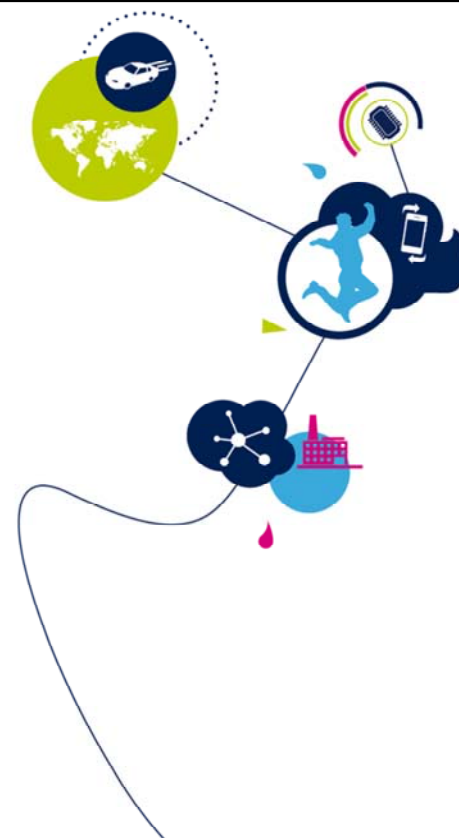


STM32MP1 – BSEC

Boot and Security Controller
Revision 1.0



Hello, and welcome to this presentation of the STM32MP1
Boot and Security Controller.

- BSEC is intended to read, program and control the accesses to the on-chip One Time Programmable (OTP) bits.
- 3K bit effective OTP area is organized in 2 regions with different properties:
 - Lower OTP area: 1K bits, 2:1 redundancy, incremental bit programming
 - Upper OTP area: 2K bits, ECC protection, word programming only
- The OTP area is used to store non volatile information:
 - Manufacturing data (Memory repair, Analog Trim, Chip ID .etc)
 - Device life cycle information to control debug access and device provisioning
 - Boot configuration.
 - Keys and security sensitive information (ST secret keys and OEM secrets)



The Boot and Security Controller is intended to read, program and control the accesses to the on-chip One Time Programmable (OTP) bits.

The 3K bit effective OTP area is organized in 2 regions with different properties:

- Lower OTP area: 1K bits, 2:1 redundancy, incremental bit programming
- Upper OTP area: 2K bits, ECC protection, word programming only

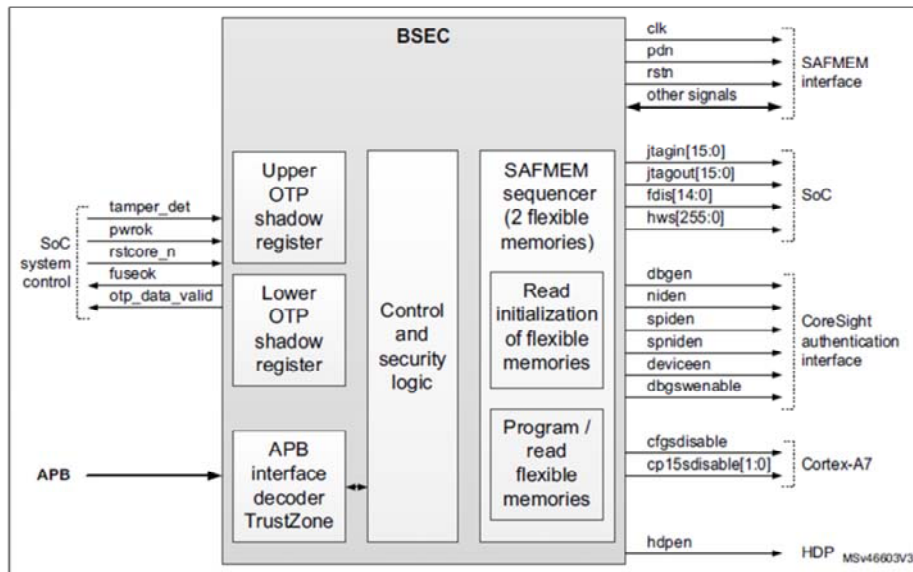
The OTP area is used to store non volatile information:

- Manufacturing data (Memory repair, Analog Trim, Chip ID .etc)

- Device life cycle information to control debug access and device provisioning
- Boot configuration.
- Keys and security sensitive information (ST secret keys and OEM secrets)

BSEC block diagram

3



This is a simplified block diagram of the Boot and Security Controller

SAFMEM is a Fuse Box divided in 2 regions, Lower and Upper OTP areas with respectively 1K bit (bit programmable) and 2K bit (word programmable).

The control logic supports reading and programming of the OTP bits.

OTP bits are read into shadow registers on Reset.

Several enabling signals are exported out to the SoC.

The shadow registers access and value of the enabling signals are conditioned to the Device Life Cycle state determined by the first words.

- 32-bit APB4 interface
- 4096 OTP bits (3072 effective bits)
- Global programming locking by sticky bits
- Permanent OTP program locking per word
- OTP word programming lock by sticky bits during the Boot phase
- Shadow OTP registers can be individually write locked by sticky bits during the Boot phase
- Shadow OTP registers can be individually read locked by sticky bits during the Boot phase to prevent reloading.



BSEC main features are:

- 32-bit APB4 interface
- 4096 raw OTP bits (=3072 effective bits) because of the 2:1 redundancy for lower OTPs
- Global programming locking by sticky bits
- Permanent OTP program locking per word
- OTP word programming lock by sticky bits during the Boot phase
- Shadow OTP registers can be individually write locked by sticky bits during the Boot phase
- Shadow OTP registers can be individually read locked by sticky bits during the Boot phase to prevent reloading.

- BSEC Scratch register for communication with external agent to store boot parameters.
- JTAG SOC interface via BSEC_JTAGIN and BSEC_JTAGOUT registers as communication channel to the JTAG TAP controller.
- Disturb-check to qualify OTP word value to improve the resistance to hardware attacks by clock and power glitches during OTP read.



The other key features are:

- BSEC Scratch register for communication with external agent to store boot parameters
- A JTAG SOC interface via BSEC_JTAGIN and BSEC_JTAGOUT registers as communication channel to the JTAG TAP controller.
- There is a disturb-check feature to qualify OTP word value to improve the resistance to hardware attacks by clock and power glitches during OTP read.

- List OTP words and bit fields.
- OTP programming (STM or User)
- Permanently locked word which are factory programmed.
- Sticky lock attributes controlled by BOOT ROM and set according to device live cycle.

** For more details see Product Reference Manual: section OTP mapping



The OTP map is describing:

- The full list of OTP words and bit fields
- Information about who is allowed to program the OTP words (STMicroelectronics or the User)
- If words are permanently locked as factory programmed: For example analog Trim and memory repair.
- Sticky lock bits controlled by BOOT ROM and set according to the device live cycle, there are 3 sticky bits per OTP word: Shadow write lock, Shadow reload lock and Shadow program lock

For more details see Product Reference Manual: section OTP mapping.

- 32 words, bit programmable with 2:1 redundancy
- Used for:
 - Device Life cycle and SoC Features (ST)
 - Boot device selection and user configuration (User)
 - Hardware configuration (ST) Factory trim bits, Memory repair .etc.
 - Product specific settings (User) BOR threshold, IWDG behavior .etc.
 - Public Key Hash



The Low OTP area is 32 words , which are bit programmable only and with 2:1 redundancy. It is used as:

- Words 0 to 2: CFG0 to CFG2 are reserved by STMicroelectronics to control the life cycle and SoC Features enabled in the Product. Only one bit from CFG0 is accessible by the user to close the device after secret provisioning.
- Words 3 to 7 can be used to define the boot device selection.
- Words 16 to 24 are used for hardware configuration.
- Word 16 includes product specific settings for the user.
- Words 24 to 31 are used for Public Key hash.

Upper OTP mapping

- 64 words, word programmable only with inherent ECC protection
- Used for:
 - ST ECDSA Private and ST Public ECDSA Certificate for SSP (ST)
 - MAC address (User)
 - RMA password (User)
 - Board information (User)
 - Remaining words can be used to store Non Volatile keys and secrets from user



The upper OTP area is 64 words, programmable only with ECC protection, and used for:

- ST ECDSA Private and ST Public ECDSA Certificate for SSP (ST)
- MAC address (User)
- RMA password (User)
- Board information (User)
- 36 Remaining words can be used to store non-volatile keys and secrets from user.

• BSEC is TrustZone aware with conditional access according to 3 register regions:

- BSEC Control registers
- Lower OTP shadow registers
- Upper OTP Shadow registers

Write access permissions vs region

OTP mode	Control registers ⁽¹⁾		Lower OTP shadow registers		Upper OTP shadow registers	
	APB secure	APB non-secure	APB secure	APB non-secure	APB secure	APB non-secure
OTP-SECURED	Yes	No	Yes	No	Yes	No
OTP-INVALID	No	No	No	No	No	No

Read access permissions vs region

OTP mode	Control registers ⁽¹⁾		Lower OTP shadow registers		Upper OTP shadow registers	
	APB secure	APB non-secure	APB secure	APB non-secure	APB secure	APB non-secure
OTP-SECURED	Yes	Yes	Yes	Yes	Yes	No
OTP-INVALID	Yes	No	No	No	No	No

• Read and Write permission are determined according to OTP mode



BSEC is TrustZone aware with conditional access according to 3 regions:

- BSEC Control registers
- Lower OTP shadow registers
- Upper OTP Shadow registers

For each regions, Read and Write permissions are determined according to the OTP mode.

- Device Life Cycle is controlled by OTP word 0
- Only relevant state after device manufacturing are shown here

	BSEC_OTP_DATA0 [6:0]	OTP mode	BSEC_OTP_STATUS SECURE	BSEC_OTP_STATUS FULLDBG	BSEC_OTP_STATUS INVALID
Open-device	0xxx1x1	OTP-SECURED open_device	1	0	0
	0 x1xxx				
	0xx11xx				
	0 xxxx1				
closed-device	1xxx1x1	OTP-SECURED closed_device	1	0	0
	1 x1xxx				
	1xx11xx				
	1 xxxx1				
	All other values	OTP-INVALID	x	x	1



The table is showing a simplified view of the Device Life cycle

Once the secret is provisioned into the OTP words during manufacturing, The device state is set to OTP-SECURED.

The transition from open-device to closed-device state is later controlled by programming the OTP word 0 bit 6 to '1'. In case the OTP fuse or word 0 is compromised, the device is set into OTP-INVALID state, which is an 'end-of-life' state protecting OTP secrets.

- On a system-reset, BSEC automatically updates all shadow registers.
- OTP mode is determined during this phase.
- BSEC_OTP_STATUS, BSEC_OTP_DISTURBED and BSEC_OTP_ERROR registers are also updated.
- **fuseok** signal is asserted at the end of this phase. This signal is used to release the reset to the SoC.



On a system-reset, BSEC automatically updates all shadow registers.

OTP mode is determined during this phase.

BSEC_OTP_STATUS, BSEC_OTP_DISTURBED and BSEC_OTP_ERROR registers are also updated.

fuseok signal is asserted at the end of this phase. This signal is used to release the reset to the SoC.

- To trigger a read operation, the software must set BSEC_OTP_CONTROL register with the word number given in ADDR field and with PROG bit set to 0.
- The software can check the BUSY bit from the BSEC_OTP_STATUS register: Once cleared, this BUSY bit indicates that the read operation is complete.
- When the read operation is finished, the BSEC state machine updates the “disturbed” and “error” status registers.
- BSEC parameters depending on OTP content, are also updated when the corresponding OTP words are read. The OTP mode is updated when a read operation of the word 0 is performed.



To trigger a read operation, the software must set the BSEC_OTP_CONTROL register with the word number given in ADDR field and with PROG bit set to 0.

The software can check the BUSY bit from the BSEC_OTP_STATUS register: Once cleared, this BUSY bit indicates that the read operation is complete.

When the read operation is finished, the BSEC state machine updates the “disturbed” and “error” status registers.

BSEC parameters depending on OTP content, are also updated when the corresponding OTP words are read. The OTP mode is updated when a read operation of the word 0 is performed.

- An OTP word can be written in multiple steps. The word value is updatable by adding bits to 1, but a bit already set to 1 cannot be written back to 0.
- To trigger a programming operation, the two following steps are required:
 - Write the word value to the BSEC_OTP_WRDATA register
 - Write the BSEC_OTP_CONTROL register with:
 - word number in ADDR field
 - PROG bit set to 1
 - LOCK bit set to 0.
- The software checks the BUSY bit from the BSEC_OTP_STATUS register: Once cleared, this BUSY bit indicates that the write operation is complete.
- In the same register, PRGFAIL bit is set if the write operation has failed.



An OTP word can be written in multiple steps. The word value can be updated by setting additional bits to '1' only. A bit already set to 1 cannot be reset to 0.

To trigger a programming operation, the following two steps are required:

Write the word value to the BSEC_OTP_WRDATA register

Write the BSEC_OTP_CONTROL register with:

The word number in ADDR field

The PROG bit set to 1

The LOCK bit set to 0.

The software checks the BUSY bit from the

BSEC_OTP_STATUS register: Once cleared, this BUSY bit indicates that the write operation is complete.

In the same register, PRGFAIL bit is set if the write operation has failed.

- BSEC is enforcing debug access according to Device Life Cycle state
- BSEC_DENABLE register is driving hardware signals to SoC including CoreSight authentication interface and specific control signals

Signal	OTP-SECURED open_device	OTP-SECURED closed_device	OTP-INVALID	Comment
dbgen	1	0	0	CoreSight authentication
niden	1	0	0	CoreSight authentication
spiden	0	0	0	CoreSight authentication
spniden	0	0	0	CoreSight authentication
deviceen	1	0	0	CoreSight authentication
dbgswenable	0	0	0	CoreSight authentication
hdpen	0	0	0	Hardware debug port tracing
cfgsdisable	0	0	0	Disable some of Cortex®-A7 GIC secure access
cp15sdisable[1:0]	0b00	0b00	0b00	Disable some of Cortex®-A7 CP15 secure access



** For more details see Product Reference Manual: section BSEC Debug control

The Boot and Security controller is controlling the debug access according to the Device Life cycle state.

The BSEC_DENABLE register is driving several hardware signals to SoC including CoreSight authentication interface and specific control signals.

For more details see the Product Reference Manual in section: BSEC Debug control.