SPPS v11.8 SP1

Release Notes

7/2018

Microsemi Headquarters
One Enterprise, Aliso Viejo,
CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
Email: sales.support@microsemi.com
www.microsemi.com

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer’s responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided “as is, where is” and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.

About Microsemi

Microsemi, a wholly owned subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions, security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Learn more at www.microsemi.com.

51300204-1/7.18

Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

Revision 1.0

Revision 1.0 is the first publication of this document (07/05/2018).

Contents

1 SPPS v11.8 SP1 Release Notes

These Release Notes highlight the changes made to the SPPS solution since the v11.7 SP3A release.

1.1 Enhancements/Changes

- New UEK3 keymodes: This release adds support for a new User SRAM-PUF symmetric keymode, UEK3. This keymode is available for M2S060, M2GL060, M2S090, M2GL090, M2S150, and M2GL150 “S” and “TS” devices. Refer to the SmartFusion2 SoC FPGA and IGLOO2 FPGA Security Best Practices User Guide for more information.
- New auth_keymode TCL parameter: The init_bitstream TCL command has a new parameter, auth_keymode. Users must specify DFK keymode if they want to continue using the DFK keymode as they were using it in previous versions.

1.2 TCL Changes

1.1.1 Job Manager TCL Changes

Job Manager TCL changes are listed in the table below. Refer to the Job Manager documentation for more information.

Command	Old	New	Comment
create_keyset		-uek3 *<value>* -uek3_base *<value>*	New parameters to specify UEK3 and UEK3_base keys.
init_bitstream	-bitstream_type "TRUSTED_FACILITY | MASTER | UEK1 | UEK2"	-bitstream_type "TRUSTED_FACILITY | MASTER | UEK1 | UEK2 | UEK3"	Supports new UEK3 bitstream type.
init_bitstream	-unique_key_types "[UPK1 | UEK1 | UPK2 | UEK2 | DPK]+"	-unique_key_types "[UPK1 | UEK1 | UPK2 | UEK2 | UEK3 | DPK]+"	UEK3 is now available as one of the unique keys.
init_bitstream		-auth_keymode "DFK | KFPE | KFP"	New parameter to specify Auth Keymode. *Note 1: User must explicitly specify DFK keymode to be compatible with previous versions.* *Note 2: KFP and KFPE are not available for IHP flow.*

1.1.2 FlashPro Express TCL Changes

FlashPro Express TCL changes are listed in the tablebelow. Refer to the FlashPro Express documentation for more information.

Command	Old	New	Comment
list_all_hsm_tickets			New TCL command to list all HSM tickets. Refer to the FlashPro Express documentation.
remove_hsm_tickets			New TCL command to remove tickets specified either using Ticket ID or job reply file. Refer to the FlashPro Express documentation.

1.3 HSM Module Firmware Revision

This release has been tested and verified on Thales HSM firmware revision 2.55.1

1.4 Thales nShield Revisions

This release has been tested and verified on Thales nShield revisions 11.62.00 and 11.70.00.

2 Known Issues

2.1 Bug 15 – Error messages shown during HSM startup in certain cases

Issue: When the HSM server executable (U-HSMServer.exe or M-HSMServer.exe) is started in the following cases, there may be error messages printed during the startup process. Ignore these error messages if you see “Session is initialized.”

- If system is restarted and HSM server is immediately started.
- If Thales nFast server has been restarted and the HSM server is immediately started.
- If HSM module reinitialization is done using Security World commands such as nopclearfail and the HSM server is immediately started.
- If changing or setting up the SEE firmware load using loadsee-setup and starting the HSM server immediately.

Note: In all the above cases, the HSM server will make multiple attempts to initialize and will stop once the “Session is initialized” message is printed. If it is not able to start even after multiple attempts, it will exit with an error message.

Workarounds:

1. Wait until the SEE firmware is loaded before starting HSM server exe.
2. Ignore the error messages if you see “Session is initialized.”

2.2 PROGRAM action ticket counter decrements incorrectly when using Factory SRAM-PUF ECC keymodes (KFP, KFPE)

Issue: When using HSM flows that use Factory SRAM-PUF ECC keymodes (KFP, KFPE) for authorization code, the number of devices for PROGRAM HSM ticket is incorrectly reduced by two each time PROGRAM action is run in FlashPro Express (on the same or different device).

Workaround:

Accommodate extra devices in HSM ticket for PROGRAM action. This can be done by specifying the number of devices in the “max_device” parameter of “new_hsmtask_ticket” in Job Manager. You can also specify “unlimited” in the “max_device” parameter if overbuild protection is not needed.