AN1442: SiWx917 SoC Secure Boot with Anti-Rollback Protection

This version of AN1442 has been deprecated.
For the latest version, see docs.silabs.com.
****

This application note describes the design of Secure boot with anti-rollback protection on SiWx917 devices. It also provides examples of how to implement the Secure Boot process and protect against firmware rollback.

For more information on provisioning the SiWx917 for secure boot, see the following: UG574: SiWx917 SoC Manufacturing Utility User Guide.

KEY FEATURES

- Describes the secure boot process for SiWx917 devices
- Describes the anti-rollback mechanism
- Describes the layout of RPS files
- Provides examples of configuring SiWx917 devices for secure boot

 Copyright © 2026 by Silicon Laboratories

SILICON LABS
CONNECTED INTELLIGENCE

The Leading Innovator in Low-Power Wireless.

IoT Portfolio
silabs.com/products

Simplicity Studio
silabs.com/simplicity

Quality
silabs.com/quality

Support & Community
silabs.com/community

Disclaimer

Silicon Labs provides customers with data sheets, application notes and product briefs ("Product Documentation") that are intended to present current, accurate and in-depth information about Silicon Labs' integrated circuits, peripherals, modules and other products ("Products"). Silicon Labs may also provide reference designs, schematics, design files, software, tools, documentation, consultation and other customer support materials ("Support Materials") that are intended solely to assist customers in developing their own modules, boards or other applications or products that include one or more Silicon Labs Products and may not be used for any other purposes.

Characterization data, device specifications, memory sizes, memory addresses and typical parameters can and do vary in different applications and are provided for illustrative purposes only, are subject to change without notice, and should not be relied upon without independent verification. Product firmware may be updated during the manufacturing process for security or reliability purposes.

Product Documentation does not imply or expressly grant any license to design or fabricate integrated circuits or modules. Customers are solely responsible for the design and distribution of their products including the acquisition of licenses to any necessary intellectual property rights.

Product Documentation and Support Materials are not authorized for use in or in connection with FDA Class III devices or military, automotive or aviation applications and shall in no circumstances be used in weapons of mass destruction or systems capable of delivering such weapons.

SILICON LABS DOES NOT WARRANT THAT PRODUCT DOCUMENTATION OR SUPPORT MATERIALS WILL MEET YOUR REQUIREMENT OR THAT THEIR OPERATION WILL BE UNINTERRUPTED OR THAT ANY SOFTWARE WILL BE ERROR-FREE. PRODUCT DOCUMENTATION AND SUPPORT MATERIALS ARE PROVIDED "AS IS" AND "WITH ALL FAULTS." SILICON LABS MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE ACCURACY, COMPLETENESS, RELIABILITY, OR SUITABILITY OF PRODUCT DOCUMENTATION OR SUPPORT MATERIALS, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. SILICON LABS DISCLAIMS ALL IMPLIED WARRANTIES.

Trademark Notice

Silicon Laboratories®, Silicon Labs®, Silabs®, and the Silicon Labs S-logo as well as other product or service names used herein are trademarks or registered trademarks of Silicon Laboratories Inc. For more information, please visit: Silicon Labs Trademark Use Guidelines - Silicon Labs. Arm®, Cortex® and Keil® are trademarks or registered trademarks of Arm Holdings or Arm Limited. All other third-party products or brand names mentioned herein are trademarks of their respective holders.

SILICON LABS CONNECTED INTELLIGENCE

400 West Cesar Chavez
Austin, TX 78701 | USA

www.silabs.com