Release Notes CryptoGeneric

Project	BMW AUTOSAR Core 4 Rel. 3 and adaptive BMW AUTOSAR Core Rel. 1
Author	BMW AG
Release Date	2017-12-14
Version	5.2.0
Status	Release
Hotline	+49 89 382 - 32233 (classic) / +49 89 382 - 22522 (adaptive)
Contact	bac@bmw.de (classic) / abac@bmw.de (adaptive) 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-6720, BAC-6588, BAC-6681, BAC-6671
5.1.0	2017-11-09	BAC-6548, 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

TODO

2 Revisions and Modifications

Revision 5.2.0 [Released]

Item	Description
CR ID:	BAC-6720
CR Headline:	Clean up Crypto
Description of Issues:	Clean up : - Removed pieces of unused code. - Fix warnings.
Description of Changes:	Removed unused code and comments. Fixed some warnings.
Changed Files:	src/Crypto_Keys.c src/Crypto_SHA256.c src/fp_mul.c src/fp_sqr.c
Compatibility:	

Item	Description
CR ID:	BAC-6588
CR Headline:	Use tomfastmath for Crypto Math functions
Description of Issues:	Changed Big Number Math functions to gain speed.
Description of Changes:	Switched to Tomfastmath based functions. (Internal functions change only).
Changed Files:	src/fp_cmp_d.c generate/include/Crypto_Cfg.h.pgen src/fp_add.c cfgdesc/Crypto_paramdef.arxml src/fp_sqr_comba_20.c src/Crypto_Math.c src/fp_mod_2d.c src/fp_cmp.c CMakeLists.txt src/fp_lshd.c src/fp_mulmod.c src/fp_rshd.c src/s_fp_sub.c src/fp_montgomery_calc_normalization.c src/fp_mul_comba.c src/fp_mul_2d.c src/fp_mul_comba.h src/fp_2expt.c src/fp_mul_comba_small_set.c

	src/fp_sqr.c src/s_fp_add.c src/fp_div.c src/Crypto_Math_Intern.h src/Crypto_EccOperations.c src/fp_montgomery_setup.c src/fp_montgomery_reduce.c src/fp_reverse.c src/fp_invmod.c src/fp_mul_comba_20.c src/fp_sqr_comba_small_set.c src/Crypto_Common_Intern.h src/fp_sqr_comba_generic.c src/fp_div_2d.c src/fp_mod.c src/fp_mul_2.c src/fp_sqr_comba.h src/fp_set.c src/fp_count_bits.c src/mp_read_unsigned_bin.c src/fp_sqr_comba.c src/fp_mul.c src/fp_div_2.c src/Crypto_ECDSA.c src/Crypto_ECDSA_Intern.h src/fp_mul_d.c src/fp_cmp_mag.c src/fp_sub.c src/fp_to_unsigned_bin.c
Compatibility:	

Item	Description
CR ID:	BAC-6681
CR Headline:	Fix or justify Misra warnings/errors
Description of Issues:	Some Misra warnings have to be corrected
Description of Changes:	Correct some MISRA warnings when possible.
Changed Files:	Corrected code to reduce number of MISRA warnings.
Compatibility:	

Item	Description
CR ID:	BAC-6671
CR Headline:	Add functionalities for RSA Verifiy (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 jumptable and the corresponding parameters are now present in the paramconf

Changed Files:	generate/include/Crypto_Cfg.h.pgen src/Crypto_HashDescriptor.c include/Crypto_KeyManagement.h CMakeLists.txt src/zeromem.c include/Crypto_RSA.h src/Crypto_EccOperations.c cfgdesc/Crypto_paramdef.arxml src/Crypto_RSA.c src/Crypto_Math_Intern.h src/Crypto_KeyManagement_Intern.h include/Crypto_Hash.h src/Crypto_Keys.c include/Crypto_Common.h src/Crypto_Common_Intern.h include/Crypto.h src/fp_unsigned_bin_size.c src/Crypto_RSA_Intern.h src/mem_neq.c include/Crypto_ECDSA.h src/Crypto_ECDSA.c src/Crypto_ECDSA_Intern.h src/fp_exptmod.c
Compatibility:	

Revision 5.1.0 [Released]

Item	Description
CR ID:	BAC-6548
CR Headline:	Improve math functions performance by allowing inlining
Description of Issues:	BMW Math functions allow inlining (as defined in AUTOSAR) in order to improve performance.
Description of Changes:	Grouped Math functions in a file and declared the relevant as LOCAL_INLINE to allow optimization from the integrator.
Changed Files:	src/bn_mp_copy.c src/bn_mp_mul_d.c src/bn_mp_div_2.c src/bn_s_mp_add.c src/bn_mp_count_bits.c src/Crypto_Math.c src/bn_mp_2expt.c src/bn_mp_init_copy.c src/bn_mp_read_unsigned_bin.c.c src/bn_fast_mp_montgomery_reduce.c src/bn_mp_cmp_mag.c src/bn_mp_div.c

	src/bn_mp_montgomery_reduce.c src/bn_mp_montgomery_setup.c src/bn_mp_zero.c src/bn_mp_mod_2d.c src/bn_s_mp_sub.c src/bn_fast_s_mp_mul_digs.c src/bn_mp_invmod.c src/bn_mp_mod.c src/bn_fast_mp_invmod.c src/bn_s_mp_sqr.c src/bn_mp_cmp_d.c src/bn_mp_sqr.c src/bn_mp_set.c src/bn_mp_invmod_slow.c src/bn_mp_mul.c src/bn_mp_montgomery_calc_normalization.c src/bn_mp_mul_2.c src/bn_mp_exch.c src/bn_mp_sub.c src/bn_mp_rshd.c src/bn_mp_clamp.c src/bn_mp_lshd.c src/bn_mp_add.c src/bn_mp_mul_2d.c src/bn_mp_div_2d.c src/Crypto_Math_Intern.h src/bn_mp_mulmod.c src/bn_s_mp_mul_digs.c src/bn_mp_cmp.c CMakeLists.txt src/bn_mp_init_size.c
Compatibility:	

Item	**Description**
CR ID:	BAC-6508
CR Headline:	Update jumptable generation to new Page version
Description of Issues:	Pgen files used to generate Crypto jumptable don’t work with the new version of page.
Description of Changes:	Updated the files so the jumptable can be generated again.
Changed Files:	include/Crypto_Certificate.h src/Crypto_CertificateHandling.c
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:	template/include/Crypto_MemMap.h.sample include/Crypto_Hash.h src/Crypto_SHA256.c src/Crypto_BitOperations.h CMakeLists.txt src/Crypto_SHA512.c src/Crypto_SHA384.c
Compatibility:	

Revision 5.0.0 [Released]