

7.8.3.3.13 KEYSLOT

Address offset: 0x500

Select key slot to operate on

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	
ID	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
Reset 0x00000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
ID	R/W	Field	Value ID	Value	Description																												
A	RW	ID	0..249	Select key slot ID to provision, push, read METADATA, revoke or block when the corresponding task is triggered.																													

7.8.3.3.14 SRC

Address offset: 0x504

Source address for provisioning

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	
ID	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
Reset 0x00000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
ID	R/W	Field	Value ID	Value	Description																												
A	RW	SRC		Source address for TASKS_PROVISION.																													

7.8.3.3.15 METADATA

Address offset: 0x508

Key slot metadata as read by TASKS_READMETADATA.

When EVENTS_METADATA has been generated, this register holds the key slot metadata.

Bit number	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	
ID	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
Reset 0x00000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
ID	R/W	Field	Value ID	Value	Description																												
A	RW	METADATA		Read metadata.																													

7.8.4 MPC — Memory Privilege Controller

The MPC peripheral is an address decoder with built-in security functions.

MPC enforces security for system memory access. It is used to divide the address space into smaller regions and assign permissions to these regions.

The main features of MPC are the following:

- Address decoding
- Configurable access permissions
- Error reporting

7.8.4.1 Override configuration

The MPC overrides are used to divide the address space into smaller regions and assign permissions to these regions.

When the device is reset, the memory in RAM and the non-volatile memory (NVM) is secure. Only secure CPUs and peripherals can read, write, or execute from secure memory.