Document Title	List of known Issues of Secure Hardware Extensions
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	971

Document Status	published
Part of AUTOSAR Standard	Foundation
Part of Standard Release	R24-11

Document Change History

Date	Release	Changed by	Description
2024-11-27	R24-11	AUTOSAR Release Management	• No content changes
2023-11-23	R23-11	AUTOSAR Release Management	• No content changes
2022-11-24	R22-11	AUTOSAR Release Management	• No content changes
2021-11-25	R21-11	AUTOSAR Release Management	• No content changes
2020-11-30	R20-11	AUTOSAR Release Management	• No content changes
2019-11-28	R19-11	AUTOSAR Release Management	• Initial release. • This is a republication of “Errata and amendments to SHE v1.1, rev439” from 2009-10-16 applicable to AUTOSAR_TR_SecureHardwareExtensions

Disclaimer

This work (specification and/or software implementation) and the material contained in it, as released by AUTOSAR, is for the purpose of information only. AUTOSAR and the companies that have contributed to it shall not be liable for any use of the work.

The material contained in this work is protected by copyright and other types of intellectual property rights. The commercial exploitation of the material contained in this work requires a license to such intellectual property rights.

This work may be utilized or reproduced without any modification, in any form or by any means, for informational purposes only. For any other purpose, no part of the work may be utilized or reproduced, in any form or by any means, without permission in writing from the publisher.

The work has been developed for automotive applications only. It has neither been developed, nor tested for non-automotive applications.

The word AUTOSAR and the AUTOSAR logo are registered trademarks.

List of known Issues of Secure Hardware Extensions

No.	Date	Severity	Problem Description	Location
1	2009-07-31	erratum	CMD_EXPORT_RAM_KEY can also issue error code ERC_KEY_NOT_AVAILABLE. *Note: The description of the command and the overview table were missing the information.*	Section 4.7.9 Table 4.6
2	2009-07-31	erratum	CMD_GET_ID may not issue error code ERC_KEY_NOT_AVAILABLE since key protection flags are not evaluated *Note: The description of the command and the overview table indicate an error code that cannot be emitted by the command.*	Section 4.7.17 Table 4.6
3	2009-07-31	erratum	CMD_EXPORT_RAM_KEY reads UID *Note: The command also needs to access the UID to calculate the messages. The referenced table is missing the corresponding information (X = used by function).*	Table 4.4
4	2009-07-31	erratum	The flag SREG.EXT_DEBUGGER has not to be set if the secure boot failed, see Figure 1 of this errata sheet for a corrected flow chart.	Figure 4.10
5	2009-08-28	detailing	Behavior of secure boot status in power saving modes, e.g., power gating, non-local clock gating etc.: whenever the CPU, a memory or SHE enters a power saving mode, the status register bit SREG.BOOT_OK has to be cleared (Figure 4.10: non-standard boot flow) *Note: The specification defines a non-standard boot flow as every boot method where the secure boot mechanism is not started due to special configurations. This includes boot strap over external interfaces, special reset vectors etc. This issue specifically classifies power down modes as non-standard boot flows, and names the* ▽	Section 4.10

▽

△

			△ *critical parts of the system to provide detailed understanding which parts of the system need to be protected by the secure boot mechanism.*	
6	2009-08-28	amend-ment	The system may provide an optional configuration bit to enable/disable another secure boot process when waking up from power saving modes. Default behavior is to not do a secure boot upon wakeup. The flag has to be stored outside of SHE, similar to the flag to configure sequential/parallel boot measurement (cf. Section 4.10.2). If the enforcement of authentic software is implemented and configured (cf. Section 4.10.5) the flag has to be one-time-programmable. *Note: To allow a flexible usage of SHE this flag may optionally be introduced to allow for secure booting after power saving modes. However, implementing this flag means to always execute the CPU's ROM code after wake-up and perform a regular secure boot as described in Section 4.10. If the microcontroller implements the enforcement of authentic software (cf. Section 4.10.5) and it is intended to be used in scenarios with periodically executed software checking for wake-up of the complete system, the microcontroller should provide a memory protection unit capable to limit the system access of executed wake-up monitor to its intended scope.* *Using the power-down modes in systems that enforce the execution of authentic software (cf. Section 4.10.5) requires a careful system design to not undermine the security of the secure boot mechanism.*	Section 4.10

▽

△

7	2009-10-13	erratum	The statement “Beware that SHE will not solve all security flaws by simply adding it to a microcontroller. It has to be supported by the application software and processes.” has to be “Beware that SHE will not solve all security flaws by simply adding it to a microcontroller but it can help to increase the security level. For this it has to be supported by the application software and processes.”	Section 4.1

List of known Issues of Secure Hardware Extensions

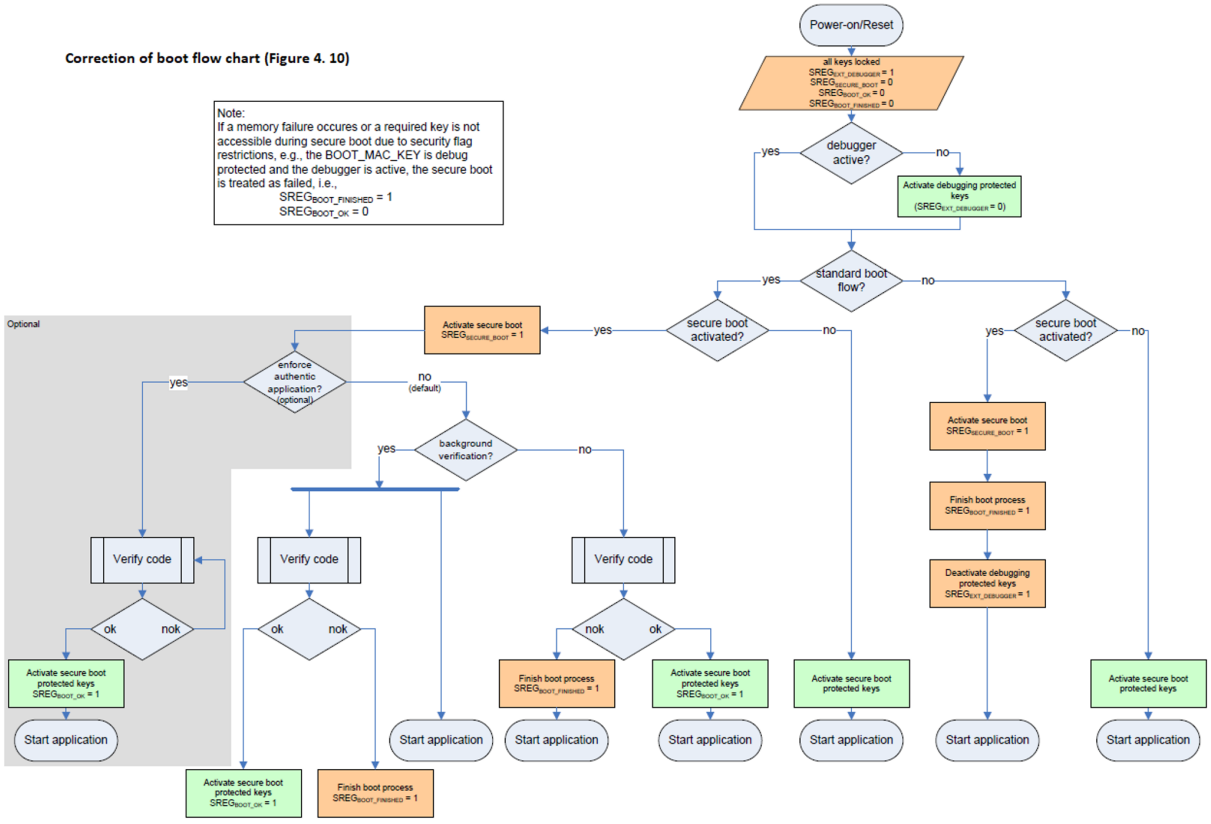

Figure 1: Correction of boot flow chart