Release Note

Revision 1.00
June 2022

Embedded Trust Device support for Arm

Introduction
This release note describes the latest features, new device support, and program corrections.

Contents

Highlights........1
Embedded Trust Device support........2
Orbit Device support........2
Installing updates........3
Important information........3
Version supported........3
Trust zone support........3
EFM32xG22 lockdown........3
RA2 Installing SBM to the board........3

Highlights

New Embedded Trust supports for devices from ST Microelectronics (STM32F4x), Renesas (RA2xx) and Silicon Labs (EFM32xG22).
New Orbit supports for devices from ST Microelectronics (STM32F4x), Renesas (RA2xx), Infineon (CY8C63xx) and Silicon Labs (EFM32xG22).
Updated device support on STM32U5x, including Trust zone.

Embedded Trust Device support

ST Microelectronics	Renesas	Microchip	NXP	Silicon Labs
STM32F4x	RA6Mx[2]	SAML11	i.MX RX 10x4[3]	EFM32xG22
STM32F7x	RA4Mx[2]		LPC55xx	
STM32L4x	RX7xx (72M/72N)		K8x, K7x	
STM32L5	RX6xx (65N)		K6x, K5x	
STM32H7x	RXxxT (RX72T)		K2x, K1x	
STM32U5x	RA2xx		KV5x	
STM32WB5x[1]				

Orbit Device support

ST Microelectronics	Renesas	Microchip	NXP	Infineon	Silicon Labs
STM32F4x	RA6Mx[2]	SAML11	i.MX RX 10x4[3]	CY8C63xx	EFM32xG22
STM32F7x	RA4Mx[2]	PIC32CM Lx	LPC55xx		
STM32L4x	RX7xx (72M/72N)		K8x, K7x		
STM32L5	RX6xx (65N)		K6x, K5x		
STM32H7x	RXxxT (RX72T)		K2x, K1x		
STM32U5x	RA2xx		KV5x		
STM32WB5x[1]					

Notes:
*subject to minimal resource memory (Flash / SRAM / TRNG)

(1) STM32WB5x Application processor provisioning only

(2) Renesas RA Cortex-M4 core centric

(3) NXP i.MX RX 10x4 Internal NVM variants

Installing updates

Updated device support is supplied in the form of a zip file archive.
These will be named with the following conventions:
et_efm32pg22c200f512im40 - Embedded trust device support for EFM32xG22
orbit_efm32pg22c200f512im40 - Orbit trust device support for EFM32xG22
These should be deployed to the relevant directory for the local ET Arm Installation.
Embedded Trust: [EMBWinstall\arm]
Orbit: [EMBWinstall\arm\stz\device_properties\arm]
Where: [EMBWinstall is the embedded workbench installation directory],
e.g. “C:\Program Files\IAR Systems\Embedded Workbench”

Important information

Version supported

Embedded Trust– ET 2.00.1

Trust zone support

Is not available in this release for EFM32xG22, will be added in a later version.

EFM32xG22 lockdown

Temporary lockdown on this device is not possible, locking down parts of flash and would persist through reset cannot be achieved. The lock for individual flash pages must be reapplied every time a device is started (which is done by SBM as part of start-up routine).
Permanent lockdown additionally disables the debug port. However, it is not possible to permanently disable mass erase on this device, therefore it is still possible to issue a software mass erase command (e.g. by calling “MSC_MassErase()” available through Gecko SDK) or use a device-specific AAP mechanism to mass erase the device and re-enable the debug port afterwards (e.g. by using a device unlock option available through Simplicity Studio).
Further details can be found in the device porting guide.

RA2 Installing SBM to the board

When downloading an SBM from workbench an "Illegal register read" error is generated. This can safely be ignored.

RA2 lockdown

However, it is not possible to permanently disable mass erase on this device, therefore it is still possible to issue a software mass erase command.
Further details can be found in the device porting guide.