

SPPS v12.0

Release Notes

2/2019



a  **MICROCHIP** company

**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

©2019 Microsemi, a wholly owned subsidiary of Microchip Technology Inc. All rights reserved. Microsemi and the Microsemi logo are registered trademarks of Microsemi Corporation. All other trademarks and service marks are the property of their respective owners.

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.

51300215-1/02.19

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.

Contents

- Revision History..... 3
 - Revision 1.0..... 3
- 1 SPPS v12.0 Release Notes 5
 - 1.1 Enhancements/Changes 5
 - 1.2 TCL Changes 5
 - 1.3 HSM Module Firmware Revision..... 5
 - 1.4 Thales nShield Revisions 5
- 2 Known Issues..... 6
 - 2.1 SPPS: New JDC file must be generated if eNVM is set to be protected by passkey, using pre-v12.0 Job Manager 6
 - 2.2 SPPS: Job Manager crashes when opening an existing Job Manager project from v11.9 6
 - 2.3 SPPS: Job Manager does not support PolarFire DAT export 6
 - 2.4 SmartFusion2/IGLOO2: eNVM update protection with FlashLock is no longer supported 6
 - 2.5 ERASE Action failure for FlashPro Express Job 6

1 SPPS v12.0 Release Notes

These Release Notes highlight the changes made to the SPPS solution for the v12.0 release.

1.1 Enhancements/Changes

SPPS v12.0 added support for PolarFire Secure Production Programming.

Note: For SPPS v12.0, Job Manager v12.0 and FlashPro Express v12.0 require U-HSM Server v12.0 and M-HSM Server v12.0, respectively.

1.2 TCL Changes

Job Manager v12.0 TCL command updated to support PolarFire:

- `init_bitstream`

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 SPPS: New JDC file must be generated if eNVM is set to be protected by passkey, using pre-v12.0 Job Manager

eNVM update protection with FlashLock is not supported. eNVM update is protected by User Encryption Keys (UEK1, UEK2 or UEK3).

Regenerate the JDC file without eNVM FlashLock Protection enable.

2.2 SPPS: Job Manager crashes when opening an existing Job Manager project from v11.9

Job Manager v12.0 does not support Job Manager project files created with releases prior to v12.0.

2.3 SPPS: Job Manager does not support PolarFire DAT export

PolarFire DAT file bitstream export from Job Manager is not supported in v12.0.

2.4 SmartFusion2/IGLOO2: eNVM update protection with FlashLock is no longer supported

Due to a silicon limitation, eNVM update protection with FlashLock has been defeated. If a JDC file generated with a pre-12.0 version of Libero SoC had the eNVM set to be protected by passkey, it must be regenerated with Libero SoC v12.0 (which does not have eNVM FlashLock Protection enabled). eNVM update protection continues to be provided by User Encryption Keys (UEK1, UEK2 or UEK3).

2.5 ERASE Action failure for FlashPro Express Job

If a HSM FlashPro Express job has tickets for PROGRAM and ERASE actions, without a ticket for the VERIFY action, the ERASE action will fail. To successfully run the ERASE action, ensure that a ticket for the VERIFY action is included. This issue will be fixed in the upcoming v12.1 release.