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																													D	C	B	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
D	RW	SECATTR			Security mapping mask
			Masked	0	Permission setting SECATTR in OVERRIDE register will not be applied
			UnMasked	1	Permission setting SECATTR in OVERRIDE register will be applied

7.8.5 SPU — System protection unit

SPU configures the access privileges for a peripheral.

SPU allows configuring access controls individually for each peripheral, and for some peripheral features. For example, a DPPI channel can be configured with different access controls than the peripheral.

SPU controls access according to TrustZone security attributes. If a peripheral or feature is configured as secure, only TrustZone secure accesses are allowed. If a peripheral or feature is configured as non-secure, then accesses are allowed both from secure and non-secure masters.

For some peripherals, the peripheral's DMA has a separate security configuration. If the peripheral is configured as secure, the peripheral's DMA can be configured to perform either secure or non-secure accesses. If the peripheral is configured as non-secure, the peripheral's DMA will always perform non-secure accesses.

7.8.5.1 General concepts

The SPU provides the register interface to configure and enforce the access privileges per peripheral, and where applicable, individual features of the peripheral such as GPIO pins, DPPI channels, etc.

Any accesses to a peripheral or a peripheral feature are validated against the SPU configuration for the security attributes.

Security attributes of a peripheral normally applies to all registers of the peripheral. However, some peripherals have split security to individual features within the peripheral, such as individual pins or DPPI channels. For these split feature peripherals, access is granted on a per-bit or per-register level. Unless mentioned otherwise, the term peripheral is used in the remainder of this section to refer to both a peripheral and an individual peripheral feature.

Each APB bus has its own SPU instance that controls the resource of that bus. The SPU must be configured for security attributes of the peripherals. The SPU is always a secure peripheral.

- See Instantiation on page 216 to find the SPU instance used by the peripheral.
- The APB bus number can be extracted from the peripheral address. See Address format on page 11 to find the APB bus number for a peripheral.
- See Block diagram on page 9 for an overview over APB buses, the peripherals on that bus, and their controlling SPU instance.

See Address format on page 11 for information on extracting the Peripheral slave index from a peripheral address.