This document provides information on how to use the HSM 500 Hardware Security Module (WWOP-HSM-500) provided by nCipher® Corporation Ltd. for enabling high-security features on a Webwasher® appliance running version 6.8.3 and higher of the appliance software.

The HSM 500 Hardware Security Module is a hardware card suitable for insertion in one of the slots on the back side of a Webwasher appliance box.


In this document...

Overview .......................................................... 2
Prerequisites ....................................................... 2
Hardware installation .......................................... 2
Creating a Security World ..................................... 3
Creating an Operator Card Set ............................... 4
Creating security keys ........................................... 4
Creating and importing certificates ........................... 5
Overview

The HSM 500 Hardware Security Module enables you to implement the use of HSM (Hardware Security Module) features on your Webwasher appliance. Using these features, Web traffic can be handled in a high-security mode, while following the provisions of the SSL (Secure Sockets Layer) protocol. This protocol requires data encryption and the use of certificates that are submitted and evaluated before traffic is allowed on a particular connection.

Processing traffic under this protocol also requires the use of appropriate keys. After installing the HSM 500 Hardware Security Module on your Webwasher appliance and configuring the necessary settings, you can create the keys that are needed in different situations. The keys are then stored on the module, thereby implementing a heightened level of protection.

A special software module is used for creating certificates. This module is the HSM Agent, which is included in the Webwasher appliance software. After creating the certificates, an import must be performed for some of them to make them available for handling SSL-secured traffic under Webwasher.

Prerequisites

Before you begin, make sure the following is installed and running on your appliance:

- CGLinux operating system, version 5.1.1 and higher
- Webwasher appliance software, version 6.8.3 and higher

**Note:** This version of the appliance software is included in version 5.1.1 of the CGLinux operating system.

The appliance software also contains the HSM Agent software module.

Hardware installation

For information on how to install the HSM 500 Hardware Security Module on your appliance box, refer to the product documentation provided by nCipher.

Refer to the *Webwasher Appliances Installation and Configuration Guide* for descriptions of the various Webwasher appliance hardware models. There you will also find information about the slots on an appliance’s back panel, where the module can be inserted.

**Note:** The appliance slot to be used for inserting the module may be occupied by an additional network card.

This is the case, for example, with the WW1100 and WW1900B appliance models.

Remove the network card to make room for the module.
Creating a Security World

Implementing the high-security features provided by the HSM 500 Hardware Security Module begins with creating a specific kind of configuration, which is termed a “Security World”. Proceed as follows:

1. Set the module to Initialization status. This can be done using a switch on the its back side:
   Move this switch to position I (= Initialization).

2. Reset the module by pressing its Clear button.
   Alternatively, you can reset the module by entering the following command on the console you are using to administer your Webwasher appliance:
   ```
   /opt/nfast/bin/nopclearfail -c -a
   ```

   **Note:** You can check if the initialization was successful with the following console mode command:
   ```
   /opt/nfast/bin/enquiry
   ```
   The output delivered by this command shows the status of the module.

3. Enter the following console mode command to create the new Security World:
   ```
   /opt/nfast/bin/new-world -i -Q 1/2
   ```
   The new Security World allows you to implement high-security features, using special administrative devices termed “Administrator Cards” and “Operator Cards”. These cards are delivered with the HSM 500 Hardware Security Module. They can be read by the card reader that is part of the module.

   Administrator Cards are required for completing tasks where the creation or the settings of a Security World are involved. Operator Cards are required for completing tasks inside an existing Security World, such as creating and using security keys.

   Furthermore, the Security World allows you to determine the number of administrators and operators that must participate in completing a task. This is done by configuring the number of Administrator and Operator Cards that must be inserted in the module’s card reader.

   You can configure the total number of cards that are eligible for completing a task, and in addition to this, the number of cards that are actually required for this task.

   The last parameter in the above command is used for this purpose. The second figure of the parameter indicates the total number of Administrator Cards that are created, while the first figure indicates the number of cards that are actually required to complete a task.

   In the sample configuration provided here, two cards are created, while only one card is needed for a task.

   **Note:** To implement a higher security standard, you may choose, for example, to let 2 out of 2 Administrator Cards be required for completing a task, or to use even more of the cards that are delivered with the module.

   For more information about the use of Administrator Cards, refer to the product documentation provided by nCipher.

4. Set the module back to Operational status by moving the switch on its back side to position O (= Operational).

5. Reset the module again by pressing the Clear button.
Creating an Operator Card Set

Before you are allowed to create keys under the high-security standards implemented through installation of the HSM 500 Hardware Security Module, one or several Operator Cards must be inserted in the module’s card reader.

These cards are delivered with the module. They are configured as members of an Operator Card Set. Proceed as follows:

1. Enter the following console mode command to create an Operator Card Set:
   
   ```sh
   /opt/nfast/bin/createocs -m1 -Q 1/2 -N <set name>
   ```

   where `-m1` is the module that this Operator Card Set belongs to and `<set name>` a variable that must be replaced by the name you give to this Operator Card Set, for example, `opcardset`.

   In the same way as for Administrator Cards (see previous section), the `1/2` parameter indicates the numbers of Operator Cards that are created with different implications. `1` is the number of cards required for completing a task inside the Security World, while `2` is the total number of cards. Again, these numbers are only examples and may be specified otherwise.

   **Note:** To implement a higher security standard, you may choose, for example, to let `2` out of `2` Operator Cards be required for completing a task, or to use even more of the cards that are delivered with the module.

   For more information about the use of Operator Cards, refer to the product documentation provided by nCipher.

2. A dialog line appears on your console monitor, asking you to configure a password for the first Operator Card:
   
   Enter a password.

3. [Conditional] If more than one Operator Card has been configured as required in Step 1, Step 2 is repeated until a password has been configured for every card:
   
   Enter as many passwords as required.

Creating security keys

Up to three different security keys can be used for handling SSL-secured traffic on your Webwasher appliance:

- One that the HSM Agent uses when connecting to the Webwasher SSL Scanner module.
  The name for this key could be, for example, `wwsslscanner`.

- One that Webwasher uses when it acts as root CA (Certificate Authority), issuing Webwasher server certificates that are sent to clients when their requests are processed in SSL-secured mode.
  Its name could be, for example, `wwca`.

- One for the initial handshake Webwasher exchanges with browsers that send requests as clients to Webwasher.
  This key is also known as “domain key”. Its name could be, for example, `wwdomain`.

Proceed as follows:

1. Enter this console mode command to create a security key:
   
   ```sh
   /opt/nfast/bin/generatekey -g hwcrhk
   ```

   where `hwcrhk` is the name of the library that stores the information about the keys.
2. A prompt on your console monitor asks you to insert an Operator Card in the module’s card reader:
   Insert an Operator Card.

3. A dialog line asks you to enter a password for the Operator Card:
   Enter the password you configured for this card (see previous section).

4. [Conditional] If more than one Operator Card has been configured as required, Steps 2 and 3 are repeated until all required Operator Cards are processed.
   Insert cards and enter passwords as required.

5. More dialog lines are displayed on the console monitor to let you configure the settings for the first key:
   Leave the default settings and enter a key name.

6. Repeat this until you have created and configured the three keys mentioned above.

---

### Creating and importing certificates

Certificates are created using the HSM Agent and imported via the Webwasher Web interface. Proceed as follows:

1. Enter the names of the security keys you created in the `hsmagent.conf` configuration file. This file is stored under:
   `/opt/hsmagent/conf/hsmagent.conf`
   Open the file with an editor and enter the following in the respective file sections:
   a. The engine ID:
      ```
      [Engine]
      ID = chil
      ```
   b. Information about the keys:
      ```
      [NetWork]
      HSMagentkey = rsa-wwsslscanner
      [LoadKeys]
      rsa-wwca
      rsa-wwca
      ```

   **Note:** The `rsa` prefix denotes the key algorithm. It is added by the HSM Agent to each of the key names that you configured. When entering a key name in the configuration file, you need to specify this prefix as well.
   Furthermore, note that the name parts following the prefix are only examples, corresponding to the ones that were given in the previous section.

2. Remove all old certificates. These are stored under:
   `/opt/hsmagent/pki/*`

3. Start the HSM Agent with the following console mode command:
   `/etc/init.d/hsmagent start`

4. A prompt on your console monitor asks you to insert an Operator Card:
   Insert an Operator Card in the module’s card reader.
5. A dialog line asks you to enter a password for the Operator Card:
   Enter the password you configured for this card.

   **Important:** Every time you start or restart the Webwasher appliance, you also need to start the HSM Agent. Since the insertion of at least one Operator Card and password is required for doing this, it cannot happen automatically.

6. [Conditional] If more than one Operator Card has been configured as required, Steps 4 and 5 are repeated until all required Operator Cards are processed:
   Insert cards and enter passwords as required.

7. Once the HSM Agent is started, use it to create certificates:
   a. Create the certificate that the HSM Agent submits to the Webwasher SSL Scanner module when connecting to it. Enter the following command after the `hsmagent` prompt that appears on your console monitor:
      
      ```
      #hsmagent -s rsa-wwsslscanner
      ```
      
      **Note:** The command contains a key name with `wwsslscanner` as part of the name. This is only an example, however, corresponding to what was proposed in the previous section.
      
      The corresponding parts of the key names mentioned in the remaining steps of the current section are examples, too.

   b. Create the Webwasher client certificate that is submitted by the SSL Scanner module to the HSM Agent when connecting to it:
      
      – Enter the following command:
      ```
      #hsmagent -w
      ```
      
      A prompt asks you to specify a Common Name for the certificate.
      Enter the IP address of the system that the SSL Scanner module runs on. This is usually the Webwasher appliance, so the address could be, for example, `127.0.0.1`.
      
      The HSM Agent creates the certificate file, for example, `127.0.0.1.pem`.

      **Note:** When the Webwasher SSL Scanner module actually connects to the HSM Agent, using a particular IP address, this address is evaluated to make sure it is identical with the one that is entered as Common Name in this certificate file.

   c. Create the certificate that Webwasher uses when it acts as root CA, issuing Webwasher server certificates that are sent to clients when their requests are processed in SSL-secured mode.
      Enter the following command:
      ```
      #hsmagent -g rsa-wwca
      ```
      
      The HSM Agent creates the `rootcacert.pem` certificate file and stores it under:
      ```
      /opt/hsmagent/pki/rootcacert.pem
      ```
8. Configure the appropriate Webwasher settings and import certificates as needed:
   a. Log in to Webwasher and, in the Web interface, go to Configuration > Certificate Management > Private Key Handling.
   b. In the HSM Agent Setup section, configure the connection from the Webwasher SSL Scanner module to the HSM Agent and import the Webwasher client certificate that the SSL Scanner submits to the HSM Agent:
      - Under HSM Agents, enter the IP address and port number of the system that the HSM Agent runs on, which is usually your Webwasher appliance. The default port number is 9531.
      - Make sure the Use encrypted connections to HSM Agents check box is marked.
      - Make sure the Use client certificate to authenticate to HSM Agents check box is also marked.
      - Use the Browse button at the bottom of the section to browse to the file containing the client certificate, for example, 127.0.0.1 pem.
      - After browsing to the appropriate file, click Import client certificate.
   c. In the Certificate Issuing Options section, configure the issuing of Webwasher server certificates that are submitted to clients of Webwasher and import the root certificate that Webwasher uses when acting as the root CA that issues these server certificates:
      - Check the radio button labeled by remote service using HSM Agent with key.
      - In the input field next to this button, enter the name of the root CA key as specified in the hsmagent.conf configuration file (see Step 1b), for example, rsa-wwca.
      - In the input field below, enter the number of days the certificate should remain valid. The default value is 365.
      - Use the Browse button at the bottom of the section to browse to the file containing the root certificate, for example, rootcacert.pem.
      - After browsing to the appropriate file, click Import root certificate.
d. In the **Handshake Options** section, configure the initialization of connections from Webwasher to browsers that send requests as clients to Webwasher:
   - Check the radio button labeled **by remote service using HSM Agent with key**.
   - In the input field next to this button, enter the name of the domain key as specified in the `hsmagent.conf` configuration file (see Step 1b), for example, `rsa-wwdomain`.
   - [Optional] Mark the **Send certificate chain in handshake** check box.

9. Click on the **Apply Changes** button, which is located above the right side of the tab, to make your settings effective.