

Release Notes CryptoClassic

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	Issues
5.2.0	2017-12-14	BAC-6668, BAC-6671
5.1.0	2017-11-09	BAC-6508, BAC-6451
5.0.0	2017-10-12	

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

1 Module Description

The Crypto module provides access to a Cryptographic library and can be used as an AUTOSAR Crypto driver.

2 Revisions and Modifications

Revision 5.2.0 [Released]

Item	Description
CR ID:	BAC-6668
CR Headline:	Incorrect name of Integration Manual
Description of Issues:	Integration Manual is incorrectly named.
Description of Changes:	Integration Manual have been correctly named.
Changed Files:	doc/CryptoClassic_IntegrationManual.pdf
Compatibility:	

Item	Description
CR ID:	BAC-6671
CR Headline:	Add functionalities for RSA Verify (PKCS1 V2)
Description of Issues:	RSA verification feature (PKCS1 V2) needs to be implemented
Description of Changes:	RSA verification feature is implemented. The corresponding interface has been added to the jumtable and the corresponding parameters are now present in the paramconf
Changed Files:	cfgdesc/CryptoClassic_paramdef.arxml generate/src/Crypto_JumpTable.c.pgen generate/include/Crypto_JumpTable.h.pgen
Compatibility:	

Revision 5.1.0 [Released]

Item	Description
CR ID:	BAC-6508
CR Headline:	Update jumtable generation to new Page version
Description of Issues:	Pgen files used to generate Crypto jumtable don't work with the new version of page.
Description of Changes:	Updated the files so the jumtable can be generated again.
Changed Files:	src/Crypto_CertificateManagement.c generate/include/Crypto_CertificateManagement.h.pgen generate/src/Crypto_CertificateManagement.c.pgen CMakeLists.txt generate/src/Crypto_JumpTable.c.pgen generate/include/Crypto_JumpTable.h.pgen
Compatibility:	

Item	Description
CR ID:	BAC-6451
CR Headline:	Add functionalities Hashes SHA 384 and SHA512
Description of Issues:	The hashes SHA 384 and SHA 512 are missing from the BMW Crypto library.
Description of Changes:	Functionalities have been added to the generic part. Jumptables have been adapted with new functions to allow access to said functionalities.
Changed Files:	cfgdesc/CryptoClassic_paramdef.arxml template/include/Crypto_MemMap.h.sample generate/include/Crypto_JumpTable.h.pgen generate/src/Crypto_JumpTable.c.pgen
Compatibility:	

Revision 5.0.0 [Released]

Item	Description
CR ID:	
CR Headline:	Initial Release for SP2021
Description of Issues:	Initial Release for SP2021
Description of Changes:	Initial Release for SP2021
Changed Files:	
Compatibility:	