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				G G G G G F E D C B A
Reset 0xFFFFFFFF				**1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1**
ID	R/W	Field	Value ID	Value	Description
			Enabled	1	Write-once enabled Writes to a 32-bit word in the BOOTCONF region are is only when the current data is 0xFFFFFFFF, otherwise the writes are ignored
F	RW1	LOCK			Enable lock of configuration register
			Disabled	0	Lock is disabled, and the RRAMC region configuration registers for the immutable boot region are writable.
			Enabled	1	Lock is enabled, and the RRAMC configuration registers for the immutable boot region are read-only.
G	RW1	SIZE			Immutable boot region size Configures the region size in kB

4.2.9.1.6 USER.ROT

Assets installed to establish initial Root of Trust in the device.

User RoT key materials

4.2.9.1.6.1 USER.ROT.PUBKEY[n].DIGEST[o] (n=0..3) (o=0..7)

Address offset: 0x200 + (n × 0x2C) + (o × 0x4)

First 256 bits of SHA2-512 digest over RoT public key generation [n].

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
Reset 0xFFFFFFFF				**1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1**
ID	R/W	Field	Value ID	Value	Description
A	RW1	VALUE			Value for word [o] in the key digest [n].

4.2.9.1.6.2 USER.ROT.PUBKEY[n].REVOKE[o] (n=0..3) (o=0..2)

Address offset: 0x220 + (n × 0x2C) + (o × 0x4)

Revocation status for RoT public key generation [n].

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
Reset 0xFFFFFFFF				**1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1**
ID	R/W	Field	Value ID	Value	Description
A	RW1	STATUS			Revocation status.
			NotRevoked	0xFFFFFFFF	Key not revoked.
					Any other value says the key is revoked.

4.2.9.1.6.3 USER.ROT.AUTHOPKEY[n].DIGEST[o] (n=0..3) (o=0..7)

Address offset: 0x2B0 + (n × 0x2C) + (o × 0x4)

First 256 bits of SHA2-512 digest over RoT authenticated operation public key generation [n].