ROM V2.0 RELEASE NOTES

Product Family: **BLE SOC**

Part Number: EM9305

Keywords: ROM, new features, bug fixes, API, 2.0

PURPOSE

The purpose of this document is to list the new features and bug fixes that have been implemented in the ROM version 2.0.

This detailed description is split in the following parts:

1. New features and behaviour (§1, Table 1-1)
2. Fixes (§0, Table 2-1)
3. API (§3)

The §1 exposes the new features that have been added into the ROM v2.0, along with improvements.

The §2 lists the bug found in ROM v1.0 that have been fixed into ROM v2.0.

The §3 list the new functions that have been added in ROM v2.0 and the function that have been removed and that are no longer useable.

REFERENCE DOCUMENTS

N/A

1. ROM NEW/CHANGED FEATURES

The Table 1-1 lists the new and modified features, changing how the new ROM v2.0 behaves compared to ROM v1.0 (when relevant).

Description	ROM v1.0	ROM v2.0
Start-up behaviour if NVM empty	Halting CPU.	Entering CONFIG mode
Change behaviour if EM info page 3 CRC check fails.	Halting CPU.	Resetting CPU.
Change behaviour if user info page 2 CRC check fails.	Halting CPU.	Resetting CPU.
Change behaviour if EM info page 3 is not locked	Resetting CPU.	Continue with startup process without resetting the CPU.
DCDC default configuration to 1.9v	Step-up mode 1.7 volts.	DCDC configured in step-up mode 1.9 volts.
Memory manager	-	Integrated in ROM as a submodule.
Persistent RAM usage	-	Optimized.
Support of deep sleep mode	-	Deep sleep support added with or without DRAM retention.
Write @address without response	-	Command added
CRC32 compute function	-	Function optimized to handle both 8 bits and 32 bits words.
PML bits critical section	-	Updating some PML bits is done through a critical section (IRQ disabled).
Transport speed improvement	-	Doubling size of buffers used by transport and activating buffers ring management.
MAC address read command	-	Command added.
DMA support for SPI and UART transport	-	DMA support added.
Security libraries	AES & CCM libraries v3.1.	AES & CCM libraries v3.2 integrated to replace v3.1.
Schnorr key read command	-	Added

Table 1-1: List of new/changed features introduced in ROM v2.0

2. ROM V1.0 FIXES

The Table 2-1 list the bugs found in ROM v1.0 that have been fixed in ROM v2.0.

Description	ROM v2.0
Wrong voltage doubler configuration when resuming from sleep mode	Fixed
DPR and NVM test registers default value not reset at start-up	Fixed
Programing last 32 bits word of a NVM page skipped	Fixed
VBat level not correctly set	Fixed
PML DCDC and ADC period configuration not done at the same time	Fixed
Incorrect procedure for switching clock between 48 MHz to 24 MHz back and forth	Fixed
Read & Write @address works on a byte by byte basis which is not efficient	Fixed (operations are done on 32 bits basis when correctly aligned).
Write @address wrong data alignment	Fixed, aligned on multiple of 4 bytes.
HTAL not started on sleep mode resuming	Fixed
RAM retention forced to 0 when entering deep sleep mode	Fixed, RAM retention not forced to 0 anymore.
RAM usage by ROM lead to scattered areas	Fixed, RAM usage optimized
DCDC T_1 and T_2 configuration not properly set	Fixed

Table 2-1: List of bug fixes introduced in ROM v2.0

3. API

3.1 NEW FUNCTIONS

The following function sorted by alphabetical order have been added in ROM v2.0.

- AES_CBC_Decrypt
- AES_CBC_Encrypt
- AES_CBC_InitCtx
- AES_CCM_DecryptAndMAC
- AES_CCM_EncryptAndMAC
- AES_CCM_GetMAC
- AES_CCM_Hash_Additional_Data
- AES_CCM_InitCtx
- AES_ClearKey
- AES_CMAC_Compute
- AES_CMAC_GetMAC
- AES_CMAC_InitCtx
- AES_CTR_Decrypt
- AES_CTR_Encrypt
- AES_CTR_InitCtx
- AES_ECB_Decrypt
- AES_ECB_Encrypt
- AES_ECB_InitCtx
- AES_ExecuteAHB
- AES_ExecuteKeyContainer
- AES_GCM_DecryptAndMAC
- AES_GCM_EncryptAndMAC
- AES_GCM_GetMAC
- AES_GCM_GMAC
- AES_GCM_Hash_Additional_Data
- AES_GCM_InitCtx
- AES_GenerateAuthenticateChallenge
- AES_GetData
- AES_InvalidateKeyContainer
- AES_KeyContainersEraseLock
- AES_KeyContainersLockPage
- AES_KeyContainersWriteLock
- AES_LoadAHB
- AES_LoadData
- AES_LoadKeyContainer
- AES_LockKeyContainer
- AES_ProcessBlock
- AES_ProcessBlockKeyContainer
- AES_SetData
- AES_SetKey
- AES_SetKeyContainer
- AES_Unload_data
- AES_WaitUntilReady
- BOOT_RomBootUp
- COMMON_hw_crc32
- Compare_big
- CTR_DRBG_AES_ENCRYPT
- CTR_DRBG_DF
- CTR_DRBG_DF_ComputeMAC_Part
- CTR_DRBG_DF_GetWordpointer
- CTR_DRBG_Generate

- CTR_DRBG_Generate_Internal
- CTR_DRBG_Generate_WithDF
- CTR_DRBG_IncrementBuffer
- CTR_DRBG_Instantiate
- CTR_DRBG_Instantiate_Internal
- CTR_DRBG_Instantiate_WithDF
- CTR_DRBG_Update
- DMA_ClearError
- DMA_ClearInterrupt
- DMA_Enable
- DMA_EnableChannel
- DMA_EnableInterrupts
- DMA_GetBusyStatus
- DMA_GetConfiguration
- DMA_GetPriority
- DMA_GetTransferStatus
- DMA_InitiateTransfer
- DMA_IsChannelEnabled
- DMA_IsEnabled
- DMA_IsOneChannelEnabled
- DMA_ReadInterrupt
- DMA_ResetChannel
- DMA_SetConfiguration
- DMA_SetHwTriggerSource
- DMA_SetPriority
- ECC_ComputePubKey
- ECC_ComputeSharedKey
- ECC_GeneratePrivateKey
- ECC_isPublicKeyValid
- ECCSchnoor_GenerateVerifierChallenge
- ECCSchnoor_Verify
- ECDSA_Verify
- EMSystem_ClearSleepModeRequest
- EMSystem_GetSleepModeRequest
- EMSystem_HandleCommand
- EMSystem_HciResetNotification
- EMSystem_Init
- EMSystem_MemoryRead
- EMSystem_MemoryWrite
- EMSystem_RegisterCommandsHandler
- EMSystem_Resume
- EMTransportManager_Init
- EMTransportManager_IsBusy
- EMTransportManager_Process
- EMTransportManager_Resume
- EMTransportManager_SendCommandCompleteEvent
- EMTransportManager_SendCommandStatusEvent
- EMTransportManager_SendEventInternal
- EMTransportManager_SendHardwareErrorEvent
- EMTransportManager_SetSendEventFct
- Erase_big
- FinalInvZ
- gEMSCmdRomCommandParsers
- gEMSCmdRomNumberOfCommandParsers
- GenerateRandomBig

- GetPRNG
- GPIO_DisableHighDrive
- GPIO_DisableJtag
- GPIO_EnableHighDrive
- GPIO_EnableJtag
- GPIO_GetInputFunctionPin
- GPIO_GetMinimumDebounce
- GPIO_GetOutputPinFunction
- GPIO_Init
- GPIO_Restore
- GPIO_Save
- GPIO_SetInputFunctionPin
- GPIO_SetMinimumDebounce
- GPIO_SetOutputPinFunction
- gSPIS_Transport
- gUART_Transport
- InitPRNG
- InvertMSWandLSW
- InvMod_binary
- IRQHandler_ArcDmaDone
- IRQHandler_ArcDmaError
- IRQHandler_SpiSlaveRx
- IRQHandler_SpiSlaveTx
- IRQHandler_UartRx
- IRQHandler_UartTx
- Memory_AllocateNonpersistent
- Memory_AllocateNonpersistentAligned
- Memory_AllocatePersistent
- Memory_AllocatePersistentAligned
- Memory_GetFreeSize
- Memory_GetNonpersistentReservedSize
- Memory_GetNonpersistentSize
- Memory_GetPersistentReservedSize
- Memory_GetPersistentSize
- Memory_GetPoolSize
- Memory_InitEx
- mul2_big
- mul4_big
- mul_bigAsm256
- mul_bigModN
- NVMINFO_CheckBlock
- NVMINFO_CheckFlag
- NVMINFO_CheckVBAT1_1p7v_StepUpModeFlag
- NVMINFO_GetMacAddress
- NVMINFO_HammingDistance
- NVMINFO_LoadBlock
- PML_DidBootWithoutDRAMRetention
- PML_GetResetFlags
- PML_SetDcdcAdcPeriods
- PML_SetDcdcT2Auto
- RedModP256
- RNG_GetAndHealthTest
- RNG_IsReady
- RNG_Random
- RNG_Random16

- RNG_Random32
- RNG_Random8
- RNG_SetSource
- SetPRNGCtx
- SPIS_BlockCommunication
- SPIS_Enable
- SPIS_GetStatusByte
- SPIS_HasPendingData
- SPIS_InitBuffers
- SPIS_InitNew
- SPIS_ReceiveDataEx
- SPIS_Restart
- SPIS_Restore
- SPIS_Save
- SPIS_SendDataEx
- SPIS_SetConfiguration
- SPIS_SetStatusByte
- sub_bigAsm256
- sub_bigModN
- UART_BlockCommunication
- UART_Enable
- UART_HasPendingData
- UART_InitBuffers
- UART_InitNew
- UART_ReceiveDataEx
- UART_Restart
- UART_Restore
- UART_Save
- UART_SendDataEx
- UART_SetBaudRate
- UART_SetBaudRateEx
- UART_SetConfiguration

For more details on how to use the above mentioned function, the reader shall check the SDK API documentation.

3.2 REMOVED FUNCTIONS

The following function does not exist anymore within the ROM v2.0.

- COMMON_hw_crc32_bytes
- gNewOpcodesLUT
- PML_GetLdoDigLevel
- PML_GetLdoVccLevel
- PML_SetAdcPeriod
- PML_SetDcdcPeriod
- PML_SetLdoDigLevel
- PML_SetVoltageDoublerPwmValue

EM Microelectronic-Marin SA ("EM") makes no warranties for the use of EM products, other than those expressly contained in EM's applicable General Terms of Sale, located at http://www.emmicroelectronic.com. EM assumes no responsibility for any errors which may have crept into this document, reserves the right to change devices or specifications detailed herein at any time without notice, and does not make any commitment to update the information contained herein.

No licenses to patents or other intellectual property rights of EM are granted in connection with the sale of EM products, neither expressly nor implicitly.

In respect of the intended use of EM products by customer, customer is solely responsible for observing existing patents and other intellectual property rights of third parties and for obtaining, as the case may be, the necessary licenses.

Important note: The use of EM products as components in medical devices and/or medical applications, including but not limited to, safety and life supporting systems, where malfunction of such EM products might result in damage to and/or injury or death of persons is expressly prohibited, as EM products are neither destined nor qualified for use as components in such medical devices and/or medical applications. The prohibited use of EM products in such medical devices and/or medical applications is exclusively at the risk of the customer