per character. Then the probability of a successful random attempt is 1/(94)^8, which is less than 1/1,000,000 for a single attempt. And if the authentication is failed 3 times consecutively in a session, authentication process will be blocked about 1 minute in case of Web UI or serial (console) access. In case of SSH connection (including connection through PPP), connection will be closed automatically if the authentication is failed 3 times consecutively. And an initial connection requires more than 1 second. So for single SSH connection attempt, user can attempt under 180 tries at best for guessing the password within one minute. And for multiple SSH connection attempts, the Digi Passport allows under 1000 connections at the same time because of memory limitation. (Each connection requires 300KB at minimum but the Digi Passport has 256MB or less memory.) Thus, user can attempt under 180*(256000/300)=153600 tries at best for guessing the password within one minute.

	But the number of possible password combinations of the Digi Passport in FIPS mode are over $(26+26+10+32)^8 \approx 6 \times 10^{15}$. So the authentication strength for multiple SSH connection is much less than 1/100,000. When user want to use remote authentication such as Radius, TACACS+, and Kerberos, user should ensure that the minimum length of password on the remote authentication server should be greater than or equals to 8 characters. If then, password strength for all cases can be kept to stronger than the requirement. And the same blocking mechanism for authentication failure, as well as the memory limitation, will be applied to the remote authentication. (Regardless of authentication method, Web UI and serial console access will be blocked about 1 minute and SSH connection will be closed automatically if the authentication is failed 3 times consecutively.) So the overall authentication strength for remote authentication can be kept to stronger than the requirement too.
Certificate based authentication	The module supports a public key based authentication with minimum 1024 bit keys. A 1024-bit key has at least 80-bits of equivalent strength. Then the probability of a successful random attempt is 1/2^80. So the authentication strength is higher than Username Password authentication of this module. This certificate based authentication is supported only in SSH connection.
SNMP authentication	The module supports SNMPv3 protocol with SHA authentication and AES privacy control in FIPS mode. The authentication for SNMPv3 is done using keyed-hash message authentication code (HMAC), which is calculated using a cryptographic hash function in combination with a user defined secret key (password - minimum 8 characters long). So the authentication strength is equal to or higher than the Username Password authentication of this module. And if the authentication is failed 3 times consecutively, authentication process will be blocked about 1 minute for all users.

3.4. Cryptographic Key Management

3.4.1. Approved Cryptographic Algorithms

The module used the following FIPS approved cryptographic algorithms.

Algorithm Type	Algorithm	Standard	FIPS Validation Certificate #	Use
Asymmetric keys	RSA	ANSIX9.31; SIG(gen); SIG(ver); RSASSA-PKCS1_V1_5; SIG(gen); SIG(ver); RSASSA-PSS; SIG(gen); SIG(ver);	398	Sign and verify operations, Key generation
	DSA	FIPS 186-2	301	Sign and verify operations, Key generation
Symmetric key	Triple-DES – CBC, CFB8, CFB64, ECB, OFB modes	FIPS 46-3	693	Encrypt/decrypt operations
	AES – CBC, CFB8, CFB128, ECB, OFB each with 128, 192, or 256 bit keys	FIPS 197	821	Encrypt/decrypt operations
HMAC	HMAC-SHA-1	FIPS 198	454	Data integrity, Code integrity
Hashing	SHA-1	FIPS 180-2	819	Hashing

RNG	ANSI X9.31	ANSI X9.31	473	Random number generation

3.4.2. Non-Approved Cryptographic Algorithms

The module used the following non-approved cryptographic algorithms.

Algorithm Type	Algorithm	FIPS Validation Certificate #	Use
Key agreement	DH (1024 and 2048 bit)	None	Key agreement
Symmetric	DES	None	Encrypt, decrypt (Non-FIPS mode only)
	RC4	None	
Asymmetric	RSA (1024bit)	None	Key wrapping
Hashing	MD5	None	Local Password Protection

3.4.3. Key Generation

The module implements the ANSI X9.31 A.2.4 based PRNG and RSA SSH host key generation. And the module also implements the FIPS 186-2 for the DSA key generation for SSH host keys.

3.4.4. Importing or Exporting Keys

Following keys can be imported to the module separately.

- SSH public key for SSH public key authentication per each user : This key can be imported to the module using CLI or Web interface. (Select System administration → User administration → select a user → Enable SSH public key authentication → Select SSH version → Upload a public key).
- Webserver HTTPS(TLS) certificate : This key can be imported to the module using CLI or Web interface. (Select System Administration → Configuration management → Configuration import → select

"location" and set "Configuration selection"(or "import of" in the console menu) to Webserver Certificate → select a file and import.)

- User Password : This key can be imported to the module using CLI or Web interface. (Select System administration → User administration → select a user → enter Password)
- RADIUS/TACACS+ secret : This key can be imported to the module using CLI or Web interface. (Select Network → Web server configuration → Authentication method → select Radius server → enter Shared secret)
- Incoming PAP/CHAP Secret [W] : This key can be imported to the module using CLI or Web interface. (Select Network → PPP configuration → Incoming PPP connections → add or select a user → enter Password)
- Triple-DES static 192 bit key (1 & 2): These keys can be imported to the module using CLI or Web interface. (Select System Administration → Security profile → Key management → enter Clustering encryption key or Configuration encryption key)
- SNMP v3 privacy/authentication password: These keys can be imported to the module using CLI or Web interface. (Select Network → SNMP configuration → Accessing control settings (SNMP-v3) → select a number → check Access control → enter Passwords)

All keys in the module can be exported or imported using CLI or Web interface in the form of an encrypted and compressed configuration file. (To export the configuration file, Select System Administration → Configuration management → Configuration export → Select location to export → Specify the file name → Press export button or select export command.) The exported configuration file includes all keys stored in the flash. For the detail list of keys stored in the flash, please see the table in the section 3.4.5

3.4.5. Cryptographic Keys and Critical Security Parameters (CSP)

The following is a list of all cryptographic keys and key components used by the Digi Passport module.

Keys or CSP	Description
Crypto Officer/ User password	Password used to authenticate User. Stored in flash.
SSH user public key	Used for SSH authentication. Stored in flash.
Bios User Password	Password used to authentication Bios user. Stored in flash.
SSH host keys	SSH sever host keys. Stored in flash.
SSH Diffie-Hellman private key	Used to encrypt initial key exchanges in SSH sessions. Not stored across power cycles, stored in RAM.
SSH Session key (AES, Triple-DES)	Used to encrypt SSH sessions. Stored in RAM.
HTTPS(TLS) Web certificate	Public key certificate for HTTPS(TLS) Web interface. Stored in flash.
SNMP v3 privacy/authentication password	Key used for SNMP v3 protocol. Stored in flash.
Incoming PAP/CHAP Secret	Used in PPP authentication. Stored in flash.
RADIUS secret	Shared secret used with authentication server. Stored in flash.
TACACS+ secret	Shared secret used with authentication server. Stored in flash.
Approved PRNG initial seed and seed key	Used to initialize approved PRNG. Stored in RAM.
Runtime approved PRNG seed and seed key	The runtime seed and seed key values. Stored in RAM.
HMAC-SHA-1 key	Used to check firmware integrity. Stored in RAM.
Triple-DES static 192 bit key (1)	Used to encrypt/decrypt configuration file to export/import. Stored in flash.
Triple-DES static 192 bit key (2)	Used to encrypt/decrypt clustering data. Stored in flash.

3.4.6. Key Zeroization

All keys and CSPs in the module will be zeroized by completing following steps;

- Using CLI or Web interface, select System administration -> Configuration management-> Configuration import-> Select location as Factory default -> Set “Configuration selection” to zeroization(Web UI) or Set “Import of” to zeroization(CLI UI) or -> Select Import menu or Press Import button.

After finishing zeroization, the unit will be rebooted automatically.
Key zeroization process can be performed only by system admin user.

3.5. Self Tests

The module implements following self tests.

3.5.1. Power-on Self Tests

- Firmware Integrity check using a 16 bit checksum
- AES KAT
- TDES KAT
- SHA KAT
- HMAC KAT
- RSA sign/verify
- DSA sign/verify
- RNG

3.5.2. Conditional Self Tests

- Continuous RNG Test
- RSA sign/verify test on key generation
- RSA encrypt/decrypt test on key generation
- Firmware load test using HMAC

4. Secure Operation

The Digi Passport meets Level 2 requirements for FIPS 140-2 compliance. The sections below describe how to place and keep the module in FIPS-approved mode of operation.
In order to operate the Digi Passport module in FIPS-approved mode, each operator should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules detailed in this section.

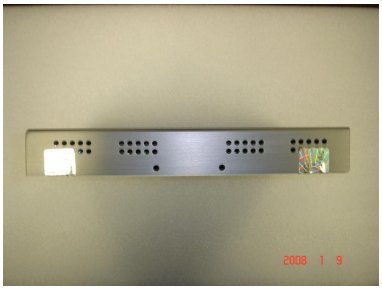
4.1. Physical Security

The module images are pre-installed in the flash and new versions of software are shipped on CDs. All shipping occurs via a reputable courier service. A Crypto Officer should also inspect to make sure the boxes have not been tampered with or damaged upon receiving the modules, which could indicate a security compromise.

The FIPS 140-2 level 2 compliant Digi Passport will be shipped with tamper evident seals. Before setting the module in FIPS approved mode of operation, a Crypto Officer should complete following instructions to provide physical security for FIPS 140-2 level 2 requirements.

1. Clean the module surface of any grease or dirt before you apply the tamper evident seals.
2. Locate the placements of tamper evident seals. (4 locations for the Digi Passport 4 FIPS and 5 locations for the Digi Passport 8 FIPS/16 2AC FIPS/32 2AC FIPS/48 2AC FIPS as shown in the figures below)

Digi Passport 4 FIPS (4 labels – bottom and both sides)

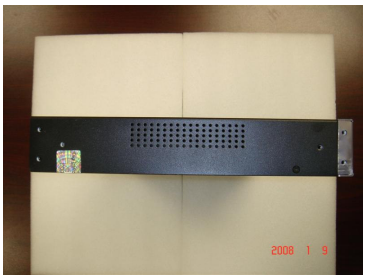


<Left>

<Bottom>

<Right>

Digi Passport 8 FIPS/16 2AC FIPS/32 2AC FIPS/48 2AC FIPS
(5 labels – bottom and both sides)



<Left>

<Bottom>

<Right>

<Upper>

<Front>

3. Apply each seal to the correct place of the module as shown above. (Apply the seal over a screw in such a manner that an attempt to remove the cover requires removal of that screw and indicates subsequent evidence of tampering. In case of the Digi Passport 8 FIPS/16 2AC FIPS/32 2AC FIPS/48 2AC FIPS, one seal should be applied to the PC card slot.)
4. Apply pressure to verify that adequate adhesion has taken place.
5. Record the serial numbers of the seals you attached to the module.
6. Allow 24 hours for the adhesive in the tamper-evident labels to cure.
7. The Crypto Officer shall periodically check the tamper evident seal to verify that the module has not been opened.

4.2. Initial Setup for FIPS Mode of Operation

The factory default mode of operation of the Digi Passport is non-FIPS mode. Once the physical security check is completed, the Crypto Officer with the Bios User role should change the mode of the module to FIPS 140-2 Level 2 compliant mode (FIPS mode) by completing steps described in this section.
(Whenever accessing serial console, user should use non-networked device to

open the serial console of Digi Passport because serial communication is not encrypted by FIPS 140-2 Level 2 compliant algorithms.)

4.2.1. Change the mode of operation

The mode of operation can be changed to FIPS mode or non-FIPS mode only through the bios menu and only the Crypto Officer with the Bios User role can perform this operation.
Bios menu can be accessed by entering <ESC> key on the serial console port of the module within 3 seconds after powering on the unit. Once the module is in the FIPS mode, the Crypto Officer with the Bios User role should enter the password to access the bios menu. But if the unit is in NON-FIPS mode, user can access the bios mode without entering password.
After entering bios menu, the Crypto Officer with the Bios User role can select “4. Change mode” menu to change the mode of operation as shown on below,

```
********************************************************************************
 MPC88x Bios v1.1.0F (Dec 16 2007 - 19:16:02)
********************************************************************************
Please wait for initializing the board.
Board initializing.....................OK
CPU checking...........................OK
DRAM checking..........................OK.
FLASH checking.........................OK.
Power checking.........................OK
(Power1 : Fail, Power2 : OK)

CPU is the MPC880 at 132Mhz(DRAM:256MB,FLASH:64MB)

Now starting the main program!!!
Press <ESC> key to enter the bios menu : 2 <=Press <ESC> key within 3 seconds
--------------------------------------------------------------------------------
 Welcome to Bios Configuration page
--------------------------------------------------------------------------------
 Select menu
 1. RTC configuration [ May 14 08 -  22:03:52 ]
 2. Hardware test
 3. Firmware upgrade [S/W Version : v1.2.0F]
 4. Change mode [NON-FIPS]
 5. Exit and boot from flash
 6. Exit and boot from flash in emergency mode
 7. Exit and reboot
  <ESC> Back, <ENTER> Refresh
 -----> 4
 Select the mode of operation (1. FIPS mode 2. NON-FIPS mode) : 1
 Changing the mode of operation will reset the current configuration of the
unit.
 Are you sure to change the mode(y/n)? y
 Resetting the configuration… Please wait a moment.
 Now this unit is running on FIPS 140-2 mode.
 You should change the default password for bios menu.
```

After changing the mode of operation, the Crypto Officer with the Bios User role should change the bios menu password also. The bios password should be 8 characters long at least.

```
--------------------------------------------------------------------------------
Welcome to Bios Configuration page
--------------------------------------------------------------------------------
Select menu
1. RTC configuration [ May 14 08 -  22:03:52 ]
2. Hardware test
3. Change password
4. Change mode [FIPS]
5. Exit and boot from flash
6. Exit and reboot
 <ESC> Back, <ENTER> Refresh
-----> 3
Enter new password :********
Re-enter new password :********
Password changed successfully. Press Enter to continue.
```

4.2.2. Change the default password of the Crypto Officer

After changing the mode of operation and the password for bios menu, the Crypto Officer with the Bios User role can select menu “5. Exit and boot the flash” or “6. Exit and reboot” menu to continue the boot process of the module.
After boot process is completed, the Crypto Officer with the System Admin user role can access the CLI menu. The factory default user name of Crypto Officer with the System Admin user role is “admin” and the password is “dbpsfips”. The Crypto Officer with the System Admin user role should change the default password using CLI menu through serial console as shown on below,
(Whenever boot process is proceeded, the Crypto Officer with the System Admin user role should confirm whether firmware integrity check and power-on self test are passed.)

```
--------------------------------------------------------------------------------
Welcome to Bios Configuration page
--------------------------------------------------------------------------------
Select menu
1. RTC configuration [ Jan 20 09 - 14:02:22 ]
2. Hardware test
3. Change password
4. Change mode[FIPS]
5. Exit and boot from flash
6. Exit and reboot
 <ESC> Back, <ENTER> Refresh
-----> 5

  <Loading Kernel Image>
  Image Name:   Kernel 2.6.12 for MPC880(Linux Kernel)
  Data Size:    1596635 Bytes
  Verifying Checksum ... OK
```

```
   Uncompressing Kernel Image ... OK
   <Loading RAMDisk Image>
   Image Name:   RAMDISK(Linux RAMDisk Image)
   Data Size:    116833 Bytes
   Verifying Checksum ... OK
   Loading Ramdisk ...OK
...
<Linux Kernel boot messages will be shown on serial console of the module>
...
INIT: version 2.85 booting

             Welcome to Passport Embedded Linux Environment
Setting hostname localhost:  [  OK  ]
Checking filesystems
Checking all file systems.
[  OK  ]
Mounting local filesystems:  [  OK  ]
Enabling swap space:  [  OK  ]
Checking the Mode of System... [FIPS MODE]

Mounting the secondary root file system
Mounting user space
Reinitializing JFFS2 file system on mtdblock5
Erased 16384 Kibyte @ 0 -- 100% complete.
Copying default configuration from default files
UM>> Bios F/W Upgrade Flag is cleared
Initializing configuration. Please wait a moment
Saving configuration. Please wait a moment
Starting Power-On Self Test
FIPS: Checking F/W integrity...Done.
FIPS: Running power-on self-test...Done.
User script will not be started. [FIPS MODE]
...
<More Linux application boot messages will be shown on serial console of the
module>
...
Starting connsvrd: [  OK  ]


DENX ELDK version 4.0
Linux 2.6.12 on a ppc

Digi Passport 48: System Ready.
Digi_Passport login:
Digi_Passport login: admin
Password:

------------------------------------------------------------------------------
 Welcome to Digi Passport 48 configuration page    (Operation mode : FIPS)
 Current time   : 05/27/2008 04:34:03   Serial No.    : D182007FIPS
 F/W Rev.      : v1.2.0F               Bios Ver.     : v1.1.0F
 MAC addr.(eth0): 00-40-9D-44-EF-12    IP addr.(eth0) : 10.0.1.28
------------------------------------------------------------------------------
1. Network
 2. Serial port
 3. Clustering
 4. Power controller
 5. Peripherals
 6. System status & log
 7. System administration
 8. Activate Passport Locator LED

[h]elp, [s]ave, [a]pply, e[x]it, [r]eboot
COMMAND (Display HELP : help)> 7
```

```
------------------------------------------------------------------------------
 System administration                Operation mode : FIPS
 /admin
------------------------------------------------------------------------------
---
 1. User administration
 2. Access lists
 3. Change password
 4. Device name              : Digi_Passport
 5. Date and time
 6. Configuration management
 7. Security profile
 8. Firmware upgrade
 9. CLI configuration

[h]elp, [s]ave, [a]pply, e[x]it, [r]eboot
COMMAND (Display HELP : help)> 3

------------------------------------------------------------------------------
 Change password
 /admin/change_pwd
------------------------------------------------------------------------------
NEW : ********
CONFIRM : ********
Password changed successfully !

------------------------------------------------------------------------------
 System administration                Operation mode : FIPS
 /admin
------------------------------------------------------------------------------
 1. User administration
 2. Access lists
 3. Change password
 4. Device name              : Digi_Passport
 5. Date and time
 6. Configuration management
 7. Security profile
 8. Firmware upgrade
 9. CLI configuration

[h]elp, [s]ave, [a]pply, e[x]it, [r]eboot
COMMAND (Display HELP : help)>
```

The password of Crypto Officer with the System Admin user role should be 8 characters long at least and must meet the following password complexity rules.

- Not contain all or part of the user's account name
- Be at least eight characters in length
- Contain at least one character from the following four categories:
  * English uppercase characters(A through Z)
  * English lowercase characters (a through z)
  * Base 10 digits (0 through 9)
  * Non-alphabetic characters (for example, !, $, #, %)
- Not contain consecutive alpha-numeric characters (for example, aa, ab, ba, 12, 43)
- Not contain repeated same string

4.2.3. Change the default SSH host keys and HTTPS certificate

After changing the password of the Crypto Officer, default SSH host keys and HTTPS certificate should be changed also.
SSH host key can be generated through the menu below,
[System Administration] -> [Security profile] -> [Key management] -> select “SSH host key generate” (CLI UI) or press “Generate” button (Web UI)
And the new HTTPS certificate can be uploaded through the menu below,
[System Administration] -> [Configuration management] -> [Configuration import] -> select “location” and set “Configuration selection”(or “import of” in the console menu) to Webserver Certificate -> select a file and import.

4.2.4. Change the default Triple-DES keys

The Crypto Officer with the System Admin user role should also change following two default Triple-DES keys to make the module run in FIPS 140-2 Level 2 compliant mode,

- Clustering encryption key
- Configuration encryption key

Each key can be changed by entering 48 hexadecimal characters (192 bits) through the menu below,
[System Administration] -> [Security profile] -> [Key management]