Manufacturer HSM Installation and Setup User Guide

Introduction

This user guide provides installation and setup instructions for the Manufacturer HSM (M-HSM) server.

The M-HSM server is used for all tasks related to execution of programing jobs by the Contract Manufacturer as a part of the Microchip SPPS flow.

This user guide contains the following sections:

- M-HSM Server, describes the M-HSM server components and system requirements.
- M-HSM Installation and Setup Scenarios, provides a general description of the installation scenarios.
- Initial M-HSM Server Installation and Setup, explains the installation and setup process.
- M-HSM Reconfiguration and Post-Installation Actions, provides instructions for the setup and maintenance actions that can be performed on an installed and provisioned M-HSM server.
- M-HSM Server Replication, explains how to replicate an existing M-HSM server to one or more new M-HSM servers.

For more information about the SPPS flow, see the Secure Production Programming Solution (SPPS) User Guide.

For installation and setup instructions for the User HSM (U-HSM), see the User HSM Installation and Setup Guide.

Table of Contents

Introduction....1

1. M-HSM Server.... 4
   - 1.1. Server Components.... 4
   - 1.2. Security World and HSM Modules.... 4
   - 1.3. System Requirements....7

2. M-HSM Installation and Setup Scenarios.... 9

3. Initial M-HSM Server Installation and Setup.... 10
   - 3.1. Software Installation....10
   - 3.2. M-HSM Server Software Installation.... 10
   - 3.3. HSM Hardware Module Installation....10
   - 3.4. M-HSM Server Provisioning....14
   - 3.5. FTP Server Setup....26

4. Running M-HSM Server as a Service.... 33
   - 4.1. Service Setup....33
   - 4.2. M-HSM Control Panel Application....35

5. M-HSM Reconfiguration and Post-Installation Actions.... 38
   - 5.1. HSM Module Replacement.... 38
   - 5.2. Import the Public Key of M-HSM....39
   - 5.3. Import the Public Keys of U-HSM....39
   - 5.4. Export the Public Keys for Sending to a U-HSM....39
   - 5.5. Import New DFK DB and Manufacturing Keys from U-HSM....39
   - 5.6. Upgrade the HSM Module Firmware....39

6. M-HSM Server Replication....40
   - 6.1. Install the Software....40
   - 6.2. Copy Over the Security World....40
   - 6.3. Copy Over the M-HSM Server.... 40
   - 6.4. Install a New HSM Module....40
   - 6.5. Start the M-HSM Server....40
   - 6.6. Set Up the FTP Server....40

7. Referenced Documents.... 41

8. Revision History.... 42

9. Microchip FPGA Technical Support.... 43
   - 9.1. Customer Service....43
   - 9.2. Customer Technical Support.... 43
   - 9.3. Website.... 43
   - 9.4. Outside the U.S....43

The Microchip Website....44

Product Change Notification Service....44

Customer Support..... 44

Microchip Devices Code Protection Feature..... 44

Legal Notice..... 45

Trademarks..... 45

Quality Management System..... 46

Worldwide Sales and Service.....47

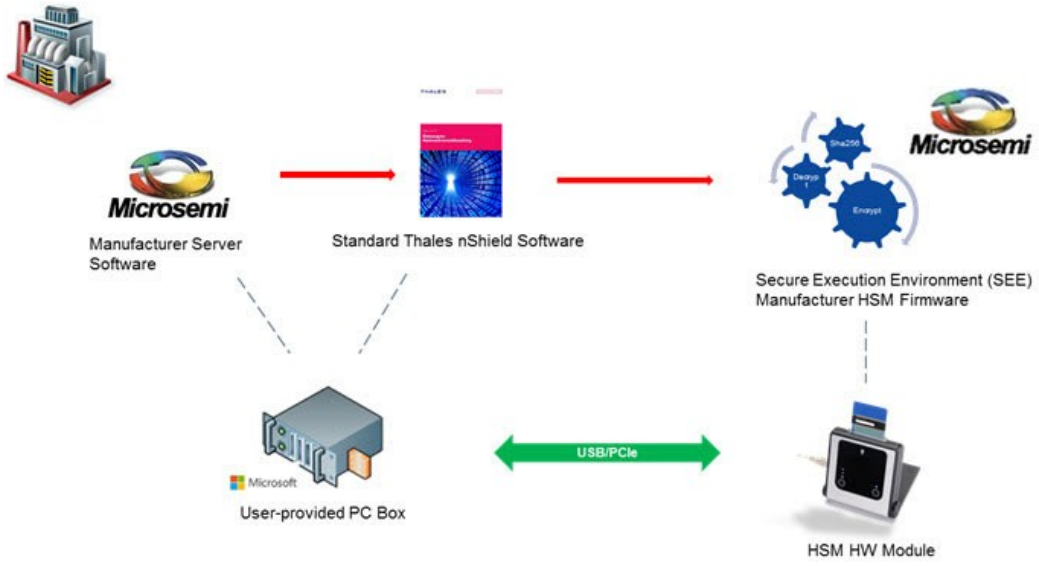
1. M-HSM Server

The M-HSM server is used by the FlashPro Express tool to generate security protocol data during the manufacturing process. FlashPro Express must be configured to work with the M-HSM. For more information, see the FlashPro Express User's Guide.

1.1 Server Components

The following figure shows the components of the M-HSM server.

Figure 1-1. M-HSM Server Components



1.2 Security World and HSM Modules

The vital component of the M-HSM server is the HSM module. The HSM module carries out cryptographic operations involving protected security keys. All data is stored outside the module on the disk of the host system in encrypted form. Every module is associated with the Security World (see the Secure Production Programming Solution (SPPS) User Guide) that combines a set of keys giving module access to the information in the database located on the PC side. The Security World can be replicated to multiple HSM servers, if needed. The HSM module is controlled through standard nCipher nShield software that includes hardware drivers and low-level components providing access to the services inside the module. Custom SEE firmware (algorithms related to the protocols implemented in Microchip devices) and known as the SEE Machine is stored on the disk of the host PC, and is loaded into the module as part of the power-up process.

1.2.1 HSM Module Types

Microchip is the official redistributor of nShield Edge (Figure 1-2) and nShield Solo HSM Modules (Figure 1-3).

Figure 1-2. nCipher nShield Edge HSM Module

Figure 1-3. nShield Solo PCIe HSM Module

The nShield Edge module is attached to USB 2.0 port of the PC and has an integrated card reader. The nShield Solo module is PCIe-based and requires a desktop PC with a spare PCIe port. The card reader is attached to the module through cable.

Note: For the HSM module specification, including performance characteristics, see the *nShield Edge and Solo User Guide for Windows*.

1.2.2 Security World Cards

Both types of HSM modules that are shipped with the nShield Security World cards (Figure 1-4) can be used to create an Administrator Card Set (ACS). The ACS provides access to the administrative functions of the Security World:

- Controls access to Security World configuration
- Authorizes recovery and replacement operations

ACS cards are initialized upon creation of the Security World.

Figure 1-4. Example of nShield Security World Card

Note: There is a special requirement regarding total and quorum numbers of ASC cards. For more information, see the *nShield Edge and Solo User Guide for Windows*.

1.2.3 Activator Card and Feature Licensing (nCipher)

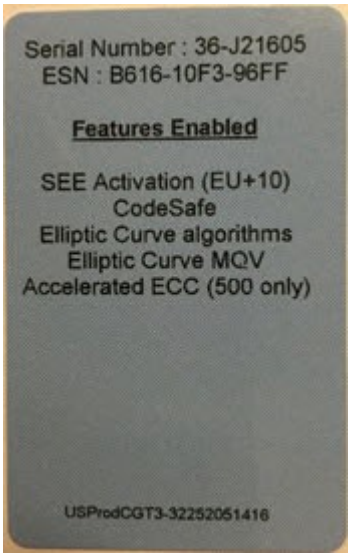
The Activator card (see Figure 1-5) enables HSM Module product features and is generated along with the license purchase. Installation instructions in this document show how to use this type of card.

Figure 1-5. Example of Activator Card

This card is linked to the specific hardware module and must match the module serial number (see Figure 1-6). The *Serial Number* field shown on the back of the card must match the serial number of the module.

All features that can be enabled by this card are listed on the back of the card.

Figure 1-6. Back of the Activator Card



Note: In addition to the Activation Cards, licensing features can be enabled using a file on disk or by entering an initialization bitstream from the keyboard. Additional licensing features can be added to the module later through a separate PO process.

1.2.4 Module Warrant File (nCipher)

Every nShield HSM Module comes with a warrant file generated by nCipher. This file provides cryptographic proof of module origin (explained in the key management section of the Secure Production Programming Solution (SPPS) User Guide). The warrant file is provided through the HSM Module purchase process.

1.2.5 HSM Module License File (Microchip)

Microchip provides a Microchip-generated license file that binds the user-created Security World with one or more HSM modules through their serial numbers.

1.3 System Requirements

The M-HSM server can run on Windows 7 x64 Pro, Windows 8.1 x64 operating systems, or Windows 10 x64. Server software is installed on a dedicated physical machine with one nShield Edge or Solo HSM module attached.

Note: It is possible to use a virtual machine to run the HSM server. However, Microchip has only validated M-HSM server functionality on the nShield Edge module using a VMWare virtual machine. Validation was performed using the nCipher-suggested method of connecting the Edge module directly to the host system and then giving the virtual machine module access through a virtual COM interface added to the host system by the module driver. See the *nShield Edge and Solo User Guide for Windows* for setup instructions.

1.3.1 Acquire M-HSM Components

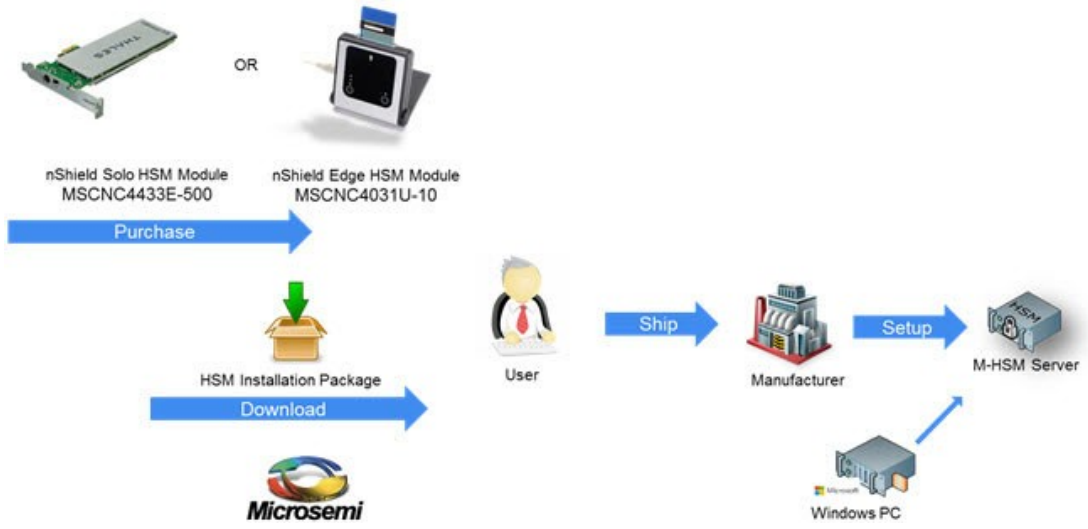
HSM hardware modules are purchased directly from Microchip. Every module comes with the components described in section Security World and HSM Modules.

Following is the list of M-HSM components. Figure 1-7 provides a high-level flow view.

- nShield Edge or Solo HSM Module
  - Module
  - Card reader (Solo module only. Edge module has integrated card reader)
  - Mounting hardware for regular and compact desktop form factors (Solo module only)
  - Set of Security World cards
  - Activator card (additional licensing features can be provided in a separate file)
- Warrant File in KLF format (created by nCipher, supplied by Microchip or requested from nCipher support)

- Licensing file (created and provided by Microchip after a Security World UUID is issued and serial number of the HSM module(s) is known)
- User provides PC with supported operating systems installed (see section System Requirements)
- M-HSM Installation Utility (download from Microchip website)
  - Third-party software prerequisite packages
  - nCipher nShield standard software
  - M-HSM Server software, including SEE Machine images

Figure 1-7. Acquiring M-HSM Parts



2. M-HSM Installation and Setup Scenarios

This section describes the following installation and setup options:

1. Initial setup:
   - 1.1. Install all required software components.
   - 1.2. Update all required M-HSM server configuration files.
   - 1.3. Install the HSM module.
   - 1.4. Provision the M-HSM server.
     - 1.4.1. Create new Security World and Administrator Card Set (ACS).
     - 1.4.2. Generate all required M-HSM server keys.
     - 1.4.3. Exchange public encryption and public verify keys with the U-HSM.
     - 1.4.4. Import Diversified Factory Key Database (DFK DB) and the manufacturing keys received from the U-HSM.
2. Post-Installation (maintenance) steps:
   - 2.1. Upgrade the HSM module firmware.
   - 2.2. Replace the HSM module.
   - 2.3. Import public keys of the U-HSM.
   - 2.4. Export public keys for sending to a U-HSM.
   - 2.5. Import new DFK DB and manufacturing keys for the target Microchip device(s).
3. Replication of the existing M-HSM server (creates a copy of already provisioned M-HSM server):
   - 3.1. Install all required software components.
   - 3.2. Copy over Security World from the source M-HSM server.
   - 3.3. Copy over the M-HSM server software and configuration files.
   - 3.4. Copy over the existing DFK DB.
   - 3.5. Replace the HSM module.

3. Initial M-HSM Server Installation and Setup

This section describes how to install and set up a new M-HSM server.

Note: Text highlighted in red in this section indicates commands and other information to take note of.

3.1 Software Installation

This section explains the manual installation process for setting up the M-HSM server.

One of the supported operating systems must be installed with all the security and stability updates applied.

1. Microsoft Visual C++ 2010 Redistributable Package (x64) available from Microsoft.
2. Visual C++ Redistributable for Visual Studio 2012 (x64) available from Microsoft.
3. .NET Framework 4.0 or up available from Microsoft.
4. FTP Server (for example, FileZilla).
5. Java Runtime 2 32-bit available from Oracle.
6. nShield Security World Software (coming with the HSM modules or can be requested from nCipher support):
   - For Windows 7 x64 Pro and Windows 8.1 x64 please use version 11.70.00.
   - For Windows 10 x64 please use version 12.50.4 with Compatibility Package v 1.0.0.
   - The installation disk contains a folder with documentation in PDF format.
   - Installation of SNMP client can be ignored as the software for this implementation does not use it.

3.2 M-HSM Server Software Installation

1. Create the top level directory.
   Note: This user guide uses `C:\Microsemi` as an example.
2. Unpack all files and subdirectories from the provided zip file under the *M-HSM* directory and copy to `C:\Microsemi`.
3. Verify that the following additional subdirectories exist:
   - `C:\Microsemi\DFKDB`: This location stores imported DFK databases.
   - `C:\Microsemi\JobDB`: This location stores job ticket database files.
   - `C:\Microsemi\JobDB\JobDBArchive`: Folder for archiving completed job ticket database files.
   - `C:\Microsemi\Logs`: For log files.

3.3 HSM Hardware Module Installation

This section describes the steps to connect a new HSM module to the PC. If you are replacing the HSM module on a configured M-HSM server, start from section HSM Module Replacement. If you are replicating the M-HSM server, see section Set Up a New HSM Module.

The M-HSM server requires the presence of a single HSM module. After the installation of nShield software, as shown in section Software Installation, the system must have module drivers and all nShield utilities installed.

3.3.1 Connect the HSM Module to the PC

Follow the instructions in the *nShield Edge and Solo User Guide for Windows* to physically connect the module to the PC.

Once the module is connected, read the module status with the `nfkminfo` utility. The output of `nfkminfo` shows information about the attached module, such as ESN (serial number), status, and so on. If the module is not detected or in the failed state, restart the nfast server and read the module status again.

```
net stop "nfast server"
```

```
net start "nfast server"
```

Note: If necessary, the HSM module can be erased to the factory state using the new-world command. For example, `new-world -e -m1` erases the module with the ID = 1 to the factory state. This operation is done in the pre-initialization mode.

3.3.2 Upgrade HSM Module Firmware

This section provides instructions for nCipher firmware upgrade. This firmware physically resides inside the HSM module and is different from the Microchip-provided SEE machine.

3.3.2.1 Firmware Revisions

The firmware revision of the HSM module that is used in SPPS must be approved by Microchip. The list of the approved firmware revisions is available in the *M-HSM Release Notes*. Additional instructions about firmware revisions may be published through Microchip security advisories.
Note: Any HSM firmware revision that is not approved by Microchip is not guaranteed to work and is not guaranteed to satisfy security requirements of the SPPS solution. The use of such firmware revisions is done at customer's own risk.

nCipher HSM module firmware images are available in the HSM Installation media, or can be obtained directly from nCipher customer service.

Note: Installation media may include various versions of the firmware that might be FIPS certified or awaiting FIPS certification. Your choice depends on the security policies of your organization.

3.3.2.2 Compatibility of Firmware Revisions

WARNING The firmware upgrade might be non-reversible. The following section provides important details.

nCipher HSM module firmware has two versioning characteristics:

- Firmware revision number
- Version Security Number (VSN)

The firmware revision number identifies the individual version of the firmware, while the VSN can group multiple revisions together and is used to restrict revision downgrade, so that the intruders cannot move a module to the firmware with known security issues. The downgrade is possible to any firmware revision with the same VSN as the one in the module. The upgrade can be done to any revision with the same or higher VSN number.

Information about firmware revisions and their respective VSN numbers is available on the Security World installation media of firmware upgrade media distributed as part of nCipher security advisories.

3.3.2.3 Read the HSM Module Firmware Revision Information

The current revision of the HSM firmware can be checked using the "enquiry" Security World utility. An example of reading the firmware revision number is shown in Figure 3-1.

Figure 3-1. Reading HSM Module Firmware Revision

```
Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        1301-C8A9-BEF7
 mode                 operational
 version              2.55.1
 speed index          544
 rec. queue           19..152
 level one flags      Hardware HasTokens
 version string       2.55.1cam7 built on Jul 08 2015 14:24:15
 checked in           000000004856847b Mon Jun 16 08:19:23 2008
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasPollCmds
FastPollSlotList HasSEE HasKLF H
asShareACL HasFeatureEnable HasFileOp HasPCIPush HasKernelInterface HasLongJobs ServerHasLongJobs
AESModuleKeys NTokenCm
ds JobFragmentation LongJobsPreferred Type2Smartcard ServerHasCreateClient HasInitialiseUnitEx
 module type code     7
 product name         nC1003P/nC3023P/nC3033P
 device name          #1 PCI bus 6 slot 5
 EnquirySix version   6
 impath kx groups     DHPrime1024 DHPrime3072
 feature ctrl flags   LongTerm
 features enabled     GeneralSEE StandardKM
 version serial       26
 rec. LongJobs queue  18
 SEE machine type     PowerPCSXF
 supported KML types  DSAp1024s160 DSAp3072s256
```

3.3.2.4 Upgrade Firmware

This section provides general guidance for the firmware update. If the firmware upgrade is done due to a Microchip security advisory, follow the instructions in the advisory. General description of the upgrade process and instruction for switching HSM module into specific mode is available in the *nShield Edge and Solo User Guide for Windows*.

Note: The firmware upgrade process erases all information contained in the module except the enabled licensing features explained in section Enable the Module Licensing Feature.

Perform the following steps for firmware upgradation:

1. Switch the module mode to the Maintenance mode. To switch the nShield Edge module to the maintenance state, use the **Mode** button to change mode to the M (Maintenance mode) and then push and hold down the **Clear** button to activate the M state.
   The mode switching on the Solo HSM module is done by moving the three-position switch to the M state and resetting the module using a paper clip. Both module controls are located on the Solo module and are accessible outside the PC box. For more detailed mode switching instructions, see the *nShield Edge and Solo User Guide for Windows*.
2. Load the new firmware using the `loadrom` command, pointing to the firmware image.
   Note: When entered, the `loadrom` command starts without prompting for user confirmation.

   Figure 3-2 shows an example of the output during firmware upgrade.

Figure 3-2. Firmware Upgrade

```
C:\>loadrom -m1 C:\shared\FWUpgrade\firmware\2-55-1\ncx1z-26.nff

 version 2.50.16cam18 built on Sep 23 2010 20:36:19
programming module #1
module erased
starting programming *+
firmware integrity mech. DSAhSHA256
module accepted signature
block size allowed by unit 1910, using 1910
loading chunk 0 ++++++++++++++++++++++++++++++++++ programming done
loading chunk 1 ++++++++++++++++++++++++++++++++++ programming done
loading chunk 2 ++++++++++++++++++++++++++++++++++ programming done
loading chunk 3 ++++++++++++++++++++++++++++++++++ programming done
loading chunk 4 ++++++++++++++++++++++++++++++++++ programming done
loading chunk 5 ++++++++++++++++++++++++++++++++++ programming done
loading chunk 6 ++++++++++++++++++++++++++++++++++ programming done
loading chunk 7 ++++++++++++++++++++++++++++++++++ programming done
loading chunk 8 ++++++++++++++++++++++++++++++++++ programming done
loading chunk 9 ++++++++++++++++++++++++++++++++++ programming done
loading chunk 10 +++++++++++++++++++++++++++++++++++ programming done
loading chunk 11 +++++++++++++++++++++++++++++++++++ programming done
programming done
```

3. Switch module mode to the Pre-Init mode.
4. Initialize the module using the `Initunit` command.

Figure 3-3. Module Initialization during Firmware Upgrade

```
C:\>initunit
Initialising Unit 1 (SetNSOPerms)
Setting dummy HKNSO
Module Key Info:
HKNSO  is:C8 39 AC 0D EE D9 A9 65 AC F9 12 0F F2 02 F9 79 8C 2C A4 5D
HKM[0] is:FD 2D 47 53 86 05 CF F4 27 53 1A 01 FD 8D E8 02 00 DD C7 55
```

5. Confirm that the module firmware revision is upgraded as expected using the `enquiry` command.

3.3.3 Enable the Module Licensing Feature

This section describes how to enable specific HSM module features.

Note: To activate new license features using the `Feature Enabling Tool (fet)` utility, the module must be switched to the pre-initialization mode.

To run the custom firmware created for the SPPS system (SEE Machine), the module must have the "SEE Activation (EU+10)" feature enabled, as shown in sample Figure 3-4. Feature status of the module can be checked or activated using `fet`.

Figure 3-4. Sample Output of Feature Activation Tool

```
C:\>fet

                              Feature Enable Tool
                              ===================

                        payShield Activation
                         |  ISO Smart Card Support
                         |   |  Remote Operator
                         |   |   |  Korean Algorithms
                         |   |   |   |  SEE Activation (EU+10)
                         |   |   |   |   |  SEE Activation (Restricted)
                         |   |   |   |   |   |  CodeSafe SSL
                         |   |   |   |   |   |   |  Elliptic Curve algorithms
                         |   |   |   |   |   |   |   |  Elliptic Curve MQV
                         |   |   |   |   |   |   |   |   |  Accelerated ECC
Mod   Electronic         |   |   |   |   |   |   |   |   |   |
No.  Serial Number
 1  586F-B963-9146 -- NO  NO  NO  NO  YES NO  NO  YES YES  NO

0. Exit Feature Enable Tool.
1. Read FEM certificate(s) from a smart card or cards.
2. Read FEM certificate from a file.
3. Read FEM certificate from keyboard.
4. Write table to file.

Enter option :
```

Choose option one and activate the features listed on your Activator Card (see section Activator Card and Feature Licensing (nCipher)). The fet auto-detects the card and performs activation. New activation status is printed on the screen.

If your Activator Card does not include the "SEE Activation (EU+10)" feature, it might have been provided to you in a separate file. The file name includes the module serial number, for example: *USProdCGT3-01253481317_SEEUE_8FD6-2609-F7A2.txt*

This file can be used during activation independently from the Activator Card by selecting option two.

If you plan to use advanced security features in Microchip devices, such as ECC PUF key modes, make sure that the "Elliptic Curve algorithms" and "Elliptic Curve MQV" are activated as shown in the preceding example.

Note: Erasing a module to the factory settings does not remove licensing features enabled using the `fet`. Licensing feature reset can only be done at the factory.

3.4 M-HSM Server Provisioning

3.4.1 Create the Security World

Security World is created with the `New-World` utility documented in the *nShield Edge and Solo User Guide for Windows*. The module must be moved to the pre-initialization mode.

The new-world utility has the following options:

- **-i**: Creates a new Security World.
- **-m**: Specifies ID of the physical HSM module to be added to the Security World.
- **-i**: Creates a new Security World.
- **-Q**: Specifies the minimum number of smart cards needed from the ACS to authorize a feature and the total number of smart cards to be used in the ACS. This example has a total of two cards, with only one card needed to authorize a feature.

- **-c**: Specifies the type of key to use for the new Security World. This example uses the AES key.

The example shown in Figure 3-5 creates a new Security World.

During creation of the Security World, the user is prompted to insert and initialize all ACS cards specified by the -Q option.

Figure 3-5. Sample Output from Creation of New Security World

```
C:\Microsemi\Tools>new-world -i -m 1 -Q 1/2 -c DLf1024s160mRijndael dseeall

Create Security World:
 Module 1: 0 cards of 2 written
 Module 1 slot 0: empty
 Module 1 slot 0: unknown card
 Module 1 slot 0:- no passphrase specified - overwriting card
 Module 1: 1 card of 2 written
 Module 1 slot 0: remove already-written card #1
 Module 1 slot 0: empty
 Module 1 slot 0: unknown card
 Module 1 slot 0:- no passphrase specified - overwriting card
Card writing complete.

security world generated on module #1; hknso = 15d0780e37252b3a1d8bf339a9bd6d779d1991bc
```

Notes:

- The values of the `hknso` parameters can be used to uniquely identify the Security World.
- If the module is not in the pre-initialization state, creation of the Security World may encounter an error:

  Figure 3-6. Error Message if Module is not in Pre-Initialization State

  ```
  12:46:57 WARNING: Module #1: Module has failed
  new-world: module 1 not suitable: module key type Rijndael not supported
  new-world: Aborting world operation.
  ```

The new Security World is a file that is created in the following location: `%NFAST_KMDATA%\local`
Note: This location also contains all other related security keys.

Once the Security World is created, the module must be moved to the operational mode.

3.4.2 Read the Status of the Security World

The status information related to the existing Security World and attached module(s) can be viewed using the `nfkminfo` utility. See the *nShield Edge and Solo User Guide for Windows* for more information.

This status information contains several important fields. The *hknso* and *hkm* fields allow the user to uniquely identify the specific Security World.

Once a module is moved to the operational state, the module status read by `nfkminfo` utility must indicate "usable" module state.

Figure 3-7 shows sample output of the `nfkminfo` utility.

Figure 3-7. Status of the Security World

```
C:\Microsemi\Tools>nfkminfo
World
 generation  2
 state       0x1f250000 Initialised !Usable Recovery !PINRecovery !ExistingClient RTC NVRAM FTO !Alw
aysUseStrongPrimes SEEDebugForAll
 n_modules   1
 hknso       15d0780e37252b3a1d8bf339a9bd6d779d1991bc
 hkm         e113ba16497e0576b99bd2f0150f126204426507 (type Rijndael)
 hkmwk       1d572201be533ebc89f30fdd8f3fac6ca3395bf0
 hkre        c59ca14ee277dca5497b2e4c5a113d238b613c0b
 hkra        078ea5ba02d3300c462e9c84988e673a09896dcb
 hkmc        4f18cdf70289ee823520bc252060ebf97eb61032
 hkrtc       90c54dafcb5836ccec08d2cd75776cb5d53d6a6c
 hknv        b8b80d9794b98588dddfedf650bfd59a7bed1765
 hkdsee      6fc988762e441e44de4a5c1a6ba6b34a2fb47aa2
 hkfto       3a70b6e939cc3ee779ddae9ce5fb79cb067c42c0
 hkmnull     0100000000000000000000000000000000000000
 ex.client   none
 k-out-of-n  1/2
 other quora m=1 r=1 nv=1 rtc=1 dsee=1 fto=1
 createtime  2015-01-13 23:29:09
 nso timeout 10 min
 ciphersuite DLf1024s160mRijndael

Module #1
 generation 2
 state      0xa InitMode
 flags      0x0 !ShareTarget
 n_slots    2
 esn        586F-B963-9146
 hkml       ac4e6e3e02f27d7a7d0a182077546a62ec390513

Module #1 Slot #0 IC 3
 generation    1
 phystype      SmartCard
 slotlistflags 0x2 SupportsAuthentication
 state         0x4 Admin
 flags         0x0
 shareno       2
 shares        LTNSO LTM LTR LTNV LTRTC LTDSEE LTFTO
 error         OK
No Cardset

Module #1 Slot #1 IC 0
 generation    1
 phystype      SoftToken
 slotlistflags 0x0
 state         0x2 Empty
 flags         0x0
 shareno       0
 shares
 error         OK
No Cardset

No Pre-Loaded Objects
```

3.4.3 Install the SEE Integ Key

The SEE Integ Key links the SEE firmware and keys used in SPPS (see the Secure Production Programming Solution (SPPS) User Guide for details). It must be installed before any other keys can be generated or exported.

The key is installed by simply copying its file *key_seeinteg_userdata-signer* located under the SEE folder of the M-HSM server directory to the Security World data folder: `%NFAST_KMDATA%\local`.

For example, `copy C:\Microsemi\SEE\key_seeinteg_userdata-signer%NFAST_KMDATA%\local`

Proper installation of the SEE Signer Key can be confirmed using the `nfkminfo -k` command:

Figure 3-8. Confirming Correct Installation of SEE Signer Key

```
C:\Program Files (x86)\nCipher\nfast\bin>nfkminfo -k

Key list - 1 key
 AppName seeinteg             Ident userdata-signer
```

3.4.3.1 Get Hash of SEE Integ Key

The hash of the Signer Key is used for key identification and referencing key signer during various operations, such as, creation of the HSM private/public key pairs.

The hash value of the Key Signer can be retrieved using `nfkminfo`:

nfkminfo -k seeinteg userdata-signer | find "hash"

See the following example:

```
C:\Microsemi\Tools>nfkminfo -k seeinteg userdata-signer | find "hash"

hash      e0d5146a74ec125f22d4b15088d424b963b88109
```

3.4.4 Create NVRAM Partition in HSM Module

This step uses the `nvram-sw` utility to create a storage partition in non-volatile memory of the HSM module for storing information that must be physically unclonable. The example in Figure 3-9 shows output during NVRAM partition creation.

To run this action:

- The module must be in the operational mode.
- The ACS (admin) card must be inserted into the card reader according to quorum number specified during creation of the Security World.

Enter the following command to create NRAM:

```
nvram-sw.exe -a -b 8096 -n udsigner -k seeinteg,userdata-signer
```

The -b parameter specifies memory size. The value of 8096 specifies partition size. This value is fixed in the current version of the M-HSM server.

Note: The -k parameter must follow the exact format: comma separated values with no spaces.

Figure 3-9. Creating ENVM Storage Inside HSM Module

```
C:\>nvram-sw.exe -a -b 8096 -n udsigner -k seeinteg,userdata-signer
Load Admin Card (for KNV):
 Module 1 slot 0: `SEEOCS'
 #2 Module 1 slot 0: empty
Card reading complete.
```

3.4.4.1 Remove Existing NVRAM Partition

If the NVRAM partition already exists in the module, it can be removed by entering the following command:

```
nvram-sw.exe -d -n udsigner
```

Note: Deletion of the existing NVRAM partition erases all tickets loaded into the module.

3.4.5 Configure the M-HSM Server and Tools

This section provides setup instructions for the M-HSM server. It assumes that the directory structure for the M-HSM server was created in the default location `C:\Microsemi`.

3.4.5.1 Update Server and Tools Configuration File

The *M-HSMMaster.config* file contains settings for the M-HSM server. Currently, there are two separate configuration files with the same name and identical content. For the default installation location, the file path is:

- `C:\Microsemi\Server\M-HSMMaster.config`, and
- `C:\Microsemi\Tools\M-HSMMaster.config`

Change the following settings as shown:

1. DFK database location—confirm that the location matches actual path:
   <add key=`G4HSMAPI.DFKDBPath` value=`C:\Microsemi\DFKDB` />
2. Ticket database location—confirm that the location matches actual path:
   <add key=`G4HSMAPI.JobTicketDBPath` value=`C:\Microsemi\JobDB`/>
3. Ticket archive directory:
   <add key=`G4HSMAPI.JTPLogArchivePath` value=`C:\Microsemi\JobDB\JobDBArchive`/>
4. M-HSM UUID 40 symbols long hex string obtained from Microchip (00..02 in this example):
   <add key=`My_UUID` value=`0000000000000000000000000000000000000002`/>
5. SEEK Secret key: `g4cm-seesk-<M_HSM_UUID>` (00..02 in this example):
   <add key=`<add key="G4HSMAPI.CSEEKey" value="g4cm-seesk-0000000000000000000000000000000000000002`/>
6. Option to automatically remove tickets pending job file import. This allows the HSM server to automatically remove tickets that do not have an associated job file loaded. By default, this service is off. To use this automatic ticket cleanup service, the user must turn it on and specify the time interval (in seconds) at which the service runs. The same time interval is also used to specify the maximum lifetime of tickets pending job file. This helps free up memory inside the HSM module.

   <add key=`TicketCleanup.Service` value=`off/`>

   <add key=`TicketCleanup.TimeoutValue` value=`86400/`> <!--TimeoutValue is in seconds.-->

3.4.6 Generate the ISK Key (*g4see-isk)

The ISK key is a global system key used for internal system functions, such as import U-HSM public keys (seepk and seespk).

Generate the ISK key as follows:

1. Open the command prompt as an administrator and change directory to `C:\Microsemi\Tools`.
2. Execute the script as shown in the following sample output.
   "%nfast_home%\python\bin\python.exe" C:\Microsemi\Tools\gensymmkey.py -u userdata-signer-i g4see-isk

Figure 3-10. Sample Output from Generation of ISK Key

```
C:\Microsemi\Tools>"%nfast_home%\python\bin\python.exe" C:\Microsemi\Tools\gensymmkey.py -u
userdata-signer -i g4see-isk
=========================================================
= Generating symmetric key with ExportAsPlain enabled
=
= KeyIdent:      simple/g4see-isk
= KeyHash:       7a7895eb 081498b9 0f05d9de 257ae43d 7896dacd
=   SEE App KeyIdent:  seeinteg/userdata-signer
=   SEE APP KeyHash:   57827118 b0e20b11 2ff56be0 820a6020 7154b8a7
=
= Open group perms:  DuplicateHandle|ReduceACL|GetACL
= SEE App perms:     ExportAsPlain|GetAppData
=========================================================

Success!  Generated key simple/g4see-isk
```

3.4.7 Install HSM Module License File

The license file is issued by Microchip and binds the UUID used by Security World and one or more HSM modules.

Once available, this file must be put in the Server and Tools directories of the current installation. The file name follows the pattern: *<M_UUID>.g4sl*. For example, 00000000000000000000000000000000000000002.g4sl.

3.4.8 Set Up SEE Machine Firmware for Loading into HSM Module

This step configures the system to load firmware into the HSM module. The `loadsee-setup` command sets up paths to the SEE Machine files. The following figure shows the sample output.

Figure 3-11. Setting Up SEE Firmware Loading

```
loadsee-setup -m 1 -s -p g4cmsee -M C:\Microsemi\SEE\M-HSMsee-edg.sar -U
C:\Microsemi\SEE\userdata.sar

Module #1 has an existing configuration:

Module #1:
  Machine file:             C:\Microsemi\SEE\M-HSMsee-edg.sar
  Encryption key:
  Signing key hash:
  Userdata file:            C:\Microsemi\SEE\userdata.sar
  WorldID published object: g4cmsee
  Postload helper:
  Postload args:

Erase this configuration? (yes/no): yes
Module #1 new SEE configuration saved, new configuration follows:

Module #1:
  Machine file:             C:\Microsemi\SEE\M-HSMsee-edg.sar
  Encryption key:
  Signing key hash:
  Userdata file:            C:\Microsemi\SEE\userdata.sar
  WorldID published object: g4cmsee
  Postload helper:
  Postload args:
```

Different HSM module types require different firmware images. All images are located in the SEE folder and have the extension *sar*. The *userdata.sar* file works with any module type.

Module Type	Firmware File
nShield Edge	M-HSMsee-edg.sar
nShield Solo	M-HSMsee-ppc.sar

The next step is to confirm that the SEE Machine firmware has loaded successfully. Use the *GetLoadingSEEName.bat* script in the Utils folder, as shown in Figure 3-12. The SEE Machine firmware is loaded when the `-MemAllocUser` variable reads a non-zero value.

Note: Actual loading of the SEE firmware after setting it up with the `loadsee-setup` command might take a few minutes for the slower Edge module. During that period, `-MemAllocUser` remains 0.

Figure 3-12. Confirming Loading of SEE Firmware

```
C:\Microsemi\Tools>C:\Microsemi\Utils\GetLoadingSEEName.bat

WorldID = 'g4cmsee'
         -MemAllocUser         933888
If MemAllocUser is 0, SEE is not loaded
```

If the module cannot load the firmware, check the correctness of the parameters specified during the `loadsee-setup` step and repeat the attempt, making sure the proper module type is selected.

3.4.9 Generate the SEE Private/Public Encryption and Signing Keys

The SEE Key pairs are created to provide secured exchange of information between U-, M-, and MFG-HSM servers. One pair of keys is used for encryption and decryption and the other pair is used for creating and verifying digital signatures.

3.4.9.1 Obtain the Manufacturer UUID from Microchip

Manufacturer UUID (M_UUID) is a 40-symbol hex string identifier that is assigned by Microchip through the Microchip Portal (see the Secure Production Programming Solution (SPPS) User Guide for details).

Example of the Manufacturer UUID: 0000000000000000000000000000000000000002

Note: UUID must have all lower-case characters.

Private/Public SEE keys must use the Manufacturer UUID assigned by Microchip.

Once the UUID value is available, update the tag in both *M-HSMMaster.config* files, under the Server and Tools directories, as explained in section Update Server and Tools Configuration File.

3.4.9.2 Generate the M-HSM Private Keys

1. Open the command prompt as an administrator and change directory to `C:\Microsemi\Tools`.
2. Create the SEE Key for encryption using the `M-HSMGenImp` utility:
   M-HSMGenImp -p g4cmsee -g -c *<key_signer_hash>* **-n g4cm-seesk-**<*M_HSM_UUID*> *M_HSM_UUID:* Microchip-assigned UUID

   The "-c" flag must be used as shown in this example. It corresponds to the userdata-signer key installed during the installation of the SEE Integ key (see section Install the SEE Integ Key).

   The following figure shows a sample:

   Figure 3-13. Creating SEE Key for Encryption and Decryption

```
C:\Microsemi\Tools>M-HSMGenImp -p g4cmsee -g -c e0d5146a74ec125f22d4b15088d424b963b88109 -n g4cm-
seesk-0000000000000000000000000000000000000002
Starting to generate SEE RSA key...
SEE RSA key: g4cm-seesk-0000000000000000000000000000000000000002  ...generated
```

   The created key is stored in the Security World directory as follows (with the highlighted part corresponding to the Manufacturer UUID):

```
key_simple_g4cm-seesk-0000000000000000000000000000000000000002
```

Once the key is generated, it must be set up in both *M-HSMMaster.config* files, in the Server and Tools directories, as described in section Update Server and Tools Configuration File.

3. Create the SEE Key for signing using the `M-HSMGenImp` utility:
   M-HSMGenImp -p g4cmsee -g -c *<key_signer_hash>* **-n g4cm-seessk-**<*M_HSM_UUID*> **-S**

   All of the parameters are same as in step 2 with the exception of name (that is, seessk vs. seesk) and a flag. The "-S" flag corresponds to generating the key for the signing operation instead of for encryption.

   The following figure shows a sample.

   Figure 3-14. Creating SEE Key for Signing and Verifying

```
C:\Microsemi\Tools>M-HSMGenImp -p g4cmsee -g -c e0d5146a74ec125f22d4b15088d424b963b88109 -n g4cm-
seessk-00000000000000000000000000000000000000002 -S
Starting to generate SEE RSA key...
SEE RSA key: g4cm-seessk-00000000000000000000000000000000000000002 ...generated
```

   The created key is stored in the Security World directory as follows (with the highlighted part corresponding to the Manufacturer UUID):

```
key_simple_g4cm-seessk-00000000000000000000000000000000000000002
```

3.4.9.3 Export the M-HSM Public Keys

This step exports the public component of the M-HSM SEE keys for importing into other HSM machines for secure information exchange. One public key is used by HSM servers to encrypt data that is to be sent back to this M-HSM server, and the other public key verifies the signature of data sent out from this M-HSM server.

3.4.9.3.1 Set Up the Warrant File

Before starting the key export, make sure to copy the HSM module warrant file from nCipher into the Tools directory. This file contains a cryptogram that identifies the origin of the HSM module. The file name follows the format:

warrant-[ESN].txt

Here, ESN is the module serial number that can be printed using the `nfkminfo` utility. The following is an example of the warrant file copied into the Tools directory:

```
C:\Microsemi\Tools\warrant-586F-B963-9146.txt
```

3.4.9.3.2 Export Public Key for Encryption

Enter the following command to export:

`ExportSeekey.bat g4cm-seesk-`<*M_UUID*>

This file is placed in the current directory (Tools, in this case). The following shows a sample output:

Figure 3-15. Export of SEE Public Key for Encryption

```
C:\Microsemi\Tools> ExportSeeKey.bat g4cm-seesk-00000000000000000000000000000000000000002
C:\Microsemi\Tools>"C:\Program Files (x86)\nCipher\nfast\python\bin\python.exe" makekeypackage.py -
i g4cm-seesk-00000000000000000000000000000000000000002
Package data for key 'simple/g4cm-seesk-00000000000000000000000000000000000000002' written to file
'pkg-g4cm-seepk-00000000000000000000000000000000000000002-2db19054'
```

3.4.9.3.3 Export Public Key for Verifying Signature

Enter the following command to export:

`ExportSeekey.bat g4cm-seessk-`<*M_UUID*>

This file is placed in the current directory (Tools, in this case). The following figure shows a sample output:

Figure 3-16. Export of SEE Public Key for Verifying Signature

```
C:\Microsemi\Tools> ExportSeeKey.bat g4cm-seessk-00000000000000000000000000000000000000002
C:\Microsemi\Tools>"C:\Program Files (x86)\nCipher\nfast\python\bin\python.exe" makekeypackage.py -
i g4cm-seessk-00000000000000000000000000000000000000002
Package data for key 'simple/g4cm-seessk-00000000000000000000000000000000000000002' written to file
'pkg-g4cm-seespk-00000000000000000000000000000000000000002-091d1213'
```

Once exported, these files must be sent for further import into the U-HSM(s) that are preparing programming jobs for this M-HSM server.

3.4.10 Open the Server Port

To make the M-HSM server accessible to the clients running outside the host operating system, the firewall rules must be changed to open 8000.

3.4.11 Start the M-HSM Server

The M-HSM server can be executed from the command line or as a Windows service.

3.4.11.1 Command Line Mode

While it can be used for the normal server operation, the command line mode is best during initial M-HSM server setup and provisioning, because it prints out error messages directly to the screen and makes it easy for the user to start and stop M-HSM server during this process. However, this mode can only be used under the admin account.

3.4.11.2 Service Mode

The service mode is designed for normal M-HSM server operation and can be used under a non-admin account. The server configuration must be performed by the user with admin privileges.

While a non-admin user has restricted access to the system resources and services, the M-HSM Control Panel application allows a non-admin user to perform certain administration tasks of the M-HSM server.

For more details about service mode of execution and setup instructions, see section Running M-HSM Server as a Service.

Using M-HSM Server in Command Line Mode

The following steps require a user account with administrative privileges.

The M-HSM server executable *M-HSMServer.exe* is located in the Server directory:

For example, `C:\Microsemi\Server\M-HSMServer.exe`

1. Start the console window: type **cmd** in the Windows Start Menu window and right-click Command Prompt desktop app. Then, choose **Run as administrator**.
2. In the open console window, navigate to the "server" directory and type **m-hsmserver.exe**.

Upon startup, the server initializes a session with the HSM module. The following figure shows the output:

Figure 3-17. M-HSM Server is Initializing Session With HSM Module

```
C:\Microsemi\Server>M-HSMServer.exe
The service is running.
Info: Ticket cleanup service is running.
Initializing session...
Session is initialized.
Press <ENTER> to exit.
```

If the SEE machine firmware load is still in progress, the session initialization waits for the load to finish. The SEE machine firmware load takes place in the following cases:

- Turning on or restarting the PC hosting the M-HSM server.
- Restarting the nCipher nFast Server service that handles HSM modules.
- HSM module reinitialization via issuing Security World commands, such as `nopclearfail`.
- Setting up or changing settings for the SEE firmware load (for example, loadsee-setup).

Note: When a session is waiting for the SEE firmware to load, session initialization time depends on the module type, and may vary from one minute for a Solo module to four minutes for an Edge module, respectively.

Sample output after session initialization is finished after waiting for SEE firmware load, as shown in Figure 3-18.

Figure 3-18. M-HSM Server is Initialized

```
C:\Microsemi\Server>M-HSMServer.exe
The service is running.
Info: Ticket cleanup service is running.
Initializing session...
Waiting for the SEE firmware to load…
Session is initialized.
Press <ENTER> to exit.
```

The session can be terminated by pressing the **Enter** key:

Figure 3-19. M-HSM Server is Stopped

```
C:\Microsemi\Server>M-HSMServer.exe
The service is running.
Info: Ticket cleanup service is running.
Initializing session...
Session is initialized.
Press <ENTER> to exit.

Session is stopping…
Server is stopped.
```

Note: During the session, the server produces log output of the HSM invocations into: `C:\ProgramData\G4KMSServer\G4KMSHSMAPI.log`

Any error information outputs into:

`C:\Microsemi\Server\M-HSMServer.log`

Both the log files are important during failure analysis and can be sent to Microchip technical support for analysis.

3.4.12 Import the M-HSM Public Keys

The M-HSM server needs to import its own public verify key, so that it can securely remove the tickets. Use the `M-HSMGenImp` utility for import:

M-HSMGenImp -p g4cmsee -i -n g4cm-seespk-<M_UUID> **-a pkg-g4cm-seespk-**<M_UUID><HEXVALUE> **-k g4see- isk**

`M_UUID`: 40 hex characters long UUID for the imported M-HSM public key.

For example, 0000000000000000000000000000000000000002

`pkg-g4cm-seespk-<M_UUID><HEX VALUE>`: This is the container file on the disk with the signature verification key to be imported.

For example, `pkg-g4cm-seespk- 0000000000000000000000000000000000000002-705f18e9`

The resulting file is created in the Security World folder. Information about this key can be viewed using the `nfkminfo -k` command.

Example of the resulting key file:

`key_simple_g4cm-seespk-0000000000000000000000000000000000000002`

Figure 3-20 shows a sample output from key import.

Figure 3-20. Importing M-HSM Public Key

```
C:\Microsemi\Tools> M-HSMGenImp.exe -i -m 1 -p g4cmsee -n g4cm-seespk-
00000000000000000000000000000000000000002-k g4see-isk -a pkg-g4cm-seespk-
00000000000000000000000000000000000000002-705f18e9
RedeemTicket successful
Starting to import SEE public key...
Vimport successful
= 20 bytes
                              705f18e9 5ac25b2c fcb66b9c 62c7b069 849394b0
= 20 bytes
                              705f18e9 5ac25b2c fcb66b9c 62c7b069 849394b0
SEE public key, g4cm-seespk-00000000000000000000000000000000000000002, imported successfully
```

3.4.13 Import the U-HSM Public Keys

The M-HSM server needs the public keys of the U-HSM to send it information in a secure way and to verify the authenticity of the data.

Use the `M-HSMGenImp` utility for imports:

M-HSMGenImp -p g4cmsee -i -n g4cu-seepk-<*U_UUID*> **-a *pkg-g4cu-seepk*-**<*U_UUID*><HEX VALUE> **-k g4see-isk**

M-HSMGenImp -p g4cmsee -i -n g4cu-seespk-<*U_UUID*> **-a pkg-g4cu-seespk-**<*U_UUID*><HEX VALUE> **-k g4see-isk**

`U_UUID`: 32 bytes long UUID for the imported U-HSM public key.

For example, 00000000000000000000000000000001

`pkg-g4cu-seepk-<U_UUID><HEX VALUE>`: This is the container file on the disk with the encryption key to be imported.

For example, pkg-g4cu-seepk-00000000000000000000000000000001-5a4a52b3

`pkg-g4cu-seespk-<U_UUID><HEX VALUE>`: This is the container file on the disk with the signature verification key to be imported.

For example, `pkg-g4cu-seespk-00000000000000000000000000000001-0754c1eb`: The resulting files are created in the Security World folder.

Example of the resulting key files:

`key_simple_g4cu-seepk-00000000000000000000000000000001` and `key_simple_g4cu-seespk-00000000000000000000000000000001`.

Information about these keys can be viewed using the `nfkminfo -k` command. Figure 3-21 shows a sample output from key import.

Figure 3-21. Importing U-HSM Public Keys

```
C:\Microsemi\Tools> M-HSMGenImp -p g4cmsee -i -n g4cu-seepk-00000000000000000000000000000001 -a
pkg-g4cu-seepk-00000000000000000000000000000001-5a4a52b3 -k g4see-isk
RedeemTicket successful
Starting to import SEE public key...
Vimport successful
= 20 bytes
                              5a4a52b3 2c9dc635 a5511840 c5489833 0af6d21a
= 20 bytes
                              5a4a52b3 2c9dc635 a5511840 c5489833 0af6d21a
SEE public key, g4cu-seepk-00000000000000000000000000000001, imported sucessfully

C:\Microsemi\Tools> M-HSMGenImp -p g4cmsee -i -n g4cu-seespk-00000000000000000000000000000001 -a
pkg-g4cu-seespk-00000000000000000000000000000001-0754c1eb -k g4see-isk
RedeemTicket successful
Starting to import SEE public key... Vimport successful
= 20 bytes
                              0754c1eb 2c9dc635 a5511840 c5489833 0af6d21a
= 20 bytes
                              0754c1eb 2c9dc635 a5511840 c5489833 0af6d21a
SEE public key, g4cu-seespk-00000000000000000000000000000001, imported sucessfully
```

3.4.14 Import U-HSM Device Data

To perform programming actions, the M-HSM server receives and imports the following data:

- DFK DB: This database includes HSM-protected per-device Diversified Factory Keys (DFK) used for initial device programming.
- Manufacturing keys: These keys are per device type and can be imported multiple times (they are ignored, if they already exist).

For information on the DFK DB and manufacturing keys, see the Secure Production Programming Solution (SPPS) User Guide.

3.4.14.1 DFK Database and Manufacturing Keys

U-HSM prepares DFK DB for M-HSM, which contains information about DFK and manufacturing keys. This database is a file with the name following this pattern:

DFK-<U_UUID>.DFKDB, where U_UUID is the UUID of the U-HSM (this is not the M-HSM UUID).

For example, DFK-00000000000000000000000000000001.DFKDB.

M-HSM imports device information using the following command:

```
M-HSMImportDeviceData.exe <DFKDB_file>
```

This step imports DFKDB and device-type specific manufacturing keys. If any of those manufacturing keys have already been imported, the utility ignores them.

For each imported manufacturing key, a new file is created in the key folder of the Security World. The file has the following format: `key_simple_g4mf-klk-<device_key_uuid>`.

For example, `key_simple_g4mf-klk-10000000000000000000000000000000000000005`.

3.4.15 Restart the HSM Server

Perform the following steps to restart the server and ensure that the M-HSM server loads the new configuration correctly:

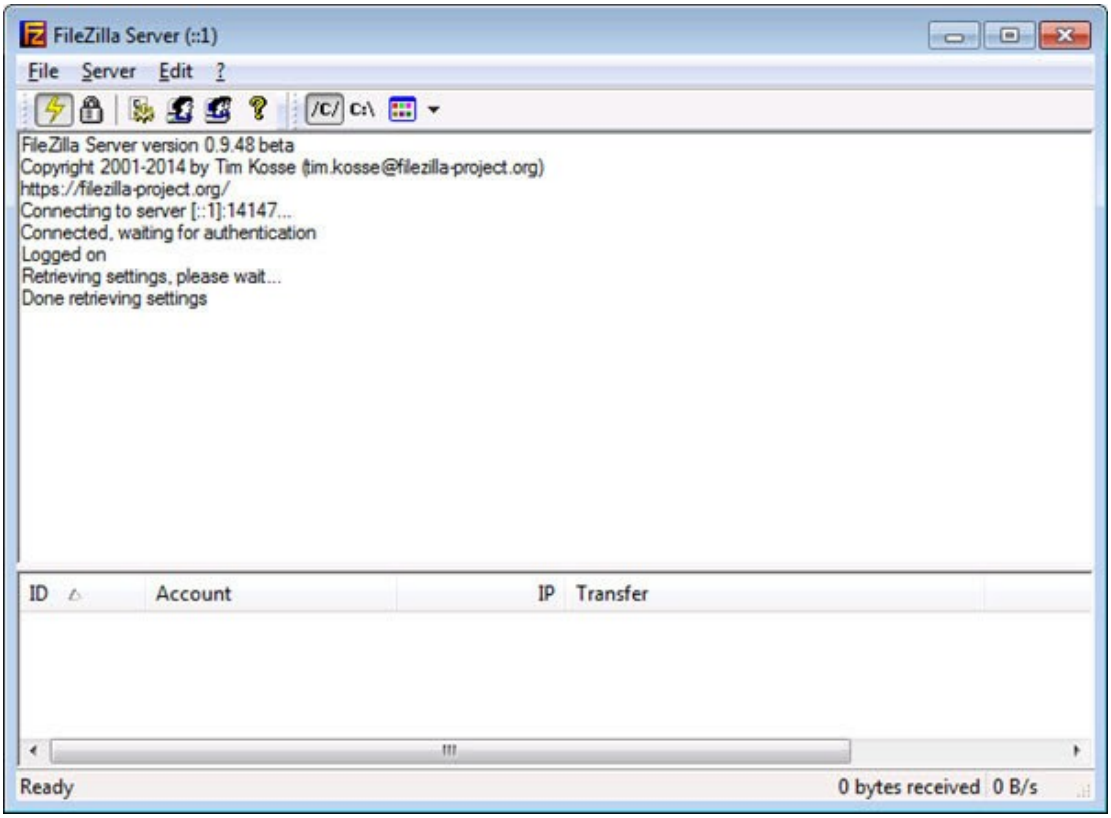
1. Stop *M-HSMServer.exe*.
2. Run "nopclearfail -c -m1".
3. Wait until the SEE machine is loaded, as shown in Figure 3-12.
4. Start *M-HSMServer.exe*.

3.5 FTP Server Setup

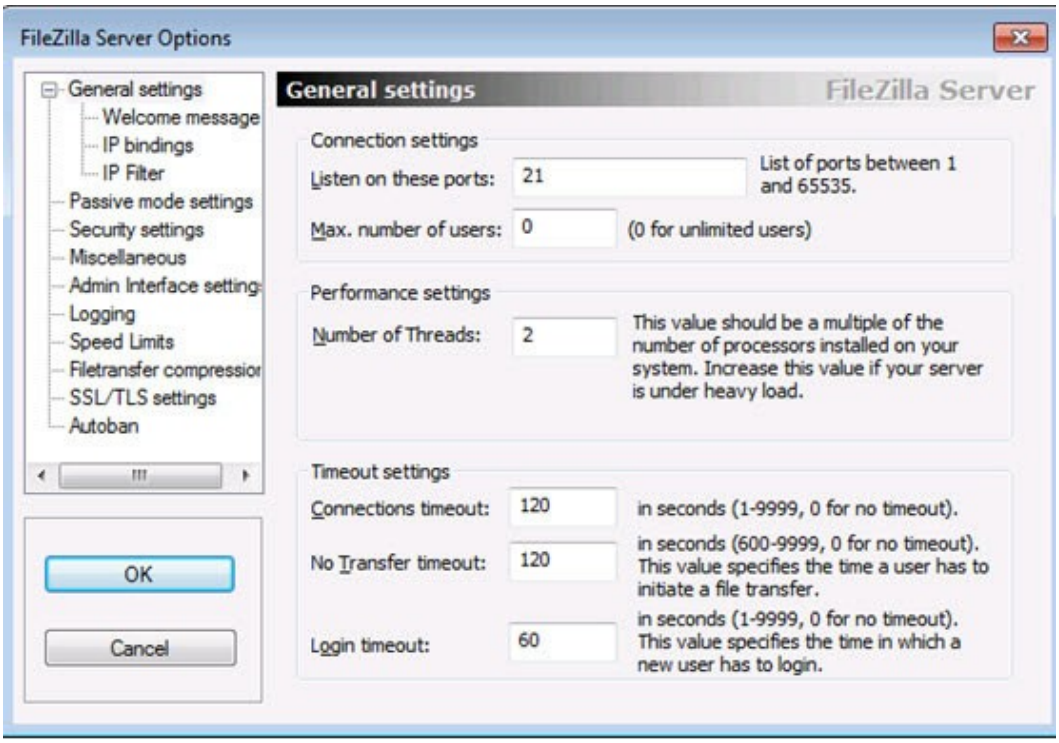
An FTP server is required on the M-HSM to provide access to the job status and job termination functions for the administrator on FlashProExpress. The server is used to retrieve information from the ticket database located in the directory specified by *M-HSMMaster.config* file (see section Update Server and ToolsConfiguration File for details).

The following example shows how to set up the FTP server using FileZilla. The FTP port is set to 21. The home directory is set to `C:\Microsemi\ftp`, and the ticket DB (/JobDB) is set to `C:\Microsemi\JobDB`.

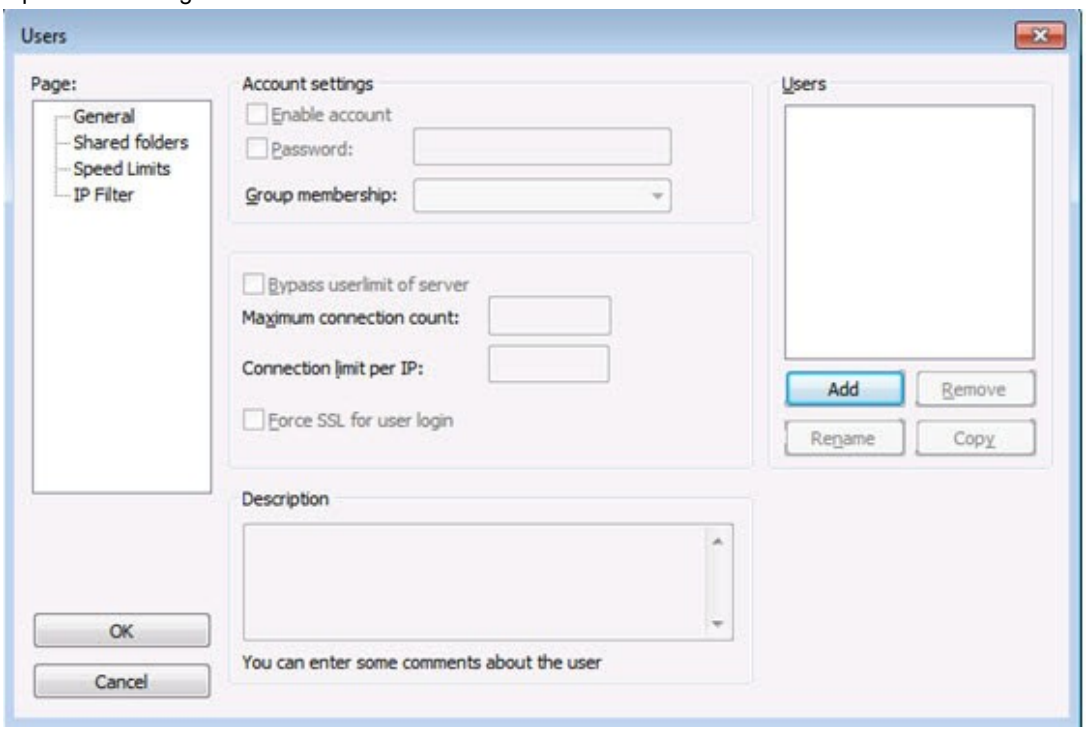
1. Open the FileZilla Server application.



2. Go to **Menu > Edit > Settings**, make sure that the default port is set to 21, and close the dialog box.

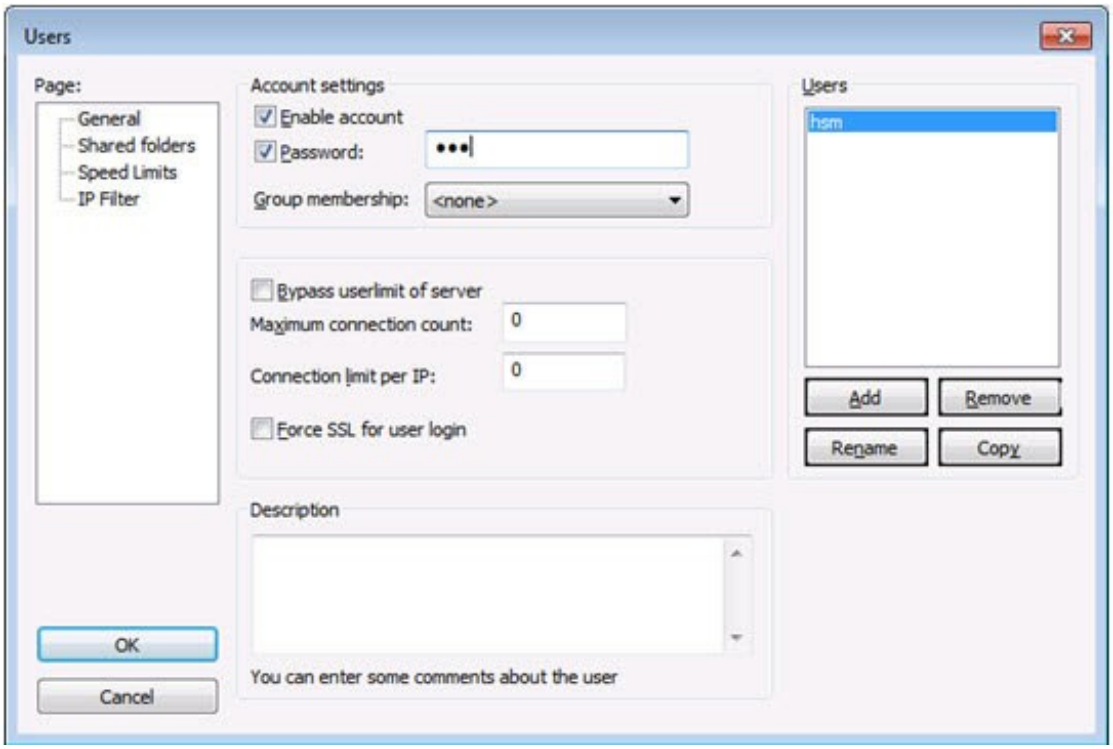


3. Open user settings: **Menu > Edit > Users**.

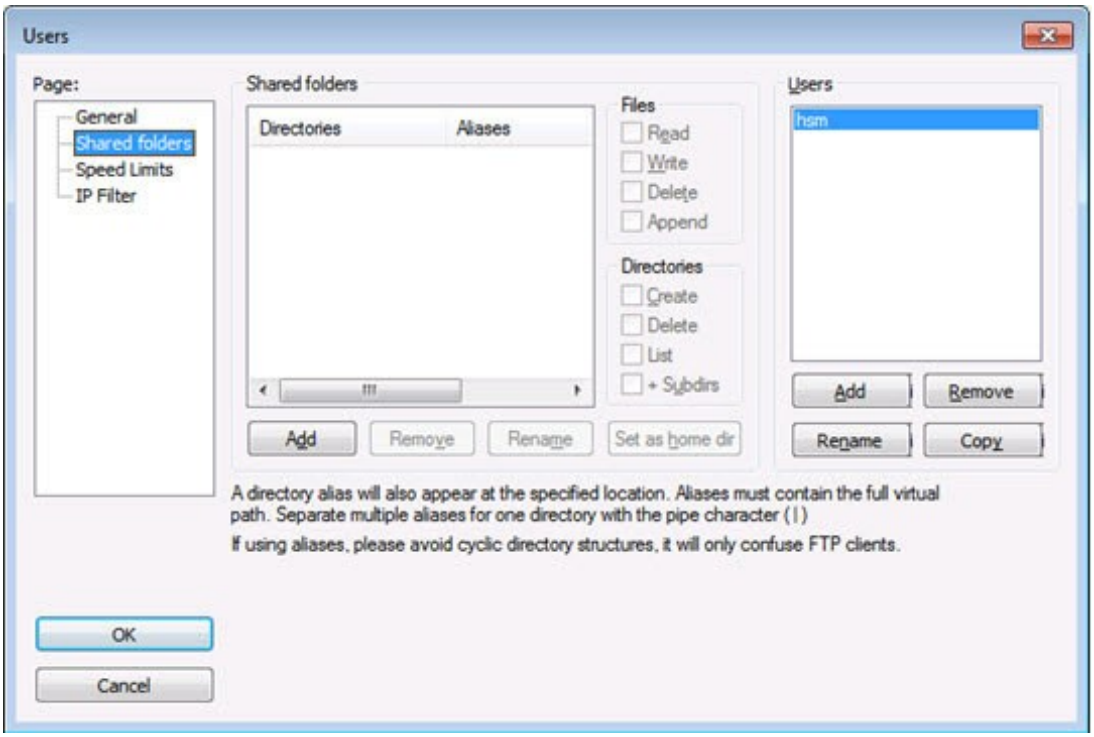


4. Click **Add** and enter the new user name, for example, **hsm**.

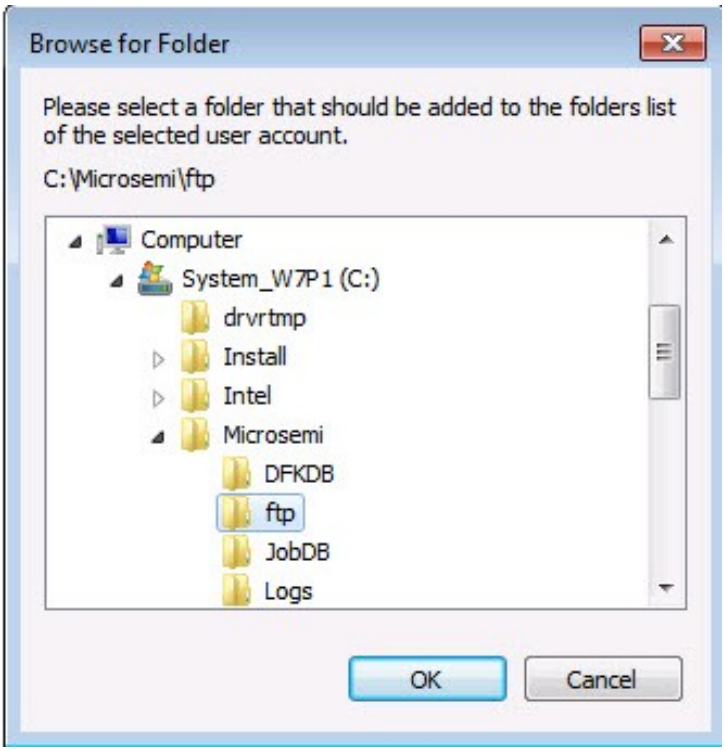
5. Click **OK**.
6. In the Users dialog box, select the Password check box and enter your password. This password is used when setting up HSM parameters for FlashPro Express.



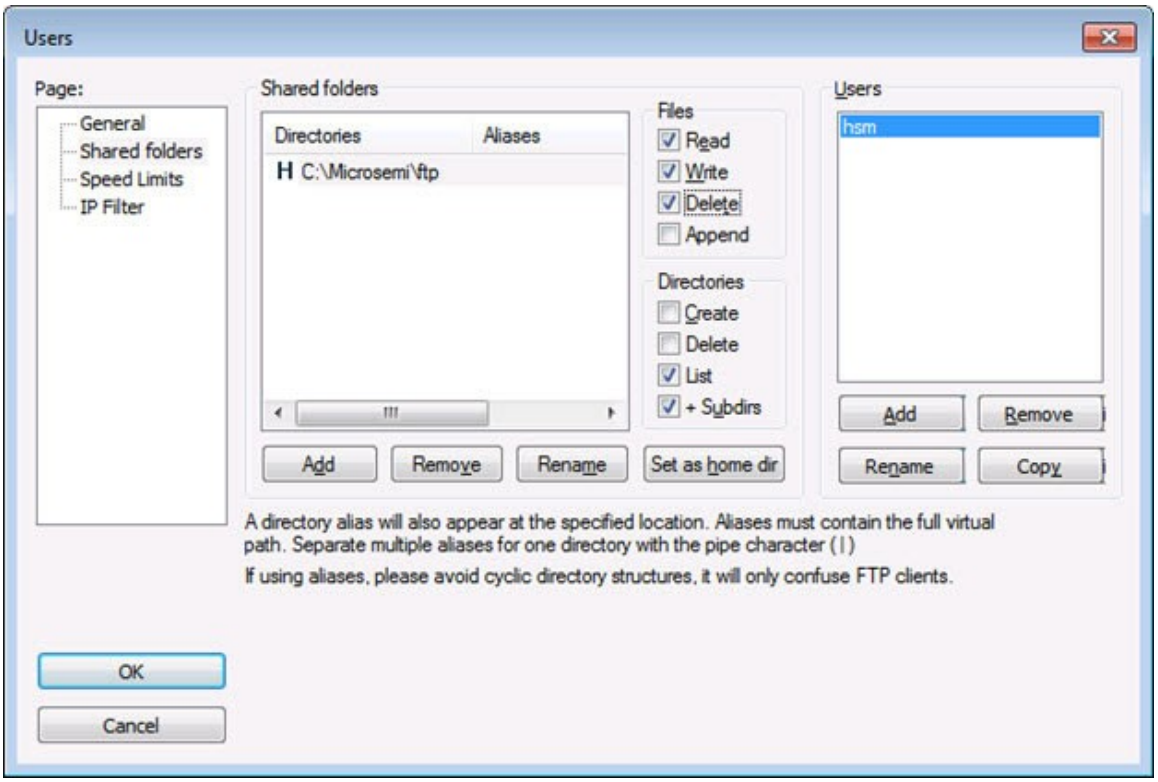
7. In the **Page** tree view, select the **Shared folders** option.



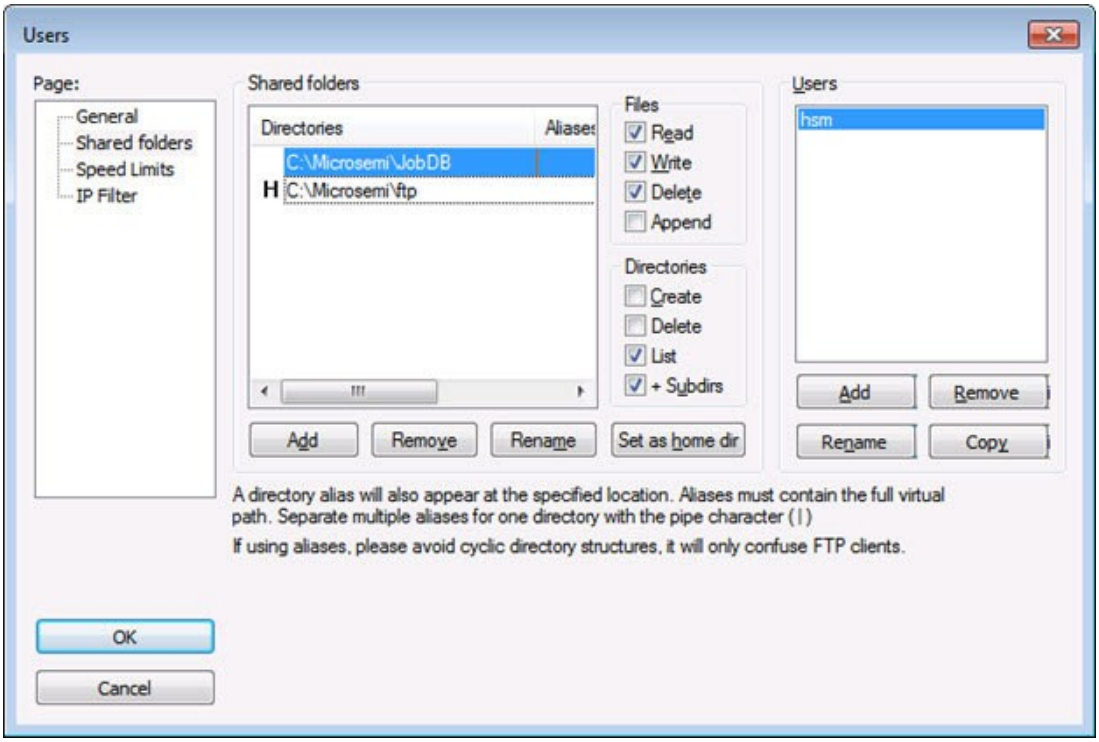
8. Click **Add**.
9. Navigate to the `C:\Microsemi\ftp` folder.
10. Click **OK**.



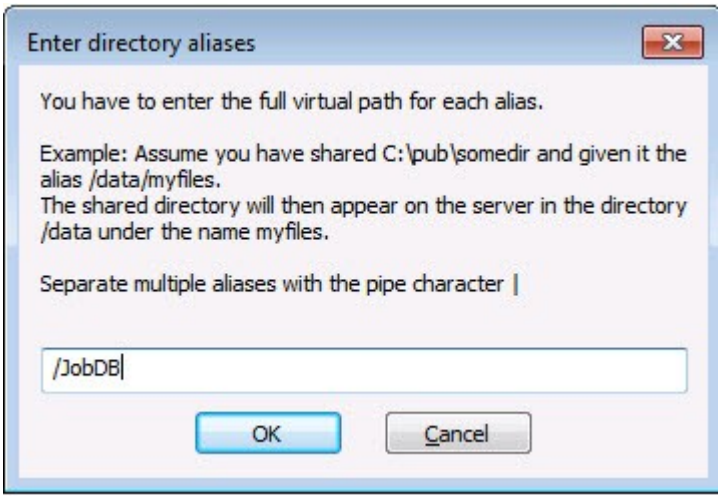
11. Set permissions for this directory to Read/Write/Delete.



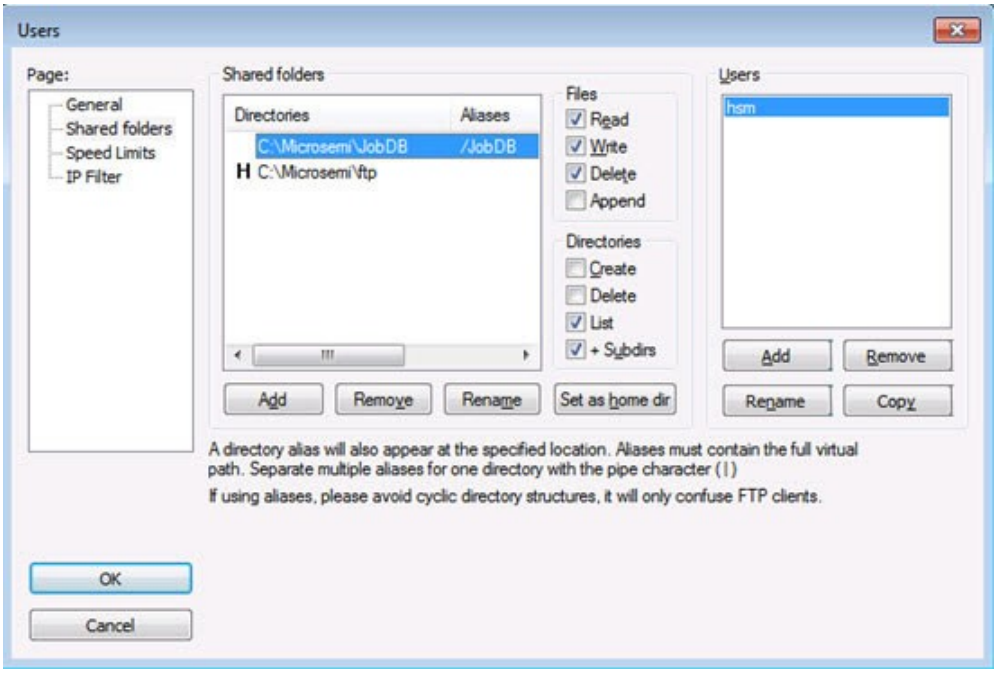
12. Repeat this step and add the location of the ticket database.



13. Make sure that the JobDB directory has Read/Write/Delete permissions.
14. Right-click the JobDB entry and choose **Edit aliases**.
15. Set alias as "/JobDB".



16. Confirm that the home directory is set to the ftp folder and alias to the JobDB, as shown in the following figure.



17. Confirm that the FTP server functions as expected. Figure 3-22 shows an example.

Figure 3-22. Checking Setup of FTP Server

```
C:\Microsemi\DFKDB>ftp sjsocprgw7p1

Connected to sjsocprgw7p1.microsemi.net.
220-FileZilla Server version 0.9.48 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
User (sjsocprgw7p1.microsemi.net:(none)): hsm
331 Password required for hsm
Password:
230 Logged on

ftp> ls
200 Port command successful
150 Opening data channel for directory listing of "/"
JobDB
226 Successfully transferred "/"

ftp> cd JobDB
250 CWD successful. "/JobDB" is current directory.
ftp> ls
200 Port command successful
150 Opening data channel for directory listing of "/JobDB"
226 Successfully transferred "/JobDB"
ftp>
```

18. Similarly, create the /JobDBArchive FTP location at the same level as /JobDB and pointing to `C:\Microsemi\JobDB\JobDBArchive`.

4. Running M-HSM Server as a Service

This section describes how to run M-HSM as a service.

The M-HSM server can be set up to run as a Windows service. This mode allows a non-admin user to operate the server once the service configuration is done under the administrator account.

In service mode, all interactions with the M-HSM server are done through the M-HSM Control Panel application.

4.1 Service Setup

The service setup and configuration steps require administrator privileges.

Before starting service configuration, ensure that the *M-HSMServer.exe* is not running.

4.1.1 Create Service Entry

Open a command prompt in As Admin mode: type **cmd** in the Windows Start menu, right-click the "cmd" entry, and run in As Admin mode.

Create a service entry called M-HSMServer, as per the following the example:

```
C:\Microsemi\SEE>sc create M-HSMServer binPath= "C:\Microsemi\server\m-hsmserver.exe"
DisplayName= "Manufacturer HSM Server"
```

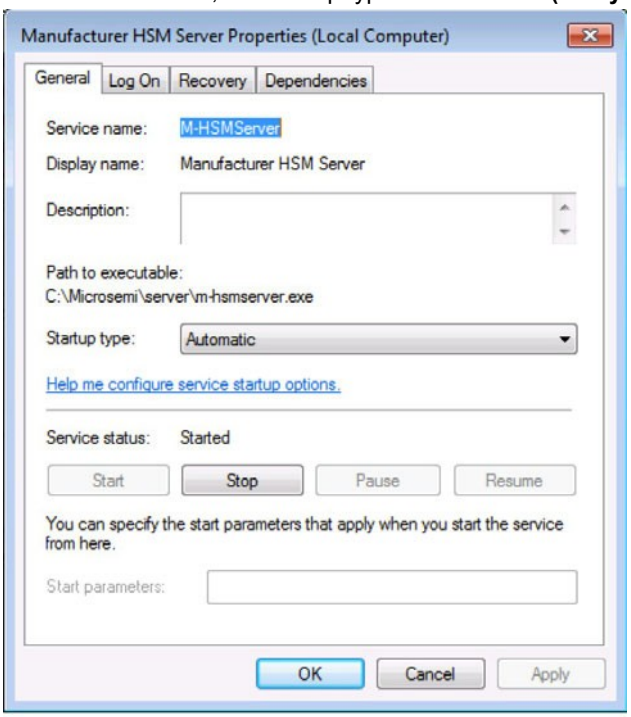
```
[SC] CreateService SUCCESS
```

Note: If you need to delete this entry, use the `sc delete M-HSMServer` command.

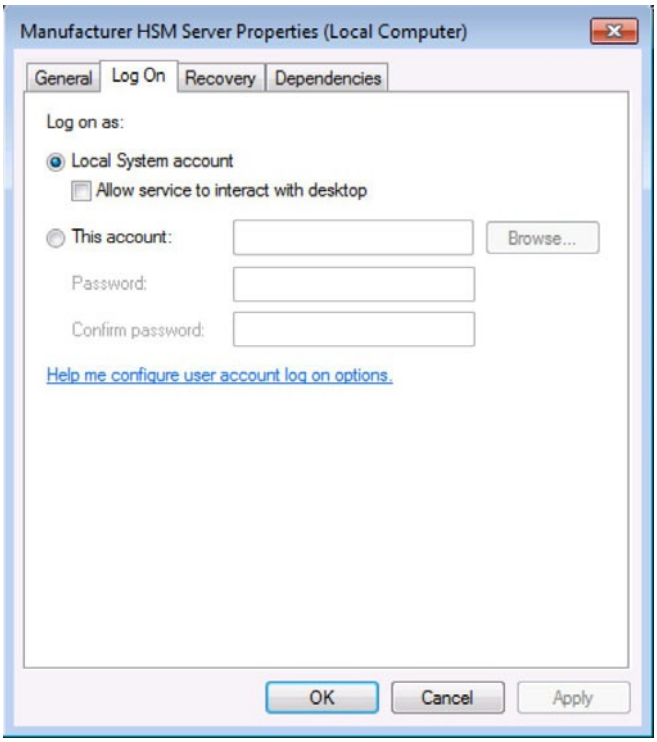
4.1.2 Update Service Properties

Perform the following steps to update service properties:

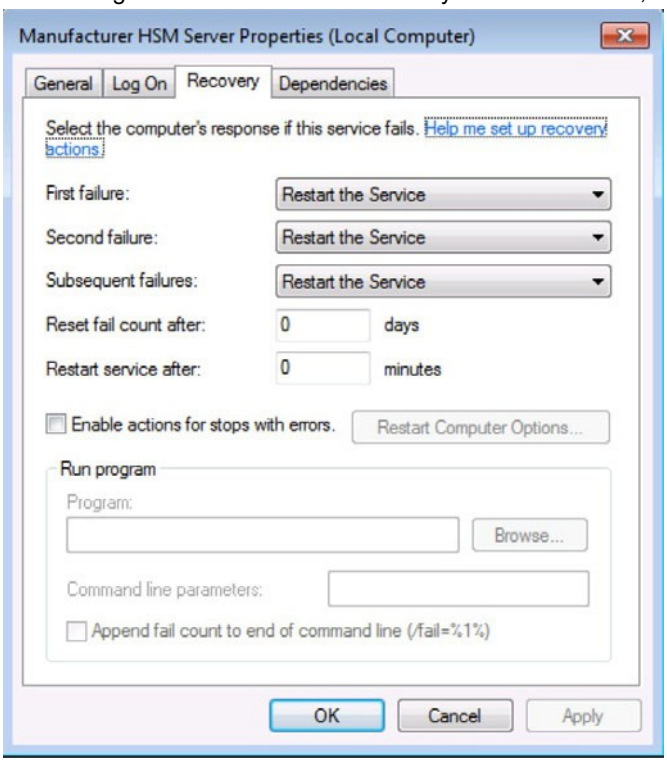
1. Open the Control Panel and go to **Services**. Find the **Manufacturer HSM Service** entry and open the service properties windows.
2. On the **General** tab, set Startup type to **Automatic (Delayed Start)**.



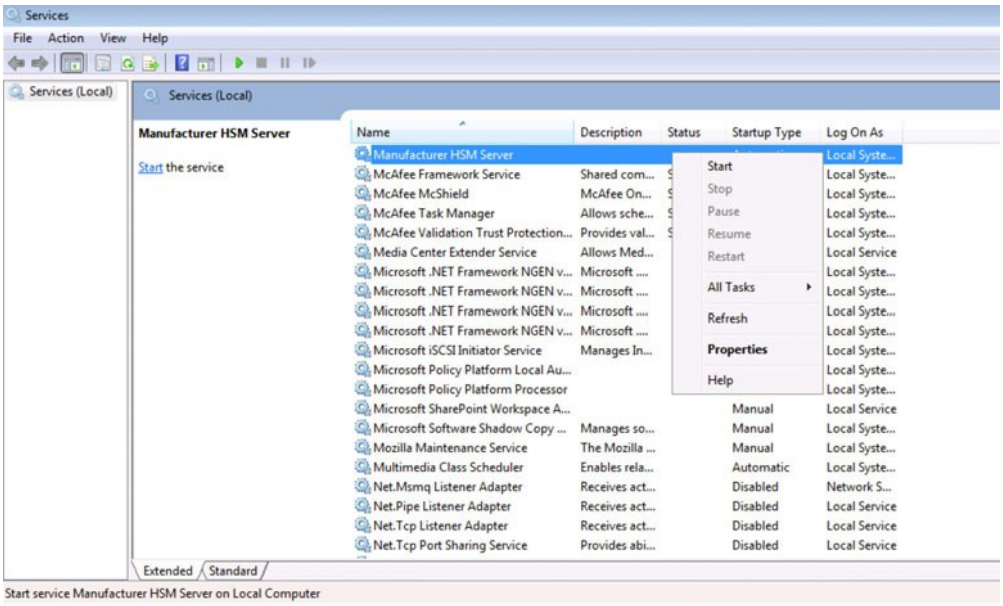
3. On the **Log On** tab, make sure "Log On as" is set to **Local System account**.



4. On the **Recovery** tab, set all failure recovery fields to **Restart the Service**, as shown in the following figure. This setting tells Windows to automatically restart the server, if an error occurs.



5. When completed, click **OK** and close the dialog box. Then, attempt to manually start the server: navigate to the Manufacturer HSM Server entry, right-click, and choose **Start**.



6. Once service is confirmed, you can reboot the PC and log in using a non-administrator user account.

Note: Under the non-administrator account, you can only observe service status using the Windows Services tool.

4.2 M-HSM Control Panel Application

The control panel application can be used under administrator and non-administrator user accounts. The control panel application provides the following functions:

- Observe status of M-HSM server
- Restart service for error recovery
- Stop and Start active session with the HSM module
- Export M-HSM server activity log

4.2.1 Setup

The M-HSM Control Panel application is located in the "M-HSMControlPanel" folder.

The application executable *M-HSMControlPanel.exe* can be started like other Windows applications and does not require admin privileges to operate.

For convenience, it can be added to the Windows start-up applications as a shortcut placed in the the Windows Startup folder:

For example, `C:\Users\hsm_nonAdmin_user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`

Once added to the startup applications, the M-HSM Control Panel application is automatically started by the Windows upon startup.

Note: Upon initial startup, the application registers its icon in the Windows registry. Once registered, the application executable name or path cannot be changed without removing that entry in the Windows Registry. See the *ReadMe.txt* file for the cleanup instructions.

Only one running instance of the application is allowed at a time.

4.2.2 Notification Icon

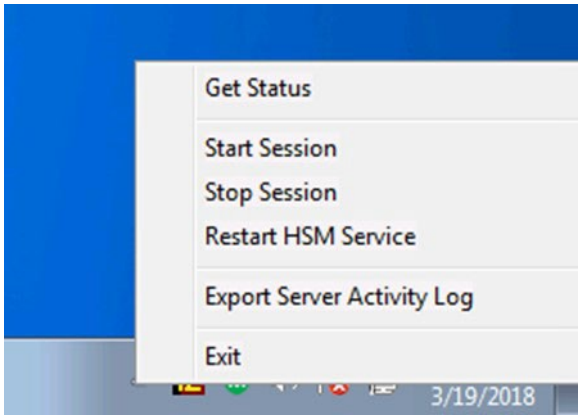
The application appears as an icon in the Windows Notification Area.

Depending on the status of the M-HSM server, the icon of the M-HSM Control Panel application can be one of the following:

- **Green**: Indicates server normal working state.
- **Red**: Indicates that the connection with the server is established, but the session with the HSM module is not active. It can be either in the Starting, Stopping, or Not Running state.
- **Gray**: Indicates connection with the server cannot be established. In most cases, this means that the service is not running.

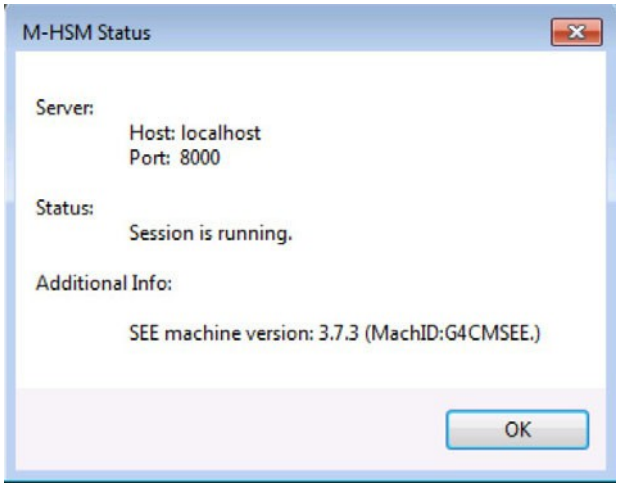
In addition to color coding, the server state is indicated in the tooltip that appears when the cursor hovers over the icon.

The following figure shows how left-clicking the application icon opens the context menu:



4.2.3 Get Status

The **Get Status** option indicates M-HSM connection state, state of the session with the HSM module, and version of the SEE firmware running on the HSM module, if session with the HSM module is active.



4.2.4 Start and Stop Session

The **Start** and **Stop** options control the active session state with the HSM module inside the M-HSM server application. The session with the HSM module automatically starts with the startup of the M-HSM server. Upon its startup, the session loads information from the server configuration files and establishes connection with the SEE machine running in the HSM module. If the SEE firmware is being loaded, the HSM server waits, until the firmware load is finished.

Stopping the session allows the user to manipulate HSM server settings and HSM module hardware without having to stop M-HSM Service.

Note: Upon receiving a session stop request, the HSM server stops accepting new client requests, while allowing requests still in progress to complete.

4.2.5 Restart M-HSM Service

This option allows user to restart M-HSM server service to recover from certain errors. This eliminates the need to restart the PC.

Note: This action might terminate client requests currently in progress and must be used with caution. It is a good practice to attempt stopping a session first.

4.2.6 Export Server Activity Log

This option retrieves the log file located in the sever directory and exports it to the file specified by the user. Information in this log file can be used to analyze current server activities.

4.2.7 Exit

This option terminates the M-HSM Control Panel application session. It does not impact M-HSM server operation, and can be restarted by a non-administrator user at any time.

5. M-HSM Reconfiguration and Post-Installation Actions

This section provides instructions for the setup and maintenance actions that can be performed on an installed and provisioned M-HSM.

5.1 HSM Module Replacement

Only one module at a time can be connected to the M-HSM.

5.1.1 Overbuild Protection During Module Maintenance

Note: If the old module is removed or erased from the M-HSM, unfinished programming jobs are not able to proceed.

For any jobs in progress, certain ticket information is stored inside the NVRAM of the HW module, which makes job tickets physically unclonable.

Module maintenance, such as replacement, firmware upgrades, and erase invalidate unfinished jobs. The user must submit a new job to continue manufacturing. However, issuing a new job without having a proof or termination of previous job(s) creates a potential threat of overbuilding. To minimize this risk, before undertaking such module maintenance actions, any active job(s) must be terminated using the `complete_prog_job` Tcl command (see the *Libero SoC/PolarFire FPGA Tcl Command Reference Guide*). This job termination command generates a Job End Certifier that can be validated on the U- HSM. This certifier is protected by the HSM and cannot be modified. It provides the user with assurance that further device programming is not possible from the old job. Once the Job End certifier has been validated by the user on the U-HSM, it is safe to issue a new job after maintenance has completed.

5.1.2 Remove the Old HSM Module

Physically disconnect the old module. The M-HSM Security World contains a file with the module information. While this file can co-exist with the files for other modules added to the system, the user can choose to remove it for security reasons. The file is located in the `%NFAST_KMDATA%\local` Security World directory.

The file name follows the pattern "module_<module_ESN>". If needed, the user can also remove the licensing file from the *<M_UUID>.g4sl* Server and Tools directories.

Note: If the old HSM module was used to create any public encryption or signing keys, then the Warrant File for this module is needed to export those keys. You can keep the old module Warrant File to enable public key export or remove it to disable this function.

5.1.3 Set Up a New HSM Module

After the module is installed on the system, it must be added to the Security World and set up to load the SEE Machine firmware per module type.

5.1.3.1 Module Installation

1. Install a new HSM module (see section HSM Hardware Module Installation).
2. Install the Microchip-issued HSM module license (see section Install HSM Module License File).
3. Install the module warrant file (see section HSM Hardware Module Installation).

5.1.3.2 Add the HSM Module to the Security World

The following steps require the Administrative Card Set (ACS). The number of required cards and their respective passphrases depend on the settings specified during Security World creation (see section Create the Security World)

1. Set the module to the Pre-Init state.
2. Add the HSM module to the Security World using the New-World command:
   `new-world --program --no-remoteshare-cert -m 1`
3. Create a new NVRAM file (see section Create NVRAM-based Storage in the HSM Module).
4. Set module to the operational state.
5. Set up the HSM module to load the SEE Machine firmware: follow instructions in section Set Up the SEE Machine Firmware for Loading into the HSM Module.

5.2 Import the Public Key of M-HSM

Follow the instructions provided in section Import the M-HSM Public Keys.

5.3 Import the Public Keys of U-HSM

Follow the instructions provided in section Import the U-HSM Public Keys.

5.4 Export the Public Keys for Sending to a U-HSM

Follow the instructions provided in section Export the M-HSM Public Keys.

5.5 Import New DFK DB and Manufacturing Keys from U-HSM

Follow the instructions provided in section Import U-HSM Device Data.

5.6 Upgrade the HSM Module Firmware

This step shows how to upgrade HSM module firmware (not the SEE Machine firmware). The firmware upgrade might be necessary in the following cases:

- The HSM module has a firmware revision that is not supported by the FlashProExpress version used (see the *M-HSM Release Notes* for the supported revisions).
- The user wants to switch to another revision of Microchip-supported firmware.
- Microchip issues a security advisory.

Notes:
If the M-HSM has any active programming jobs, they are disabled through the firmware upgrade. Also, the firmware upgrade erases NVRAM and any information about module association with the Security World. The following steps show how to upgrade the firmware of the HSM module and restore the HSM module on the M-HSM server:

1. Read the important notes in section Upgrade HSM Module Firmware regarding the firmware upgrade procedure and firmware revisions compatibilities. If the firmware upgrade is initiated by a Microchip security advisory, the instructions in the advisory shall supersede the instructions in this guide.
2. Terminate any active job(s) and forward job end certifier to the U-HSM.
   Read important information regarding overbuild protection during HSM module maintenance operations in section Overbuild Protection During Module Maintenance.
3. Upgrade the HSM module firmware.
   HSM module firmware upgrade instructions are provided in section Upgrade HSM Module Firmware.
4. Restore the module association with the Security World.
   Follow the instructions provided in section Add the HSM Module to the Security World.
5. Start the M-HSM server.
   Follow the instructions provided in section Start the M-HSM Server and confirm successful server startup.
6. Resubmit new programming jobs, if necessary.

6. M-HSM Server Replication

An existing M-HSM server can be replicated to one or more new M-HSM servers. As a result, the replicated server gets a copy of the Security World, all HSM keys, imported public keys, the DFK DB, and the manufacturing keys already existing on the source system.

Note: Programming jobs cannot be replicated, but they can be transferred. The overbuild protection does not allow cloning of any job that may exist in the source system. Job tickets reside inside the physical HSM module, and can only be transferred to the new system along with the physical module.

The following sections provide instructions for M-HSM server replication.

6.1 Install the Software

Follow the instructions provided in section Software Installation and install all required software packages.

6.2 Copy Over the Security World

Copy the content of the Security World directory from the source to the destination machine. The location of the security world directory is: `%NFAST_KMDATA%\local`.

This step copies over the entire security environment:

- Security World data
- Created M-HSM keys
- Imported public keys
- Imported MFG keys

6.3 Copy Over the M-HSM Server

1. Copy HSM server software components from the source HSM to the destination folder of the new server (the default location is `C:\Microsemi`).
2. On the destination machine, delete the ticket db files (job cannot be replicated):
   - `C:\Microsemi\JobDB`
   - `C:\Microsemi\JobDB\JobDBArchive`

6.4 Install a New HSM Module

Follow the instructions provided in section Set Up a New HSM Module.

6.5 Start the M-HSM Server

Follow the instructions provided in section Start the M-HSM Server.

6.6 Set Up the FTP Server

Follow the instructions provided in section FTP Server Setup.

7. Referenced Documents

This user guide references the following documents:

- *Secure Production Programming Solution*
- *Programming Job Manager User Guide*
- *FlashPro Express User Guide*
- *Libero SoC Design Flow User Guide*
- *PolarFire FPGA Design Flow User Guide*
- *nShield Edge and Solo User Guide for Windows (nCipher)*
- *User HSM Installation and Setup Guide*

8. Revision History

Revision	Date	Description
B	12/2020	Following is the summary of changes: • Edited section System Requirements. • Edited the list of the M-HSM components in section Acquire the M-HSM Components. • Edited the list of installation and setup options in section M-HSM Installation and Setup Scenarios. • Edited the manual installation process in section 3.1 Software Installation. • Added new section Create NVRAM Partition in the HSM Module. • Added new section Remove Existing NVRAM Partition. • Edited section Service Mode. • Edited section Update Service Properties. • Added note in section Remove the Old HSM Module.
A	11/2020	Document is formatted as per Microchip template. Initial revision.

9. Microchip FPGA Technical Support

Microchip FPGA Products Group backs its products with various support services, including Customer Service, Customer Technical Support Center, a website, and worldwide sales offices. This section provides information about contacting Microchip FPGA Products Group and using these support services.

9.1 Customer Service

Contact Customer Service for non-technical product support, such as product pricing, product upgrades, update information, order status, and authorization.

- From North America, call **800.262.1060**
- From the rest of the world, call **650.318.4460**
- Fax, from anywhere in the world, **650.318.8044**

9.2 Customer Technical Support

Microchip FPGA Products Group staffs its Customer Technical Support Center with highly skilled engineers who can help answer your hardware, software, and design questions about Microchip FPGA Products. The Customer Technical Support Center spends a great deal of time creating application notes, answers to common design cycle questions, documentation of known issues, and various FAQs. So, before you contact us, please visit our online resources. It is very likely we have already answered your questions.

You can communicate your technical questions through our Web portal and receive answers back by email, fax, or phone. Also, if you have design problems, you can upload your design files to receive assistance. We constantly monitor the cases created from the web portal throughout the day. When sending your request to us, please be sure to include your full name, company name, and your contact information for efficient processing of your request.

Technical support can be reached at soc.microsemi.com/Portal/Default.aspx.

For technical support on RH and RT FPGAs that are regulated by International Traffic in Arms Regulations (ITAR), log in at soc.microsemi.com/Portal/Default.aspx, go to the **My Cases** tab, and select **Yes** in the ITAR drop-down list when creating a new case. For a complete list of ITAR-regulated Microchip FPGAs, visit the ITAR web page.

You can track technical cases online by going to My Cases.

9.3 Website

You can browse a variety of technical and non-technical information on the Microchip FPGA Products Group home page, at www.microsemi.com/soc.

9.4 Outside the U.S.

Customers needing assistance outside the US time zones can either contact technical support at (https://soc.microsemi.com/Portal/Default.aspx) or contact a local sales office.

Visit About Us for sales office listings and corporate contacts.

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods being used in attempts to breach the code protection features of the Microchip devices. We believe that these methods require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Attempts to breach these code protection features, most likely, cannot be accomplished without violating Microchip's intellectual property rights.
- Microchip is willing to work with any customer who is concerned about the integrity of its code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable." Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Trademarks

ISBN: 978-1-5224-7397-8

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-72400 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-72884388 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820