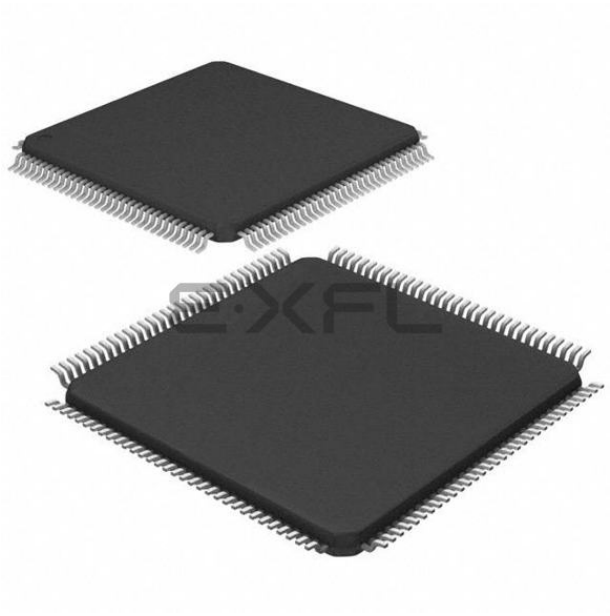
Microchip Technology - ATSAMD51P20A-AU Datasheet



Welcome to E-XFL.COM

What is "Embedded - Microcontrollers"?

"Embedded - Microcontrollers" refer to small, integrated circuits designed to perform specific tasks within larger systems. These microcontrollers are essentially compact computers on a single chip, containing a processor core, memory, and programmable input/output peripherals. They are called "embedded" because they are embedded within electronic devices to control various functions, rather than serving as standalone computers. Microcontrollers are crucial in modern electronics, providing the intelligence and control needed for a wide range of applications.

Applications of "Embedded - Microcontrollers"

Details	
Product Status	Active
Core Processor	ARM® Cortex®-M4F
Core Size	32-Bit Single-Core
Speed	120MHz
Connectivity	EBI/EMI, I²C, IrDA, LINbus, MMC/SD, QSPI, SPI, UART/USART, USB
Peripherals	Brown-out Detect/Reset, DMA, I²S, POR, PWM
Number of I/O	99
Program Memory Size	1MB (1M x 8)
Program Memory Type	FLASH
EEPROM Size	-
RAM Size	256K x 8
Voltage - Supply (Vcc/Vdd)	1.71V ~ 3.63V
Data Converters	A/D 32x12b; D/A 2x12b
Oscillator Type	Internal
Operating Temperature	-40°C ~ 85°C (TA)
Mounting Type	Surface Mount
Package / Case	128-TQFP
Supplier Device Package	128-TQFP (14x14)
Purchase URL	https://www.e-xfl.com/product-detail/microchip-technology/atsamd51p20a-au

Table 6-5. Trace Port Interface Unit Pinout

Signal	Supply	I/O pin
TRACE DATA[3]	VDDIO	PC24
TRACE DATA[2]	VDDIO	PC25
TRACE DATA[1]	VDDIO	PC26
TRACE DATA[0]	VDDIO	PC28
TRACE CLK	VDDIO	PC27
SWO	VDDIO	PB30, PC27

6.2.4 Supply Controller Pinout

The outputs of the Supply Controller (SUPC) are not mapped to the normal PORT functions. They are controlled by registers in the SUPC.

Table 6-6. SUPC Pinout

Signal	I/O pin
OUT0	PB01
OUT1	PB02

Note: If the RTC is enabled to use the pins shared with the SUPC, the RTC will have higher priority.

6.2.5 RTC Pinout

The pins used for Tamper Detection by the Real Time Counter (RTC) are not mapped to the regular PORT functions. These pins and their multiplexing is controlled by register settings of the RTC. If one or more pins of the tamper detection feature is not used by the RTC then the pin could be used for other IO functions, by ensuring the corresponding TAMPCTRL.INACT function is disabled.

Table 6-7. RTC Pinout

RTC Signal	I/O Pin
IN0	PB00
IN1	PB02
IN2	PA02
IN3	PC00
IN4	PC01
OUT	PB01

Important: If both Supply Controller (SUPC) and RTC are configured to drive pin PB1 or PB2, the RTC has priority.

Module	Source	Line
	RESRDY	119
ADC1 - Analog Digital Converter 1	OVERRUN	120
	WINMON	
	RESRDY	121
AC - Analog Comparators	COMP 0	122
	COMP 1	
	WIN 0	
DAC - Digital-to-Analog Converter	OVERRUN A 0	123
	OVERRUN A 1	
	UNDERRUN A 0	
	UNDERRUN A 1	
	EMPTY 0	124
	EMPTY 1	125
	RESRDY 0	126
	RESRDY 1	127
I2S - Inter-IC Sound Interface	RXOR 0	128
	RXOR 1	
	RXRDY 0	
	RXRDY 1	
	TXRDY 0	
	TXRDY 1	
	TXUR 0	
	TXUR 1	
PCC - Parallel Capture Controller	PCC	129
AES - Advanced Encryption Standard	ENCCMP	130
	GFMCMP	
TRNG - True Random Generator	IS0	131
ICM - Integrity Check Monitor	ICM	132
PUKCC - Public-Key Cryptography Controller	PUKCC	133
QSPI - Quad SPI interface	QSPI	134
SDHC0 - SD/MMC Host Controller 0	SDHC0	135
	TIMER	

Offset	Name	Bit Pos.								
0x1FE8	PID2	7:0	REVISION[3:0]				JEPU	JEPIDCH[2:0]		
		15:8								
		23:16								
		31:24								
0x1FEC	PID3	7:0	REVAND[3:0]				CUSMOD[3:0]			
		15:8								
		23:16								
		31:24								
0x1FF0	CID0	7:0	PREAMBLEB0[7:0]							
		15:8								
		23:16								
		31:24								
0x1FF4	CID1	7:0	CCLASS[3:0]				PREAMBLE[3:0]			
		15:8								
		23:16								
		31:24								
0x1FF8	CID2	7:0	PREAMBLEB2[7:0]							
		15:8								
		23:16								
		31:24								
0x1FFC	CID3	7:0	PREAMBLEB3[7:0]							
		15:8								
		23:16								
		31:24								

12.13 Register Description

Registers can be 8, 16, or 32 bits wide. Atomic 8-, 16- and 32-bit accesses are supported. In addition, the 8-bit quarters and 16-bit halves of a 32-bit register, and the 8-bit halves of a 16-bit register can be accessed directly.

Some registers are optionally write-protected by the Peripheral Access Controller (PAC). Optional PAC write-protection is denoted by the "PAC Write-Protection" property in each individual register description. For details, refer to 12.5.7 Register Access Protection.

This flag is set on a zero-to-one transition of the BOD12 Synchronization Ready bit in the Status register (STATUS.B12SRDY) and will generate an interrupt request if INTENSET.B12SRDY=1.

Writing a '0' to this bit has no effect.

Writing a '1' to this bit clears the BOD12 Synchronization Ready interrupt flag.

Bit 4 – BOD12DET BOD12 Detection
This flag is cleared by writing a '1' to it.

This flag is set on a zero-to-one transition of the BOD12 Detection bit in the Status register (STATUS.BOD12DET) and will generate an interrupt request if INTENSET.BOD12DET=1.

Writing a '0' to this bit has no effect.

Writing a '1' to this bit clears the BOD12 Detection interrupt flag.

Bit 3 – BOD12RDY BOD12 Ready
This flag is cleared by writing a '1' to it.

This flag is set on a zero-to-one transition of the BOD12 Ready bit in the Status register (STATUS.BOD12RDY) and will generate an interrupt request if INTENSET.BOD12RDY=1.

Writing a '0' to this bit has no effect.

Writing a '1' to this bit clears the BOD12 Ready interrupt flag.

The BOD12 can be enabled at startup from Flash User Row.

Bit 2 – B33SRDY BOD33 Synchronization Ready
This flag is cleared by writing a '1' to it.

This flag is set on a zero-to-one transition of the BOD33 Synchronization Ready bit in the Status register (STATUS.B33SRDY) and will generate an interrupt request if INTENSET.B33SRDY=1.

Writing a '0' to this bit has no effect.

Writing a '1' to this bit clears the BOD33 Synchronization Ready interrupt flag.

Bit 1 – BOD33DET BOD33 Detection
This flag is cleared by writing a '1' to it.

This flag is set on a zero-to-one transition of the BOD33 Detection bit in the Status register (STATUS.BOD33DET) and will generate an interrupt request if INTENSET.BOD33DET=1.

Writing a '0' to this bit has no effect.

Writing a '1' to this bit clears the BOD33 Detection interrupt flag.

Bit 0 – BOD33RDY BOD33 Ready
This flag is cleared by writing a '1' to it.

This flag is set on a zero-to-one transition of the BOD33 Ready bit in the Status register (STATUS.BOD33RDY) and will generate an interrupt request if INTENSET.BOD33RDY=1.

Writing a '0' to this bit has no effect.

Writing a '1' to this bit clears the BOD33 Ready interrupt flag.

The BOD33 can be enabled.

Cleared on read.

Bit 6 – TFC Transmit Frame Corruption Due to AHB Error
Transmit frame corruption due to AHB error. Set if an error occurs during reading a transmit frame from the AHB, including HRESP errors and buffers exhausted mid frame.

Bit 5 – RLEX Retry Limit Exceeded
Retry Limit Exceeded Transmit error.

Cleared on read.

Bit 4 – TUR Transmit Underrun
This interrupt is set if the transmitter was forced to terminate an ongoing frame transmission due to further data being unavailable.

This interrupt is also set if a transmitter status write back has not completed when another status write back is attempted.

This interrupt is also set when the transmit DMA has written the SOP data into the FIFO and either the AHB bus was not granted in time for further data, or because an AHB not OK response was returned, or because the used bit was read.

Bit 3 – TXUBR TX Used Bit Read
Set when a transmit buffer descriptor is read with its used bit set.

Cleared on read.

Bit 2 – RXUBR RX Used Bit Read
Set when a receive buffer descriptor is read with its used bit set.

Cleared on read.

Bit 1 – RCOMP Receive Complete
A frame has been stored in memory.

Cleared on read.

Bit 0 – MFS Management Frame Sent
The PHY Maintenance Register has completed its operation.

Cleared on read.

25. NVMCTRL – Nonvolatile Memory Controller

25.1 Overview

Non-volatile memory (NVM) is a reprogrammable flash memory that retains program and data storage, even when powered off. The NVM Controller (NVMCTRL) embeds two banks; one bank can be read while the other is programmed (RWW). It is connected to the AHB and APB bus interfaces for system access to the NVM block. The AHB interfaces are used for reads and writes to the NVM block, while the APB interface is used for commands and configuration.

25.2 Features

- Two 32-bit AHB interfaces for reads and writes in the NVM main address space
- SmartEEPROM (integrated EEPROM emulation algorithm)
- Read while write (Any bank can be read while programming the other one)
- All NVM sections are memory mapped to the AHB, including calibration and system configuration
- 32-bit APB interface for commands and control
- Programmable wait states for read optimization
- 32 regions can be individually protected or unprotected
- Additional protection for boot loader
- Supports device protection through a security bit
- Interface to Power Manager to power-down flash blocks while in sleep modes
- Can optionally wake up on exit from sleep or on first access
- Single line cache per AHB interface
- Dual bank for safer application upgrade
- Error Correction Code (ECC)

26.6.2 ICM Hash Area

The ICM Hash Area is a contiguous area of system memory that the controller and the processor can access. The physical location is configured in the ICM hash area start address register. This address is a multiple of 128 bytes. If the CDWBN bit of the context register is cleared (i.e., Write Back activated), the ICM controller performs a digest write operation at the following starting location: *(HASH) + (RID<<5), where RID is the current region context identifier. If the CDWBN bit of the context register is set (i.e., Digest Comparison activated), the ICM controller performs a digest read operation at the same address.

26.6.2.1 Message Digest Example

Considering the following 512 bits message (example given in FIPS 180-4):

“61626380000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000018”

The message is written to memory in a Little Endian (LE) system architecture.

Memory Address	Address Offset / Byte Lane			
	0x3 / 31:24	0x2 / 23:16	0x1 / 15:8	0x0 / 7:0
0x000	80	63	62	61
0x004–0x038	00	00	00	00
0x03C	18	00	00	00

The digest is stored at the memory location pointed at by the ICM_HASH pointer with a Region Offset.

Memory Address	Address Offset / Byte Lane			
	0x3 / 31:24	0x2 / 23:16	0x1 / 15:8	0x0 / 7:0
0x000	36	3e	99	a9
0x004	6a	81	06	47
0x008	71	25	3e	ba
0x00C	6c	c2	50	78
0x010	9d	d8	d0	9c

Memory Address	Address Offset / Byte Lane			
	0x3 / 31:24	0x2 / 23:16	0x1 / 15:8	0x0 / 7:0
0x000	22	7d	09	23
0x004	22	d8	05	34
0x008	77	a4	42	86
0x00C	b3	55	a2	bd
0x010	e4	bc	ad	2a
0x014	f7	b3	a0	bd
0x018	a7	9d	6c	e3

Writing a '1' to these bits will clear the SERCOM6 interrupt flag.

Bit 1 – SERCOM5 Interrupt Flag for SERCOM5
This flag is set when a Peripheral Access Error occurs while accessing the SERCOM5, and will generate an interrupt request if INTENCLR/SET.ERR is '1'.

Writing a '0' to these bits has no effect.

Writing a '1' to these bits will clear the SERCOM5 interrupt flag.

Bit 0 – SERCOM4 Interrupt Flag for SERCOM4
This flag is set when a Peripheral Access Error occurs while accessing the SERCOM4, and will generate an interrupt request if INTENCLR/SET.ERR is '1'.

Writing a '0' to these bits has no effect.

Writing a '1' to these bits will clear the SERCOM4 interrupt flag.

Value	Description
0x1F	Channel 30 selected
0x20	Channel 31 selected
other	Reserved

32.9.4 Data Direction Toggle

Name: DIRTGL
Offset: 0x0C
Reset: 0x00000000
Property: PAC Write-Protection

This register allows the user to toggle the direction of one or more I/O pins, without doing a read-modify-write operation. Changes in this register will also be reflected in the Data Direction (DIR), Data Direction Set (DIRSET) and Data Direction Clear (DIRCLR) registers.

Tip: The I/O pins are assembled in pin groups (”PORT groups”) with up to 32 pins. Group 0 consists of the PA pins, group 1 is for the PB pins, etc. Each pin group has its own PORT registers, with a 0x80 address spacing. For example, the register address offset for the Data Direction (DIR) register for group 0 (PA00 to PA31) is 0x00, and the register address offset for the DIR register for group 1 (PB00 to PB31) is 0x80.

Bit	31	30	29	28	27	26	25	24
	DIRTGL[31:24]							
Access	RW	RW	RW	RW	RW	RW	RW	RW
Reset	0	0	0	0	0	0	0	0

Bit	23	22	21	20	19	18	17	16
	DIRTGL[23:16]							
Access	RW	RW	RW	RW	RW	RW	RW	RW
Reset	0	0	0	0	0	0	0	0

Bit	15	14	13	12	11	10	9	8
	DIRTGL[15:8]							
Access	RW	RW	RW	RW	RW	RW	RW	RW
Reset	0	0	0	0	0	0	0	0

Bit	7	6	5	4	3	2	1	0
	DIRTGL[7:0]							
Access	RW	RW	RW	RW	RW	RW	RW	RW
Reset	0	0	0	0	0	0	0	0

Bits 31:0 – DIRTGL[31:0] Port Data Direction Toggle
Writing '0' to a bit has no effect.

Writing '1' to a bit will toggle the corresponding bit in the DIR register, which reverses the direction of the I/O pin.

Value	Description
0	The corresponding I/O pin in the PORT group will keep its configuration.
1	The direction of the corresponding I/O pin is toggled.

37. QSPI - Quad Serial Peripheral Interface

37.1 Overview

The Quad SPI Interface (QSPI) circuit is a synchronous serial data link that provides communication with external devices in Master mode.

The QSPI can be used in “SPI mode” to interface serial peripherals, such as ADCs, DACs, LCD controllers and sensors, or in “Serial Memory Mode” to interface serial Flash memories.

The QSPI allows the system to execute code directly from a serial Flash memory (XIP) without code shadowing to SRAM. The serial Flash memory mapping is seen in the system as other memories (ROM, SRAM, DRAM, embedded Flash memories, etc.,).

With the support of the quad-SPI protocol, the QSPI allows the system to use high performance serial Flash memories which are small and inexpensive, in place of larger and more expensive parallel Flash memories.

37.2 Features

- Master SPI Interface:
  - Programmable Clock Phase and Clock Polarity
  - Programmable transfer delays between consecutive transfers, between clock and data, between deactivation and activation of chip select (CS)
- SPI Mode:
  - To use serial peripherals, such as ADCs, DACs, LCD controllers, CAN controllers, and sensors
  - 8-bit, 16-bit, or 32-bit programmable data length
- Serial Memory Mode:
  - To use serial Flash memories operating in single-bit SPI, Dual SPI and Quad SPI
  - Supports “execute in place” (XIP). The system can execute code directly from a Serial Flash memory.
  - Flexible Instruction register, to be compatible with all Serial Flash memories
  - 32-bit Address mode (default is 24-bit address) to support Serial Flash memories larger than 128 Mbit
  - Continuous Read mode
  - Scrambling/Unscrambling “On-the-Fly”
  - Double data rate support
- Connection to DMA Channel Capabilities Optimizes Data Transfers
  - One channel for the receiver and one channel for the transmitter
- Register Write Protection

38.8.4.2 Address of Data Buffer

Name: ADDR
Offset: 0x00 & 0x10
Reset: 0xxxxxxxx
Property: NA

Bit	31	30	29	28	27	26	25	24
	ADDR[31:24]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	x	x	x	x	x	x	x	x

Bit	23	22	21	20	19	18	17	16
	ADDR[23:16]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	x	x	x	x	x	x	x	x

Bit	15	14	13	12	11	10	9	8
	ADDR[15:8]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	x	x	x	x	x	x	x	x

Bit	7	6	5	4	3	2	1	0
	ADDR[7:0]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	x	x	x	x	x	x	x	x

Bits 31:0 – ADDR[31:0] Data Pointer Address Value
These bits define the data pointer address as an absolute word address in RAM. The two least significant bits must be zero to ensure the start address is 32-bit aligned.

Value	Description
0	No Message RAM Watchdog event occurred.
1	Message RAM Watchdog event due to missing READY.

Bit 25 – BO Bus_Off Status

Value	Description
0	Bus_Off status unchanged.
1	Bus_Off status changed.

Bit 24 – EW Error Warning Status

Value	Description
0	Error_Warning status unchanged.
1	Error_Warning status changed.

Bit 23 – EP Error Passive

Value	Description
0	Error_Passive status unchanged.
1	Error_Passive status changed.

Bit 22 – ELO Error Logging Overflow

Value	Description
0	CAN Error Logging Counter did not overflow.
1	Overflow of CAN Error Logging Counter occurred.

Bit 21 – BEU Bit Error Uncorrected
Message RAM bit error detected, uncorrected. Generated by an optional external parity / ECC logic attached to the Message RAM. An uncorrected Message RAM bit sets CCCR.INIT to 1. This is done to avoid transmission of corrupted data.

Value	Description
0	Not bit error detected when reading from Message RAM.
1	Bit error detected, uncorrected (e.g. parity logic).

Bit 20 – BEC Bit Error Corrected
Message RAM bit error detected and corrected. Generated by an optional external parity / ECC logic attached to the Message RAM.

Value	Description
0	Not bit error detected when reading from Message RAM.
1	Bit error detected and corrected (e.g. ECC).

Bit 19 – DRX Message stored to Dedicated Rx Buffer
The flag is set whenever a received message has been stored into a dedicated Rx Buffer.

Value	Description
0	No Rx Buffer updated.
1	At least one received message stored into a Rx Buffer.

42.8.11 Hash Key (GCM mode only)

Name: HASHKEY
Offset: 0x5C + n*0x04 [n=0..3]
Reset: 0x00000000
Property: PAC Write-protection

Bit	31	30	29	28	27	26	25	24
	HASHKEY[31:24]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bit	23	22	21	20	19	18	17	16
	HASHKEY[23:16]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bit	15	14	13	12	11	10	9	8
	HASHKEY[15:8]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bit	7	6	5	4	3	2	1	0
	HASHKEY[7:0]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bits 31:0 – HASHKEY[31:0] Hash Key Value
The four 32-bit HASHKEY registers contain the 128-bit Hash Key value computed from the AES KEY. The Hash Key value can also be programmed offering single GF128 multiplication possibilities.

```
    _PUKCL_SELFTEST   PUKCL_SelfTest;
    _PUKCL_SMULT      PUKCL_Smult;
    _PUKCL_SQUARE     PUKCL_Square;
    _PUKCL_SWAP       PUKCL_Swap;

    // ECC
    _PUKCL_ZPECCADD                    PUKCL_ZpEccAdd;
    _PUKCL_ZPECCDBL                    PUKCL_ZpEccDbl;
    _PUKCL_ZPECCADDSUB                 PUKCL_ZpEccAddSub;
    _PUKCL_ZPECCMUL                    PUKCL_ZpEccMul;
    _PUKCL_ZPECDSAGENERATE             PUKCL_ZpEcDsaGenerate;
    _PUKCL_ZPECDSAVERIFY               PUKCL_ZpEcDsaVerify;
    _PUKCL_ZPECDSAQUICKVERIFY          PUKCL_ZpEcDsaQuickVerify;
    _PUKCL_ZPECCQUICKDUALMUL           PUKCL_ZpEccQuickDualMul;
    _PUKCL_ZPECCONVPROJTOAFFINE        PUKCL_ZpEcConvProjToAffine;
    _PUKCL_ZPECCONVAFFINETOPROJECTIVE PUKCL_ZpEcConvAffineToProjective;
    _PUKCL_ZPECRANDOMIZECOORDINATE     PUKCL_ZpEcRandomiseCoordinate;
    _PUKCL_ZPECPOINTISONCURVE          PUKCL_ZpEcPointIsOnCurve;

    // ECC
    _PUKCL_GF2NECCADD                    PUKCL_GF2NEccAdd;
    _PUKCL_GF2NECCDBL                    PUKCL_GF2NEccDbl;
    _PUKCL_GF2NECCMUL                    PUKCL_GF2NEccMul;
    _PUKCL_GF2NECDSAGENERATE             PUKCL_GF2NEcDsaGenerate;
    _PUKCL_GF2NECDSAVERIFY               PUKCL_GF2NEcDsaVerify;
    _PUKCL_GF2NECCONVPROJTOAFFINE        PUKCL_GF2NEcConvProjToAffine;
    _PUKCL_GF2NECCONVAFFINETOPROJECTIVE PUKCL_GF2NEcConvAffineToProjective;
    _PUKCL_GF2NECRANDOMIZECOORDINATE     PUKCL_GF2NEcRandomiseCoordinate;
    _PUKCL_GF2NECPOINTISONCURVE          PUKCL_GF2NEcPointIsOnCurve;
    } P;
} PUKCL_PARAM,
```

43.3.3.2.1 PUKCL_HEADER Structure

The PUKCL_HEADER is common for all services of the library. This header includes standard fields to indicate the requested service, sub-service, options, return status, and so on, as shown in the following tables.

Different terms used in the below description to be understood, are as follows:

- Parameter – Represents a variable used by the PUKCL. Every parameter belongs to either PUKCL_HEADER or PUKCL Service Specific Header
- Type – Indicates the data type. For details on data type, please refer to `CryptoLib_typedef_pb.h` file in the library
- Dir – Direction. Indicates whether PUKCL considers the variable as input or output. Input means that the application passes data to the PUKCL using the variable. Output means that the PUKCL uses the variable to pass data to the application.
- Location – Suggests whether the parameter need to be stored in Crypto RAM or device SRAM. The PUKCL driver has macros for placing parameters into Crypto RAM, so that the user does not have to worry about the addresses
- Data Length – If a parameter is a pointer variable, the Data Length column shows the size of the data pointed by the pointer

Table 43-1. PUKCL_HEADER Structure

Parameter	Type	Direction	Location	Data Length	Before Executing the Service	After Executing the Service
u1Service	u1	I	–	–	Required service	Executed service
u1SubService	u1	I	–	–	Required sub-service	Executed sub-service
u2Option	u2	I	–	–	Required option	Executed option
Specific	PUKCL_STATUS	I/O	–	–	See Table 43-2	See Table 43-2

43.3.5.1.7 Modular Reductions Service Parameters Definition

Table 43-44. RedMod Service Parameters

Parameter	Type	Direction	Location	Data Length	Before Executing the Service	After Executing the Service
u2Options	u2	I	–	–	Options (see below)	Options (see below)
Specific/CarryIn	Bits	I	–	–	Must be set to zero.	–
Specific/Gf2n	Bit	I	–	–	GF(2^n) Bit	–
Specific/ CarryOut Zero Violation	Bits	I	–	–	–	Carry Out, Zero Bit and Violation Bit filled according to the result
nu1ModBase (see **Note 1**)	nu1	I	Crypto RAM	u2ModLength + 4	Base of N	Base of N untouched
nu1CnsBase	nu1	I	Crypto RAM	u2ModLength + 12	Base of Cns	Base of Cns filled with the Setup Constant
u2ModLength	u2	I	–	–	Length of N	Length of N
nu1RBase	nu1	I	Crypto RAM	GF(p): 64 bytes GF(2n): 68 bytes	Base of R as a workspace	Base of R workspace corrupted
nu1XBase (see **Note 2**)	nu1	I	Crypto RAM	2*u2ModLength + 8	Base of X as a workspace	Base of X workspace corrupted

Note:

1. The Modulus is to be given as a u2ModLength Aligned Significant Length Bytes however, it has to be provided as a u2ModLength + 4 bytes long number, having the four high-order bytes set to zero.
2. Before the X (pointed by {nu1XBase,2 * u2ModLength + 8}) LSB bytes, four supplementary bytes will be saved/restored. Other four supplementary bytes will also be saved/restored after the X MSB bytes. All these supplementary bytes may be entirely in the Crypto RAM (therefore, do not place the X area too near the end of the Crypto RAM) and shall not overlap with other area used by the service.

46.8.10 Window Control

Name: WINCTRL
Offset: 0x0A
Reset: 0x00
Property: PAC Write-Protection, Write-Synchronized

Bit	7	6	5	4	3	2	1	0
						WINTSEL0[1:0]		WEN0
Access						R/W	R/W	R/W
Reset						0	0	0

Bits 2:1 – WINTSEL0[1:0] Window 0 Interrupt Selection
These bits configure the interrupt mode for the comparator window 0 mode.

Value	Name	Description
0x0	ABOVE	Interrupt on signal above window
0x1	INSIDE	Interrupt on signal inside window
0x2	BELOW	Interrupt on signal below window
0x3	OUTSIDE	Interrupt on signal outside window

Bit 0 – WEN0 Window 0 Mode Enable

Value	Description
0	Window mode is disabled for comparators 0 and 1.
1	Window mode is enabled for comparators 0 and 1.

48.7.1.4 Event Control

Name: EVCTRL
Offset: 0x06
Reset: 0x0000
Property: PAC Write-Protection, Enable-Protected

Bit	15	14	13	12	11	10	9	8
			MCEO1	MCEO0				OVFEO
Access			R/W	R/W				R/W
Reset			0	0				0

Bit	7	6	5	4	3	2	1	0
			TCEI	TCINV		EVACT[2:0]		
Access			R/W	R/W		R/W	R/W	R/W
Reset			0	0		0	0	0

Bit 13 – MCEO1 Match or Capture Channel x Event Output Enable [x = 1..0]
These bits enable the generation of an event for every match or capture on channel x.

Value	Description
0	Match/Capture event on channel x is disabled and will not be generated.
1	Match/Capture event on channel x is enabled and will be generated for every compare/capture.

Bit 12 – MCEO0 Match or Capture Channel x Event Output Enable [x = 1..0]
These bits enable the generation of an event for every match or capture on channel x.

Value	Description
0	Match/Capture event on channel x is disabled and will not be generated.
1	Match/Capture event on channel x is enabled and will be generated for every compare/capture.

Bit 8 – OVFEO Overflow/Underflow Event Output Enable
This bit enables the Overflow/Underflow event. When enabled, an event will be generated when the counter overflows/underflows.

Value	Description
0	Overflow/Underflow event is disabled and will not be generated.
1	Overflow/Underflow event is enabled and will be generated for every counter overflow/underflow.

Bit 5 – TCEI TC Event Enable
This bit is used to enable asynchronous input events to the TC.

Value	Description
0	Incoming events are disabled.
1	Incoming events are enabled.

48.7.2.13 Counter Value, 16-bit Mode

Name: COUNT
Offset: 0x14
Reset: 0x00
Property: PAC Write-Protection, Write-Synchronized, Read-Synchronized

Note: Prior to any read access, this register must be synchronized by user by writing the according TC Command value to the Control B Set register (CTRLBSET.CMD=READSYNC).

Bit	15	14	13	12	11	10	9	8
	COUNT[15:8]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bit	7	6	5	4	3	2	1	0
	COUNT[7:0]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bits 15:0 – COUNT[15:0] Counter Value
These bits contain the current counter value.

Table 49-8. Fault n Capture Action

Value	Name	Description
0x0	DISABLE	Capture on valid recoverable Fault n is disabled
0x1	CAPT	On rising edge of a valid recoverable Fault n, capture counter value on channel selected by CHSEL[1:0]. INTFLAG.FAULTn flag rises on each new captured value.
0x2	CAPTMIN	On rising edge of a valid recoverable Fault n, capture counter value on channel selected by CHSEL[1:0], if COUNT value is lower than the last stored capture value (CC). INTFLAG.FAULTn flag rises on each local minimum detection.
0x3	CAPTMAX	On rising edge of a valid recoverable Fault n, capture counter value on channel selected by CHSEL[1:0], if COUNT value is higher than the last stored capture value (CC). INTFLAG.FAULTn flag rises on each local maximun detection.
0x4	LOCMIN	On rising edge of a valid recoverable Fault n, capture counter value on channel selected by CHSEL[1:0]. INTFLAG.FAULTn flag rises on each local minimum value detection.
0x5	LOCMAX	On rising edge of a valid recoverable Fault n, capture counter value on channel selected by CHSEL[1:0]. INTFLAG.FAULTn flag rises on each local maximun detection.
0x6	DERIV0	On rising edge of a valid recoverable Fault n, capture counter value on channel selected by CHSEL[1:0]. INTFLAG.FAULTn flag rises on each local maximun or minimum detection.

Bits 11:10 – CHSEL[1:0] Recoverable Fault n Capture Channel
These bits select the channel for capture operation triggered by recoverable Fault n.

Value	Name	Description
0x0	CC0	Capture value stored into CC0
0x1	CC1	Capture value stored into CC1
0x2	CC2	Capture value stored into CC2
0x3	CC3	Capture value stored into CC3

Bits 9:8 – HALT[1:0] Recoverable Fault n Halt Operation
These bits select the halt action for recoverable Fault n.

Value	Name	Description
0x0	DISABLE	Halt action disabled
0x1	HW	Hardware halt action