SPPS v11.8 SP3

Release Notes

6/2018

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

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.

51300203-1/6.18

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 (06/20/2018).

Contents

1 SPPS v11.8 SP3 Release Notes

These Release Notes highlight the changes made to the SPPS solution since the v11.8 SP1 release.

1.1 Enhancements/Changes

- New Factory ECC PUF keymodes: This release adds support for a new Factory SRAM-PUF ECC keypair, (KFP, KFPE) in IHP flow. These keymodes are only 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.
- A new Windows service mode of operation is now available for U-HSM and M-HSM servers. It allows operation of both HSM servers using non-admin account. Refer to the installation guides for details.
- Security and stability fixes in Job Manager, FlashPro Express, and M-HSM server.

1.2 TCL Changes

No SPPS-related TCL commands have been modified.

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 and Limitations

2.1 NEW: Bug 29 - SPPS: Ticket counter decrements incorrectly when using Factory SRAM-PUF ECC keymodes (KFP, KFPE)

Issue: When using HSM flow that uses Factory SRAM-PUF ECC keymodes (KFP, KFPE) for authorization code, the number of devices per HSM ticket is incorrectly reduced as follows when running programming actions in FlashPro Express:

1. Running PROGRAM action once decreases the program ticket counter by 2.
2. Running ERASE action once decreases 1 erase ticket counter and 1 verify ticket counter (if VERIFY has not been run).
3. Running PROGRAM action again on the same DSN decreases the program ticket counter by 2.

Affected versions: Version 11.8 and later.

Workaround:

1. When adding an HSM ticket for ERASE action, you also need to add an HSM ticket for VERIFY action.
2. Accommodate extra devices for each HSM ticket. 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.