

#### 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 "<u>Embedded -</u> <u>Microcontrollers</u>"

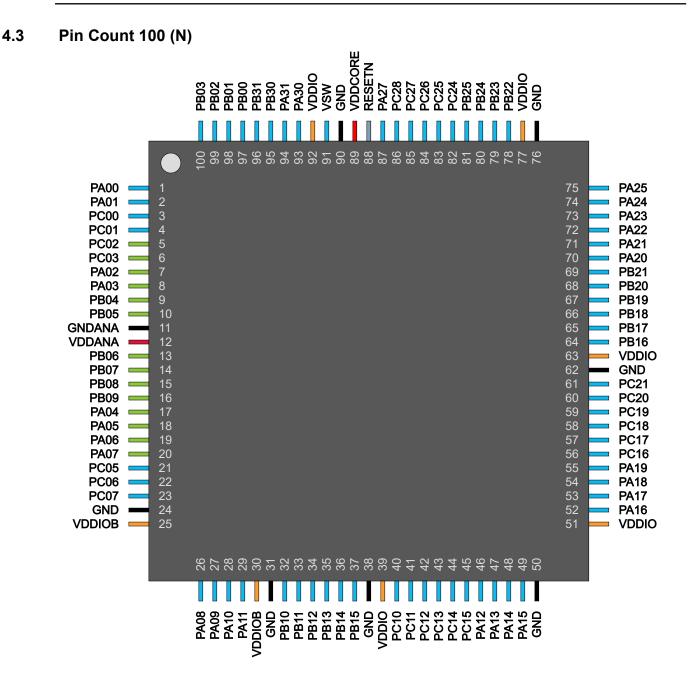
#### Details

E·XFI

Product Status	Active
Core Processor	ARM® Cortex®-M4F
Core Size	32-Bit Single-Core
Speed	120MHz
Connectivity	CANbus, EBI/EMI, Ethernet, I <sup>2</sup> C, IrDA, LINbus, MMC/SD, QSPI, SPI, UART/USART, USB
Peripherals	Brown-out Detect/Reset, DMA, I <sup>2</sup> S, POR, PWM, WDT
Number of I/O	81
Program Memory Size	512KB (512K x 8)
Program Memory Type	FLASH
EEPROM Size	
RAM Size	192K × 8
Voltage - Supply (Vcc/Vdd)	1.71V ~ 3.63V
Data Converters	A/D 28x12b; D/A 2x12b
Oscillator Type	Internal
Operating Temperature	-40°C ~ 85°C (TA)
Mounting Type	Surface Mount
Package / Case	100-TQFP
Supplier Device Package	100-TQFP (14x14)
Purchase URL	https://www.e-xfl.com/product-detail/microchip-technology/atsame54n19a-au

Email: info@E-XFL.COM

Address: Room A, 16/F, Full Win Commercial Centre, 573 Nathan Road, Mongkok, Hong Kong



Pinout

# 6. I/O Multiplexing and Considerations

# 6.1 Multiplexed Signals

Each pin is by default controlled by the PORT as a general purpose I/O and alternatively it can be assigned a different peripheral functions. To enable a peripheral function on a pin, the Peripheral Multiplexer Enable bit in the Pin Configuration register corresponding to that pin (PINCFGn.PMUXEN, n = 0-31) in the PORT must be written to '1'. The selection of peripheral function A to N is done by writing to the Peripheral Multiplexing Odd and Even bits in the Peripheral Multiplexing register (PMUXn.PMUXE/O) of the PORT.

This table describes the peripheral signals multiplexed to the PORT I/O pins.



**Important:** Not all signals are available on all devices. Refer to the Configuration Summary for available peripherals.

## Table 6-1. Multiplexed Peripheral Signals

8	5	8	TFBGA	58	Pad	A	в						С	D	E	F	G	н	1	J	к	L	М	N
QFN 48	TQFP/QFN/WLCSP 64	Тагр 100	120	TQFP 128	Name	EIC	ANARE F		ADC1	AC	DAC	PTC	SERCO M	SERCO M	тс	тсс	TCC, PDEC	QSPI, CAN1, USB, CORTE X_CM4	CANO	I <sup>2</sup> S	PCC	GMAC	GCLK, AC	CCL
48	64/C6	100	B2	128	PB03	EXTIN T[3]		ADC0/ AIN[15]	-	-	-	X21/Y2 1	-	SERCO M5/ PAD[1]	TC6/ WO[1]	-	-	-	-	-	-	-	-	-
1	01/B8	1	A1	1	PA00	EIC/ EXTIN T[0]	-	-	-	-	-		-	SERCO M1/ PAD[0]	TC2/ WO[0]	-	-	-	-	-	-	-	-	-
2	02/C8	2	B1	2	PA01	EIC/ EXTIN T[1]	-	-	-	-	-		-	SERCO M1/ PAD[1]	TC2/ WO[1]	-	-	-	-	-	-	-	-	-
		3	C1	3	PC00	EIC/ EXTIN T[0]	-	-	ADC1/ AIN[10]	-	-		-	-	-	-	-	-	-	-	-	-	-	-
		4	C2	4	PC01	EIC/ EXTIN T[1]	-	-	ADC1/ AIN[11]	-	-		-	-	-	-	-	-	-	-	-	-	-	-
		5	D1	7	PC02	EIC/ EXTIN T[2]	-	-	ADC1/ AIN[4]	-	-		-	-	-	-	-	-	-	-	-	-	-	-
		6	E2	8	PC03	EIC/ EXTIN T[3]	-	-	ADC1/ AIN[5]	-	-		-	-	-	-	-	-	-	-	-	-	-	-
3	03/C7	7	E1	9	PA02	EIC/ EXTIN T[2]		ADC0/ AIN[0]	-	-	DAC/ VOUT[ 0]		-	-	-	-	-	-	-	-	-	-	-	-
4	04/D6	8	F2	10	PA03	EXTIN	ANARE F/ VREFA	ADC0/ AIN[1]	-	-	-	X0/Y0	-	-	-	-	-	-	-	-	-	-	-	-
	05/D7	9	F1	11	PB04	EIC/ EXTIN T[4]	-	-	ADC1/ AIN[6]	-	-	X22/Y2 2	-	-	-	-	-	-	-	-	-	-	-	-
	06/D8	10	G1	12	PB05	EIC/ EXTIN T[5]	-	-	ADC1/ AIN[7]	-	-	X23/Y2 3	-	-	-	-	-	-	-	-	-	-	-	-
		-	G2	13	PD00	EIC/ EXTIN T[0]	-	-	ADC1/ AIN[14]	-	-		-	-	-	-	-	-	-	-	-	-	-	-
		-	H1	16	PD01	EIC/ EXTIN T[1]	-	-	ADC1/ AIN[15]	-	-		-	-	-	-	-	-	-	-	-	-	-	-
	09/E7	13	H2	17		EIC/ EXTIN T[6]	-	-	ADC1/ AIN[8]	-	-	X24/Y2 4	-	-	-	-	-	-	-	-	-	-	-	CCL/ IN[6]

**Processor and Architecture** 

SRAM Port Connection	Port ID	Connection Type	QoS	default QoS
SDHC0 - SD/MMC Host Controller	8	Direct	STATIC-1	0x1
SDHC1 - SD/MMC Host Controller	9	Direct	STATIC-1	0x1
CAN0 - Control Area Network	10	Direct	IP-MRCFG.QOS	0x1
CAN1 - Control Area Network	11	Direct	IP-MRCFG.QOS	0x1
GMAC - Ethernet MAC	12	Direct	STATIC-2	0x2
USB - Universal Serial Bus - Configuration Access	13	Direct	IP- QOSCTRL.CQOS	0x3
USB - Universal Serial Bus - Data Access	13	Direct	IP- QOSCTRL.DQOS	0x3

**Note:** 1. Using 32-bit access only.

# DSU - Device Service Unit

## 12.13.15 Peripheral Identification 7

	Name: Offset: Reset: Property:	PID7 0x1FDC 0x00000000 Read-Only						
Bit	31	30	29	28	27	26	25	24
Access								
Reset								
Bit	23	22	21	20	19	18	17	16
Access								
Reset								
Bit	15	14	13	12	11	10	9	8
Access								
Reset								
Bit	7	6	5	4	3	2	1	0
Access								
Reset								

# **DMAC – Direct Memory Access Controller**

### 22.8.6 Debug Control

Name:DBGCTRLOffset:0x0DReset:0x00Property:PAC Write-Protection

Bit	7	6	5	4	3	2	1	0
								DBGRUN
Access								R/W
Reset								0

#### Bit 0 – DBGRUN Debug Run

This bit is not reset by a software reset.

This bit controls the functionality when the CPU is halted by an external debugger.

Value	Description
0	The DMAC is halted when the CPU is halted by an external debugger.
1	The DMAC continues normal operation when the CPU is halted by an external debugger.

	Name: Offset: Reset: Property:	NSR 0x008 0x00000004 -						
Bit	31	30	29	28	27	26	25	24
Access								
Reset								
Bit	23	22	21	20	19	18	17	16
Access								
Reset								
Bit	15	14	13	12	11	10	9	8
BR			10	12				
Access								
Reset								
Bit	7	6	5	4	3	2	1	0
						IDLE	MDIO	
Access						R	R	
Reset						1	0	

### 24.9.3 GMAC Network Status Register

**Bit 2 – IDLE** PHY Management Logic Idle The PHY management logic is idle (i.e., has completed).

Bit 1 - MDIO MDIO Input Status

Returns status of the MDIO pin.

	Name: Offset: Reset: Property:	TPFCP 0x0C4 0x00000000 -						
Bit	31	30	29	28	27	26	25	24
Access								
Reset								
Bit	23	22	21	20	19	18	17	16
Access					I			
Reset								
Bit	15	14	13	12	11	10	9	8
				PQ	[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
Bit	7	6	5	4	3	2	1	0
					[7:0]			
Access		R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

#### 24.9.28 GMAC Transmit PFC Pause Register

### Bits 15:8 – PQ[7:0] Pause Quantum

When the Remove FCS bit in the GMAC Network Configuration register (NCFGR.RFCS) is written to '1', and one or more bits in this bit field are written to '0', the associated PFC pause frame's pause quantum field value is taken from the Transmit Pause Quantum register (TPQ).

For each entry equal to '1' in this bit field, the pause quantum associated with that entry will be zero.

#### Bits 7:0 - PEV[7:0] Priority Enable Vector

When the Remove FCS bit in the GMAC Network Configuration register (NCFGR.RFCS) is written to '1', the priority enable vector of the PFC priority-based pause frame is set to the value stored in this bit field.

### 24.9.97 GMAC PTP Peer Event Frame Received Seconds Low Register

Name:	PEFRSL
Offset:	0x1F8
Reset:	0x00000000
Property:	Read-Only

31	30	29	28	27	26	25	24		
			RUD[	31:24]					
R	R	R	R	R	R	R	R		
0	0	0	0	0	0	0	0		
23	22	21	20	19	18	17	16		
RUD[23:16]									
R	R	R	R	R	R	R	R		
0	0	0	0	0	0	0	0		
15	14	13	12	11	10	9	8		
			RUD	[15:8]					
R	R	R	R	R	R	R	R		
0	0	0	0	0	0	0	0		
7	6	5	4	3	2	1	0		
			RUE	[7:0]					
R	R	R	R	R	R	R	R		
0	0	0	0	0	0	0	0		
	R 0 23 R 0 15 R 0 7 R	R       R         0       0         23       22         R       R         0       0         115       14         R       R         0       0         7       6         R       R         R       R         R       R         R       R         R       R         R       R	R       R       R         0       0       0         23       22       21         R       R       R         0       0       0         15       14       13         R       R       R         0       0       0         7       6       5         R       R       R         R       R       R	R       R       R       R         0       0       0       0       0         23       22       21       20       RUD[         23       22       21       20       RUD[         R       R       R       R       0       0         15       14       13       12       RUD[         R       R       R       R       0       0         7       6       5       4       RUD[         R       R       R       R       RUD[         R       R       R       R       R         0       0       0       0       0         7       6       5       4       RUD[         R       R       R       R       RUD[         7       7       7       7       7       7         8       8       8       8       8       10	$\begin{array}{c c c c c c c c } RUD[31:24] \\ \hline R & R & R & R & R \\ \hline 0 & 0 & 0 & 0 & 0 \\ \hline 23 & 22 & 21 & 20 & 19 \\ \hline RUD[23:16] \\ \hline R & R & R & R & R \\ \hline 0 & 0 & 0 & 0 & 0 \\ \hline 15 & 14 & 13 & 12 & 11 \\ \hline RUD[15:8] \\ \hline R & R & R & R & R \\ \hline 0 & 0 & 0 & 0 & 0 \\ \hline 7 & 6 & 5 & 4 & 3 \\ \hline RUD[7:0] \\ \hline R & R & R & R & R \\ \hline \end{array}$	$\begin{array}{c c c c c c c c c } RUD[31:24] \\ \hline R & R & R & R & R \\ \hline 0 & 0 & 0 & 0 & 0 \\ \hline 23 & 22 & 21 & 20 & 19 & 18 \\ \hline 22 & 21 & 20 & 19 & 18 \\ \hline R & R & R & R & R \\ \hline 0 & 0 & 0 & 0 & 0 \\ \hline 15 & 14 & 13 & 12 & 11 & 10 \\ \hline 15 & 14 & 13 & 12 & 11 & 10 \\ \hline 15 & 14 & 13 & 12 & 11 & 10 \\ \hline R & R & R & R & R \\ \hline 0 & 0 & 0 & 0 & 0 \\ \hline \hline 7 & 6 & 5 & 4 & 3 & 2 \\ \hline R & R & R & R & R \\ \hline R & R & R & R & R \\ \hline R & R & R & R & R \\ \hline \end{array}$	$\begin{array}{c c c c c c c c c c c c c c c c c c c $		

### Bits 31:0 - RUD[31:0] Register Update

The register is updated with the value that the IEEE 1588 Timer Seconds Register holds when the SFD of a PTP receive primary event crosses the MII interface. An interrupt is issued when the register is updated.

### Bit 6 – NVME NVM Error

0: No NVM errors have been received since the last clear.

1: At least one NVM error has occurred since the last clear.

This bit can be cleared by writing a one to its bit location.

### Bit 5 – ECCDE ECC Dual Error

0: No ECC dual errors have been received since the last ECCERR register read.

1: At least one ECC error has occurred since the last ECCERR register read.

This bit is cleared when the ECCERR register is read.

#### Bit 4 – ECCSE ECC Single Error

0: No ECC single errors have been received since the last ECCERR register read.

1: At least one ECC error has occurred since the last ECCERR register read.

This bit is cleared when the ECCERR register is read.

#### Bit 3 – LOCKE Lock Error

0: No LOCK errors have been received since the last clear.

1: At least one LOCK error has occurred since the last clear.

This bit can be cleared by writing a one to its bit location.

#### Bit 2 – PROGE Programming Error

0: No PROG errors have been received since the last clear.

1: At least one PROG error has occurred since the last clear.

This bit can be cleared by writing a one to its bit location.

#### Bit 1 – ADDRE Address Error

0: No ADDRE error has been detected since the last clear.

1: At least one ADDRE error has been detected since the last clear.

This bit can be cleared by writing a one to its bit location.

#### Bit 0 – DONE Command Done

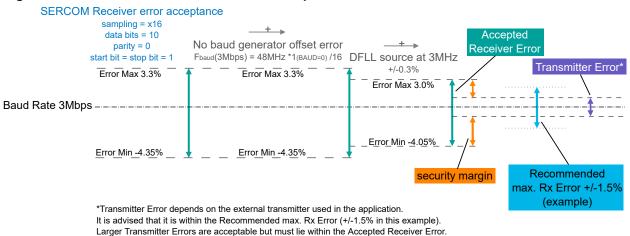
0: The NVM controller has not completed any command since the last clear.

1: At least one command has completed since the last clear.

This bit can be cleared by writing a one to its bit location.

# SAMD5x/E5x Family Data Sheet SERCOM USART - SERCOM Synchronous and Asyn...

### Figure 34-6. USART Rx Error Calculation Example



#### **Related Links**

33.6.2.3 Clock Generation – Baud-Rate Generator33.6.2.3.1 Asynchronous Arithmetic Mode BAUD Value Selection

#### 34.6.3 Additional Features

#### 34.6.3.1 Parity

Even or odd parity can be selected for error checking by writing 0x1 to the Frame Format bit field in the Control A register (CTRLA.FORM).

If *even parity* is selected (CTRLB.PMODE=0), the parity bit of an outgoing frame is '1' if the data contains an odd number of bits that are '1', making the total number of '1' even.

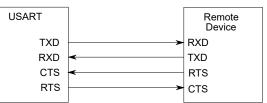
If *odd parity* is selected (CTRLB.PMODE=1), the parity bit of an outgoing frame is '1' if the data contains an even number of bits that are '0', making the total number of '1' odd.

When parity checking is enabled, the parity checker calculates the parity of the data bits in incoming frames and compares the result with the parity bit of the corresponding frame. If a parity error is detected, the Parity Error bit in the Status register (STATUS.PERR) is set.

#### 34.6.3.2 Hardware Handshaking

The USART features an out-of-band hardware handshaking flow control mechanism, implemented by connecting the RTS and CTS pins with the remote device, as shown in the figure below.

#### Figure 34-7. Connection with a Remote Device for Hardware Handshaking

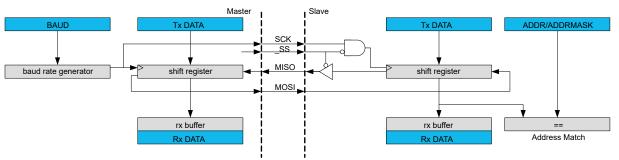


Hardware handshaking is only available in the following configuration:

- USART with internal clock (CTRLA.MODE=1),
- Asynchronous mode (CTRLA.CMODE=0),
- and Flow control pinout (CTRLA.TXPO=2).

## 35.3 Block Diagram

Figure 35-1. Full-Duplex SPI Master Slave Interconnection



## 35.4 Signal Description

### Table 35-1. SERCOM SPI Signals

Signal Name	Туре	Description
PAD[3:0]	Digital I/O	General SERCOM pins

One signal can be mapped to one of several pins.

### **Related Links**

6. I/O Multiplexing and Considerations

## 35.5 **Product Dependencies**

In order to use this peripheral, other parts of the system must be configured correctly, as described below.

#### 35.5.1 I/O Lines

In order to use the SERCOM's I/O lines, the I/O pins must be configured using the IO Pin Controller (PORT).

When the SERCOM is configured for SPI operation, the SERCOM controls the direction and value of the I/O pins according to the table below. Both PORT control bits PINCFGn.PULLEN and PINCFGn.DRVSTR are still effective. If the receiver is disabled, the data input pin can be used for other purposes. In master mode, the slave select line ( $\overline{SS}$ ) is hardware controlled when the Master Slave Select Enable bit in the Control B register (CTRLB.MSSEN) is '1'.

5-2. SPI Pin Configuration
5-2. SPI Pin Configuration

Pin	Master SPI	Slave SPI
MOSI	Output	Input
MISO	Input	Output
SCK	Output	Input
SS	Output (CTRLB.MSSEN=1)	Input

# USB – Universal Serial Bus

PTOKEN[1:0] <u>(1)</u>	Description
0x0	SETUP(2)
0x1	IN
0x2	OUT
0x3	Reserved

1. PTOKEN field is ignored when PTYPE is configured as EXTENDED.

2. Available only when PTYPE is configured as CONTROL

Theses bits are cleared upon sending a USB reset.

Writing a one to this bit will clear the Transfer Fail interrupt Enable bit and disable the corresponding interrupt request.

Value	Description
0	The Transfer Fail interrupt is disabled.
1	The Transfer Fail interrupt is enabled and an interrupt request will be generated when the Transfer Fail interrupt Flag is set.

**Bit 0 – TRCPT** Transfer Complete Bank x interrupt Disable

Writing a zero to this bit has no effect.

Writing a one to this bit will clear the Transfer Complete interrupt Enable bit x and disable the corresponding interrupt request.

Value	Description
0	The Transfer Complete Bank x interrupt is disabled.
1	The Transfer Complete Bank x interrupt is enabled and an interrupt request will be
	generated when the Transfer Complete interrupt x Flag is set.

#### 39.8.14 Protocol Status

Name:	PSR
Offset:	0x44
Reset:	0x00000707
Property:	Read-only

### Note:

- 1. When a frame in CAN FD format has reached the data phase with BRS flag set, the next CAN event (error or valid frame) will be shown in FLEC instead of LEC. An error in a fixed stuff bit of a CAN FD CRC sequence will be shown as a Form Error, not Stuff Error.
- 2. The Bus\_Off recovery sequence (see CAN Specification Rev. 2.0 or ISO 11898-1) cannot be shortened by setting or resetting CCCR.INIT. If the device goes Bus\_Off, it will set CCCR.INIT of its own accord, stopping all bus activities. Once CCCR.INIT has been cleared by the CPU, the device will then wait for 129 occurrences of Bus Idle (129 \* 11 consecutive recessive bits) before resuming normal operation. At the end of the Bus\_Off recovery sequence, the Error Management Counters will be reset. During the waiting time after the resetting of CCCR.INIT, each time a sequence of 11 recessive bits has been monitored, a Bit0 Error code is written to PSR.LEC, enabling the CPU to readily check up whether the CAN bus is stuck at dominant or continuously disturbed and to monitor the Bus\_Off recovery sequence. ECR.REC is used to count these sequences.

Bit	31	30	29	28	27	26	25	24
Access								
Reset								
Bit	23	22	21	20	19	18	17	16
					TDCV[6:0]			
Access		R	R	R	R	R	R	R
Reset		0	0	0	0	0	0	0
Bit	15	14	13	12	11	10	9	8
		PXE	RFDF	RBRS	RESI		DLEC[2:0]	
Access		R	R	R	R	R	R	R
Reset		0	0	0	0	1	1	1
Bit	7	6	5	4	3	2	1	0
	BO	EW	EP	ACT	[1:0]		LEC[2:0]	
A						_	_	
Access	R	R	R	R	R	R	R	R

#### Bits 22:16 – TDCV[6:0] Transmitter Delay Compensation Value

Value	Description
0x00 -	Position of the secondary sample point, defined by the sum of the measured delay from
0x7F	CAN_TX to CAN_RX and TDCR.TDCO. The SSP position is, in the data phase, the number
	of mtq between the start of the transmitted bit and the secondary sample point. Valid values
	are 0 to 127 mtq.

#### 39.8.24 High Priority Message Status

Name:	HPMS
Offset:	0x94
Reset:	0x00000000
Property:	Read-only

This register is updated every time a Message ID filter element configured to generate a priority event matches. This can be used to monitor the status of incoming high priority messages and to enable fast access to these messages.

Bit	31	30	29	28	27	26	25	24
Access								
Reset								
Bit	23	22	21	20	19	18	17	16
Access		I	I	L		Į	ļ	ļ]
Reset								
Bit	15	14	13	12	11	10	9	8
	FLST				FIDX[6:0]			
Access	R	R	R	R	R	R	R	R
Reset	0	0	0	0	0	0	0	0
Bit	7	6	5	4	3	2	1	0
	MSI[1:0]				BIDX	([5:0]		
Access	L	_		R	R	R	R	R
A00033	R	R	R	R. R.	IN IN	IX IX	n n	n n
Reset	R 0	R 0	R 0	0	0	0	0	0

#### Bit 15 – FLST Filter List

Indicates the filter list of the matching filter element.

Value	Description
0	Standard Filter List.
1	Extended Filter List.

#### Bits 14:8 - FIDX[6:0] Filter Index

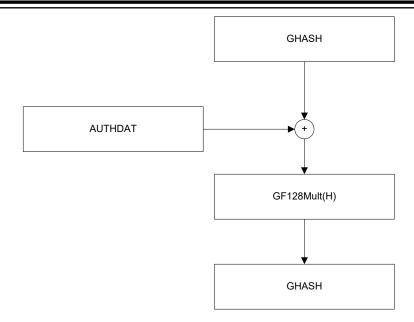
Index of matching filter element. Range is 0 to SIDFC.LSS - 1 (standard) or XIDFC.LSE - 1 (extended).

#### Bits 7:6 - MSI[1:0] Message Storage Indicator

This field defines the message storage information to a FIFO.

Value	Name	Description
0x0	NONE	No FIFO selected.
0x1	LOST	FIFO message lost.
0x2	FIFO0	Message stored in FIFO 0.
0x3	FIFO1	Message stored in FIFO 1.

AES – Advanced Encryption Standard



#### 42.6.3.1.3 Plain text Processing

- Set CTRLB.NEWMSG for the new set of plain text processing.
- Load CIPLEN reg.
- Load (J0+1) in INTVECT register.
- As described in NIST documentation J 0 = IV || 0 31 || 1 when len(IV)=96 and J0 =GHASH<sub>H</sub> (IV || 0 s+64 || [len(IV)] 64 ) (s is the minimum number of zeroes that should be padded with the Initialization Vector to make it a multiple of 128) if len(IV) != 96.
- Load plain text in DATA register.
- Set CTRLB.START as 1.
- Wait for INTFLAG.ENCCMP to be set.
- AES Hardware generates output in DATA register.
- Intermediate GHASH is stored in GHASH register and Cipher Text available in DATA register.
- Continue 3 to 6 till the input of plain text to get the cipher text and the Hash keys.
- At the last input, set CTRLB.EOM.
- Write last in-data to DATA reg.
- Set CTRLB.START as 1.
- Wait for INTFLAG.ENCCMP to be set.
- AES Hardware generates output in DATA register and final Hash key in GHASH register.
- Load [LEN(A)]64||[LEN(C)]64 in DATA register and set CTRLB.GFMUL and CTRLB.START as 1.
- Wait for INTFLAG.GFMCMP to be set.
- AES Hardware generates final GHASH value in GHASH register.

#### 42.6.3.1.4 Plain text processing with DMAC

- Set CTRLB.NEWMSG for the new set of plain text processing.
- Load CIPLEN reg.
- Load (J0+1) in INTVECT register.
- Load plain text in DATA register.
- Wait for INTFLAG.ENCCMP to be set.

# Public Key Cryptography Controller (PUKCC)

```
PUKCL _GF2NEccMul(nulModBase) = <Base of the ram location of P>;
       PUKCL
PUKCL _GF2NEccMul(nu1CnsBase) = <Base of the ram location of Cns>;
PUKCL _GF2NEccMul(nulPointBase) = <Base of the ram location of the A point>;
PUKCL _GF2NEccMul(nulABase) = <Base of the ram location of the parameters a and b of the
elliptic
curve>;
PUKCL _GF2NEccMul(nu1KBase) = <Base of the ram location of the scalar number>;
PUKCL _GF2NEccMul(nulWorkspace) = <Base of the ram location of the workspace>;
PUKCL
      GF2NEccMul(u2KLength) = <Length of the ram location of the scalar number>;
. . .
// vPUKCL Process() is a macro command, which populates the service name
// and then calls the library..
vPUKCL Process (GF2NEccMulFast, & PUKCLParam);
if (PUKCL (u2Status) == PUKCL OK)
            {
else // Manage the error
```

#### 43.3.7.4.6 Constraints

No overlapping between either input and output are allowed. The following conditions must be avoided to ensure the service works correctly:

- nu1ModBase, nu1CnsBase, nu1PointBase, nu1ABase, nu1KBase, nu1Workspace are not aligned on 32-bit boundaries
- {nu1ModBase, u2ModLength + 4}, {nu1CnsBase, u2ModLength + 8}, {nu1PointBase, 3\*u2ModLength+ 12}, {nu1ABase, 2\*u2ModLength + 8}, {nu1KBase, u2KLength} or {nu1Workspace, 8\*u2ModLength + 44} are not in Crypto RAM
- u2ModLength is either: < 12, > 0xffc or not a 32-bit length
- All overlapping between {nu1ModBase, u2ModLength + 4}, {nu1CnsBase, u2ModLength +8}, {nu1PointBase, 3\*u2ModLength + 12}, {nu1ABase, 2\*u2ModLength + 8}, {nu1KBase, u2KLength} and {nu1Workspace, 8\*u2ModLength + 44}

#### 43.3.7.4.7 Status Returned Values

#### Table 43-99. GF2NEccMulFast Service Return Codes

Returned Status	Importance	Meaning
PUKCL_OK	—	The computation passed without problem.

#### 43.3.7.5 Projective to Affine Coordinates Conversion

#### 43.3.7.5.1 Purpose

This service is used to perform a point coordinates conversion from a projective representation to an affine.

#### 43.3.7.5.2 How to Use the Service

#### 43.3.7.5.3 Description

The operation performed is:

$$Pt_{X \ Affine \ coordinate} = \left[\frac{Pt_{XProjective \ coordinate}}{(Pt_{Z \ Projective \ coordinate})}\right]$$
$$Pt_{Y \ Affine \ coordinate} = \left[\frac{Pt_{Y \ Projective \ coordinate}}{(Pt_{Z \ Projective \ coordinate})^2}\right]$$

In this computation, the following parameters need to be provided:

#### 48.7.3.4 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.

**I2S - Inter-IC Sound Controller** 

Offset	Name	Bit Pos.	
		15:8	DATA[15:8]
		23:16	DATA[23:16]
		31:24	DATA[31:24]
0x34	RXDATA	7:0	DATA[7:0]
		15:8	DATA[15:8]
		23:16	DATA[23:16]
		31:24	DATA[31:24]

# 51.9 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 require synchronization when read and/or written. Synchronization is denoted by the "Read-Synchronized" and/or "Write-Synchronized" property in each individual register description.

Some registers are enable-protected, meaning they can only be written when the module is disabled. Enable-protection is denoted by the "Enable-Protected" property in each individual register description.

Optional write-protection by the Peripheral Access Controller (PAC) is denoted by the "PAC Write-Protection" property in each individual register description.

# **Electrical Characteristics at 85°C**

The user must choose a crystal oscillator where the crystal load capacitance  $C_L$  is within the range given in the table. The exact value of  $C_L$  can be found in the crystal data sheet. The capacitance of the external capacitors ( $C_{LEXT}$ ) can then be computed as follows:

 $C_{\text{LEXT}} = 2(C_{\text{L}} - C_{\text{STRAY}} - _{\text{SHUNT}}),$ 

where  $C_{STRAY}$  is the capacitance of the pins and PCB,  $C_{SHUNT}$  is the shunt capacitance of the crystal.

Table 54-43. 32 kHz Crystal Oscillator Electrical Characteristics

Symbol	Parameter	Condition	s	Min.	Тур.	Max.	Units	
Fout <sup>(1)</sup>	Crystal oscillator frequency	-		-	32.768	-	kHz	
CL(1)	Crystal load capacitance	-		-	-	12.5	pF	
C <sub>SHUNT</sub> <sup>(1)</sup>	Crystal shunt capacitance	-		-	-	1.7	pF	
C <sub>M</sub> (1)	Motional capacitance	-		2	-	7	fF	
ESR	Crystal Equivalent Series Resistance -	f=32.768	Std. Gain	-	-	58	kΩ	
	SF=3	kHz, CL=12.5 pF	High Gain	-	-	90		
CXIN32k	Parasitic load capacitor	-		-	3.1	-	pF	
C <sub>XOUT32k</sub>				-	3.2	-		
<sup>t</sup> STARTUP	Startup time	f=32.768	Std. Gain	-	12	28	kCycles	
		kHz, CL=12.5 pF, CM=2.0 fF	High Gain	-	9	23		

#### Note:

1. These values are based on simulation. They are not covered by production test limits or characterization.

#### Table 54-44. Power Consumption

Symbol	Parameter	Condition s	Та	Gain Mode	Тур.	Max.	Units
I <sub>DD</sub>	Current	VDD=3.0V	Max 85°C	Std.	1.5	2	μΑ
	consumptio n		Typ 25°C	High	1.9	3	