BMW GROUP

Rolls-Royce Motor Cars Limited

Crypto Classic Integration Manual

Project	BMW AUTOSAR 4 Core Rel. 3
Author	BMW AG
Release Date	2017-12-14
Version	5.2.0
Status	Release
Hotline	+49 89 382 - 32233
Contact	bac@bmw.de
	https://asc.bmw.com/jira/browse/BSUP (extern)
	https://asc.bmwgroup.net/jira/browse/BSUP (intern)

Revision History

Version	Date	Description
5.2.0	2017-12-14	Version Update
5.1.0	2017-11-09	Version Update
5.0.0	2017-10-12	Initial version for SP2021

Company
Bayerische
Motoren Werke
Aktiengesellschaft
Postal address
BMW AG
80788 München
Office address
Forschungs- und
Innovationszentrum
(FIZ)
Hufelandstr. 1
80937 München
Telephone
Switchboard
+49 89 382-0
Internet
www.bmwgroup.com

Table of Contents

1 Introduction

This Integration Manual describes the basis functionality and the configuration and integration of the Crypto module.

Functional overview

The main objective of the Crypto functionality is to provide a hardware independant cryptography library which shall be usable by all BMW ECUs.

The Crypto Module provides the following Crypto primitives :

- SHA-256
- SHA-384
- SHA-512
- ECDSA Signature verification (P-256/P-384/P-521)
- Certificate parsing and signature verification.

2 Related documentation

References

3 Limitations

No limitations are known.

4 Software Architecture

Dependencies on AUTOSAR modules

The current version of the Module Crypto does not depend on any BSW module.

Dependencies to other modules

Crypto includes headers from the BMW BUtil module.

5 Integration

Configuration of other Modules

No other module needs to be configured to perform integration of the Crypto library.

Configuration

For a detailed description of the configuration parameters, please consult the description in the Crypto parameter definition file.

Configuration of the RTE

There are no special requirement for RTE configuration.

Key File

The security key file is generated with BMW backend system SWL-SEC for every ECU. This key file named Crypto_Keys.h needs to be included directly.