Configuring the FIPS 140 Module for the BIG-IP 520/540 Platform

- Introducing the FIPS 140 hardware security module
- Initializing the FIPS 140 hardware security module and creating the security world
- Using the Key Management System
- Additional configuration options

Introducing the FIPS 140 hardware security module

The 520/540 platforms, support a hardware security module (HSM) that is certified at the Federal Information Processing Standards (FIPS) 140-2, level 3. The FIPS standard is a set of requirements designed to facilitate the construction, and measure the security of cryptographic modules, and define methods for protecting cryptographic keys from unauthorized access. Typically, the cryptographic keys are generated inside the FIPS 140-certified hardware security module (HSM), and never leave except when in encrypted form known only to the HSM itself.

Note

For more details about the FIPS standards, see the National Institute of Standards and Technology (NIST) Web site for the Computer Security Resource Center (CSRC) at the URL: ***http://csrc.nist.gov/publications/fips****.*

With this HSM installed, you can encrypt private keys on the BIG-IP platform with a triple Data Encryption Standard (3-DES) 168 bit key that resides only on the FIPS 140 module. The 3-DES key is further encrypted with a key spread across one to five smart cards.

This document describes how to configure the FIPS 140 security module on the BIG-IP 520/540 platform with software version 4.5 PTF-08 or later installed.

In order to configure FIPS 140 hardware support, you need to complete the following tasks:

- Initialize the FIPS 140 hardware and set up the security world. For more information, see *Initializing the FIPS 140 hardware security module and creating the security world*, on page 1-2.
- Generate keys using the Configuration utility. For more information, see *Generating keys and certificate requests*, on page 1-7

Note

All BIG-IP products except the BIG-IP LoadBalancer, BIG-IP FireGuard Controller, and the BIG-IP Cache Controller support this configuration.

Initializing the FIPS 140 hardware security module and creating the security world

After you install the BIG-IP system in the network and run the Setup utility, you can initialize the FIPS 140 hardware security module (HSM). This is how you prepare the HSM for the security world. The ***security world*** is the environment you create for secure life-cycle management of keys based on nCipher technology. To create the security world, you run various utilities from the command line on the BIG-IP system. You can initialize the HSM and set up the security world in these situations:

- On a single unit or first unit configured in a redundant system. For more information, see *Creating the security world on a single unit or the first unit in a redundant system*, on page 1-2.
- On a redundant system with one HSM in each BIG-IP unit (only required if you have a redundant system). For more information, see *Configuring the security world on the second unit in a redundant system*, on page 1-5.

Note

You need a paper clip or ballpoint pen and at least two of the smart cards provided with the security module (three are recommended) before you begin the initialization process.

Creating the security world on a single unit or the first unit in a redundant system

If you are configuring the FIPS hardware on a BIG-IP system, you need to set up the security world on a single unit or the first unit configured in a redundant system.

To create the security world on a single unit or the first unit configured in a redundant system

1. Locate the switch labeled **M-O-I** on the FIPS 140 card at the back of the controller. Then using a paper clip or your finger tip, move the switch to the **I** position (as shown in Figure 1.1).

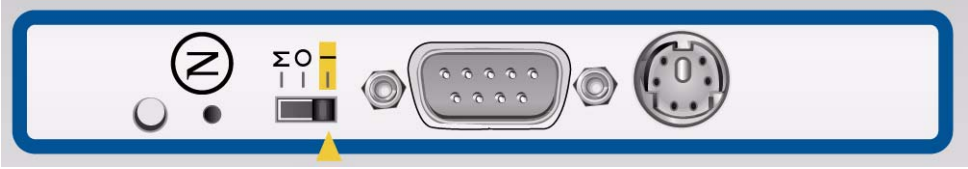

Figure 1.1 *This figure shows the M-O-I switch on the FIPS 140 security module*

2. With a ballpoint pen tip, gently push the reset button (as shown in Figure 1.2).
   If you have done this correctly, the LED blinks quickly for a moment and then blinks slowly again.

Figure 1.2 *The reset button on the FIPS 140 security module*

3. Type the following command to create the security world:

   `new-world -i -s 0 -k 1 -n 2 -m 1`

   Figure 1.3 is an example session with the **new-world** utility.

```
# bigip:# new-world -i -s 0 -k 1 -n 2 -m 1
new-world: no card in module 1 slot 0
Insert new adminstrator card 1 into module 1 slot 0 and press return...
Passphrase for new administrator card 1:
Verify passphrase for new administrator card 1:
Insert new adminstrator card 2 into module 1 slot 0 and press return...
Module 1 slot 0 contains an unrecognized card. Overwrite it? (yes/no): yes
Passphrase for new administrator card 2:
Verify passphrase for new administrator card 2:
security world created; hknso = b01400700f3e39a4ea17ec34b557dd6b0dcfc859
```

Figure 1.3 *Example of a security world initialization session with the* ***new-world*** *utility*

4. This **new-world** configuration creates a cardset that requires only one card to be present for card or module management, but also provides the other card as a backup of the first. Figure 1.4 demonstrates the proper orientation of the smart card before you insert it into the card reader. For more information about cardsets, please refer to the nCipher manual, ***Key management user guide***, Chapter 6: *Managing cards*. This manual is included on the BIG-IP Software and Documentation CD.
5. Move the **M-O-I** switch (as shown in Figure 1.1) to O and, with the paperclip, press the reset button (as shown in Figure 1.2).
6. Generate keys and certificates using the Configuration utility. For detailed information, see *Using the Key Management System*, on page 1-7.

7. After you generate the keys, your next task depends on what type of system you are configuring:
   - If this is a single unit, after you create the security world, you can configure the SSL Accelerator. For more information, see *Additional configuration options*, on page 1-9.
   - If this is a primary unit in a redundant system, complete the tasks described in the section *Configuring the security world on the second unit in a redundant system*, on page 1-5

.

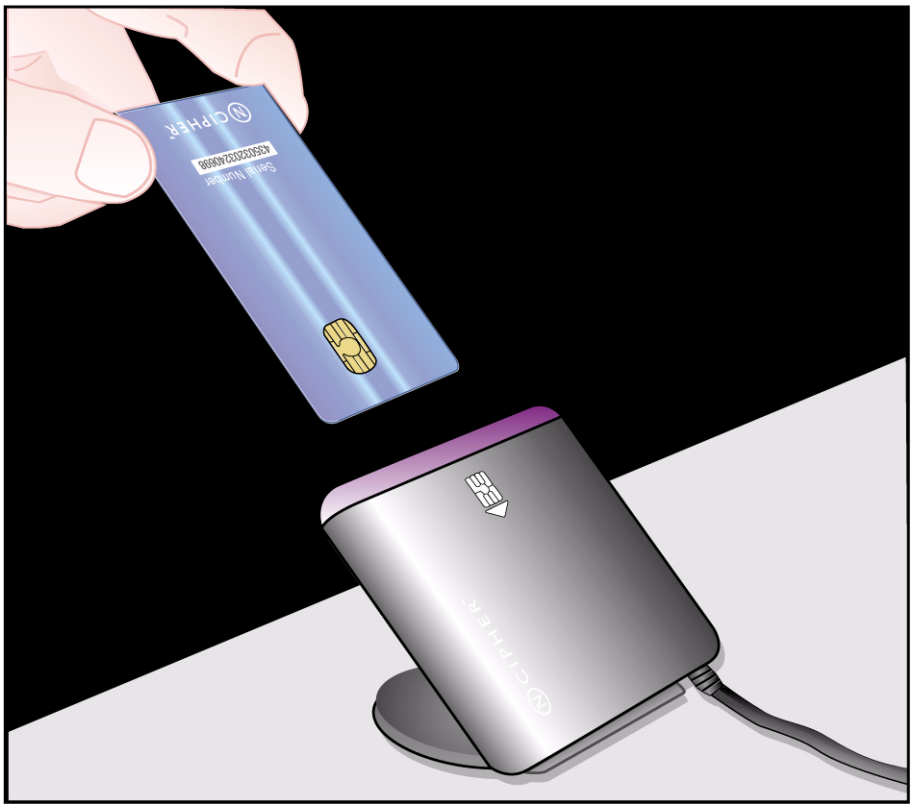

Figure 1.4 *The proper way to insert a smart card in the card reader*

Configuring the security world on the second unit in a redundant system

The second unit in the redundant system must be brought into the same security world as your first unit. This is a simple process, but one that must be done after you run the Setup utility and synchronize the configurations of the units in the redundant system. This means that both units in the redundant system must be synchronized in order to synchronize the SSL keys. This section describes how to synchronize both BIG-IP units in a redundant system, and how to configure the security world on the second unit in a redundant system.

◆ Note

You must configure the BIG-IP redundant system for fail-over for this configuration to function properly. If you have not configured the redundant system, refer to Chapter 13, ***Configuring a Redundant System****, in the* ***BIG-IP Reference Guide****.*

To synchronize the BIG-IP system configuration from the command line

Before you configure the security world on the redundant system, synchronize the BIG-IP system configuration. To synchronize the BIG-IP system configuration from the command line, type the following command on the first unit:

```
b config sync all
```

To configure the security world on the redundant system

After you synchronize the BIG-IP system configuration, you need to initialize the HSM and configure the security world on the second unit in the redundant system. You need a ballpoint pen, or other fine-tipped implement to press the reset button.

Before you start, you need the required number of administrator smart cards from the administrator cardset you created when initializing the security world on the first unit.

1. On the front of the second BIG-IP platform in the redundant system, locate the switch labelled **M-O-I** (as shown in Figure 1.1). Then using a paper clip or your fingernail, move the switch to the **I** position.
2. With the end of the ballpoint pen, gently push the reset button (as shown in Figure 1.2). If you have done this correctly, the LED blinks quickly for a moment, and then blinks slowly again.
3. Place your administrator smart card into the card reader attached to the FIPS 140 security module in the redundant unit. Figure 1.4 shows the proper orientation of the smart card.

4. At the console of the second unit in the redundant system, run the **new-world** command. (See Figure 1.5 for an example session).

   new-world -l -m 1

5. Return to the front of the controller. Move the **M-O-I** switch to O and, with the ballpoint pen, press the reset button in the hole next to the switch (as shown in Figure 1.2).

   After you bring the second controller into the security world, you can configure the SSL Accelerator. For more information, see *Additional configuration options*, on page 1-9.

```
bigip:# new-world -l -m 1
Passphrase for administrator card 1:
security world loaded; hknso = f2ec05b1dfa58f4ffaff1be7f197430bafd48bce
```

Figure 1.5 *An example session with the* ***new-world*** *utility*

Using the Key Management System

Managing certificates and public-private key pairs can be confusing, especially when you have more than one proxy defined. To help you manage certificates and keys, the BIG-IP system provides a set of key management screens within the Configuration utility.

Collectively, these screens are known as the ***Key Management System (KMS)***.

For additional information on how to manage key pairs and certificates, see the ***BIG-IP Reference Guide version 4.5***, Chapter 7, *SSL Accelerator Proxies*.

◆ Note

*If you have a redundant system, after you generate, import, or install certificates, you need to use the **b configsync all** command to transfer these keys to the redundant unit.*

Generating keys and certificate requests

Using the SSL Certificate Administration screen within the Configuration utility, you can generate a new key pair and certificate request.

To generate a new key pair and certificate request

1. In the navigation pane, click **Proxies**.
2. Click the Cert Admin tab.
3. Click the **Generate New Key Pair/Certificate Request** button. This displays the Create Certificate Request screen.
4. Make sure that the **Security Type** is set to **FIPS**.
5. Type in the data for all boxes on the screen.
6. Click the **Generate Key Pair/Certificate Request** button.

   Use the certificate request to get a signed certificate from your Certificate Authority.

Installing certificates

When you recieve a signed certificate from your Certificate Authority, you can install that certificate, using the Certificate Properties screen.

To install a certificate

1. In the navigation pane, click **Proxies**.
2. Click the Cert Admin tab.
3. In the Certificate ID column, click the certificate you want to install. The Certificate Properties screen displays.
4. Click the **Install Certificate** button.

Importing existing public keys and certificates

No additional software is needed to import an existing private key. You can import existing keys, using the Certificate Properties screen.

To import a key

1. In the navigation pane, click **Proxies**.
2. Click the Cert Admin tab.
3. Click **Import**. Make sure that the import type is **Key**.
4. Click **Continue**.
5. If you copied the key text from another application, paste the key into the Key Contents window. Enter the key name in the **Key Identifier** field.
6. If you saved the key to a file, click the **Browse** button, locate the key file, then enter the key name in the **Key Identifier** field.
7. If you want to overwrite an existing key identifier, select an identifier from the list.
8. Click the **Install Key** button.

Note

After you import or generate keys on a redundant system, make sure you synchronize the BIG-IP system configuration. To synchronize the BIG-IP system configuration, see ***To synchronize the BIG-IP system configuration from the command line****, on page 1-5.*

WARNING

From a security standpoint, it is better to generate a new key instead of importing a plain text key which may have already been compromised. To generate a new key, see ***Generating keys and certificate requests****, on page 1-7.*

Additional configuration options

After you complete the configuration, you have a number of options:

- After you have initialized the security world and generated keys, you can manage the keys with the Key Management System. For more information about the Key Management System, see the ***BIG-IP Reference Guide***, Chapter 7, *Using the Key Management System*, under the *Authentication* section.
- There are additional SSL Accelerator options you can configure. For more information, see the ***BIG-IP Reference Guide***, Chapter 7, *SSL Accelerator Proxies.*
- All configurations have health monitoring options. Refer to the ***BIG-IP Reference Guide***, Chapter 11, *Monitors*.
- When you create a pool, there is an option to set up persistence and a choice of load balancing methods. Refer to the ***BIG-IP Reference Guide***, Chapter 4, *Pools*.