MS6001

Summary Datasheet

SEAL SQ
semiconductors + quantum

Features

General

- Based on the ARM® SecurCore® SC300™ 32-bit RISC Processor featuring:
  - Harvard architecture
  - Thumb2® High-code-density Instruction Set
  - 3-stage pipeline architecture
  - 8-bit,16-bit,32-bit data access
  - Nested Vector Interrupt Controller
  - Memory Protection Unit
- On-chip Programmable System Clock up to 50MHz
- Very Low Power Consumption
  - GLow power Idle and Power down Modes
- ESD Protection：±4000V
- Operating range:
  - From 1.62V to 5.5V
  - From - 40°C to 105°C

Memory

- 1MBytes of FLASH Memory:
  - Pages of 128 bytes
  - 2 Kbytes of OTP
  - 500,000 Write/Erase Cycles at 25°C using Wear-Leveling
  - 10 Years Data Retention
  - Flash write & erase low power modes
- 64 Kbytes of ROM for Crypto Library, Wear-Leveling and Secure Bootloader code
- 24 Kbytes of RAM Memory (20 Kbytes of ARM CPU Core RAM, 4 Kbytes of Ad-X™3 RAM, shared with the ARM CPU Core)

Peripherals

- One ISO 7816 Controller
  - Up to 625 Kbps at 5MHz
  - Compliant with T=0 and T=1 Protocols
- High Speed SPI Interface up to 20Mbits/s
- I²C Interface up to 1Mbits/s
- 5 GPIOs (including IO0 and IO1)
- Three 16-bit Timers
- SysTick 24-bit timer, part of the SC300
- Interfaces and Class detectors
- Random Number Generator (RNG)
- Hardware DES/TDES DPA /DEMA Resistant
- Hardware AES
- CRC 16 & 32 Engine (Compliant with ISO/IEC 3309)
- 32-bit Cryptographic Accelerator (Ad-X3 for Public Key Operations)
  - RSA, DSA, ECC, ECDH
- High performance Hardware Java Card Accelerator

6631JS – 24Feb23

Security

- Dedicated Hardware for Protection Against SPA/DPA/SEMA/DEMA Attacks
- Advanced Protection Against Physical Attack, Including Active Shield, Enhanced Protection Object, Stack Checker, Slope Detector, Parity Errors
- Environmental Protection Systems
- Voltage Monitor
- Frequency Monitor
- Temperature Monitor
- Light Protection
- Secure Memory Management/Access Protection
- Memory Protection Unit, part of the SC300

Development Tools

- IAR Embedded Workbench® EWARM (1)
- Software Libraries and Application Notes

Certification Targeted

- AIS-31
- CC EAL5+
- FIPS 140-3

1. Licence not included - contact IAR

Description

The MS6001 architecture is based on the ARM® SecurCore® SC300 which offer high performance and very low power consumption. The core features a Thumb-2 instruction set, low interrupt latency, hardware divide, interruptible/continuable multiple load and store instructions, automatic state save and restore for interrupts, tighly integrated interrupt controller and multiple core buses capable of simultaneous accesses. Pipeline techniques are employed ensuring that all parts of the processing and memory systems can operate continously.

The SC300 instruction set provides the exceptional performance expected of a modern 32-bit architecture, with the high code density of 8-bit and 16-bit microcontrollers.The processor closely integrates a configurable nested vectored interrupt controller (NVIC), to deliver industry leading interrupt performance. To offer efficient low-power modes, the NVIC features a deep sleep function that enables the entire device to be rapidly powered down.

The MS6001 features a ROM memory dedicated to the storage of low level drivers, bootloader, Wear Leveling and cryptographic code. A large flash memory mapped in both data and code space provide a flexible way to store user data and program code.

The Ad-X3 hardware cryptographic accelerator featured in the MS6001 is dedicated to perform fast encryption or authentication functions.

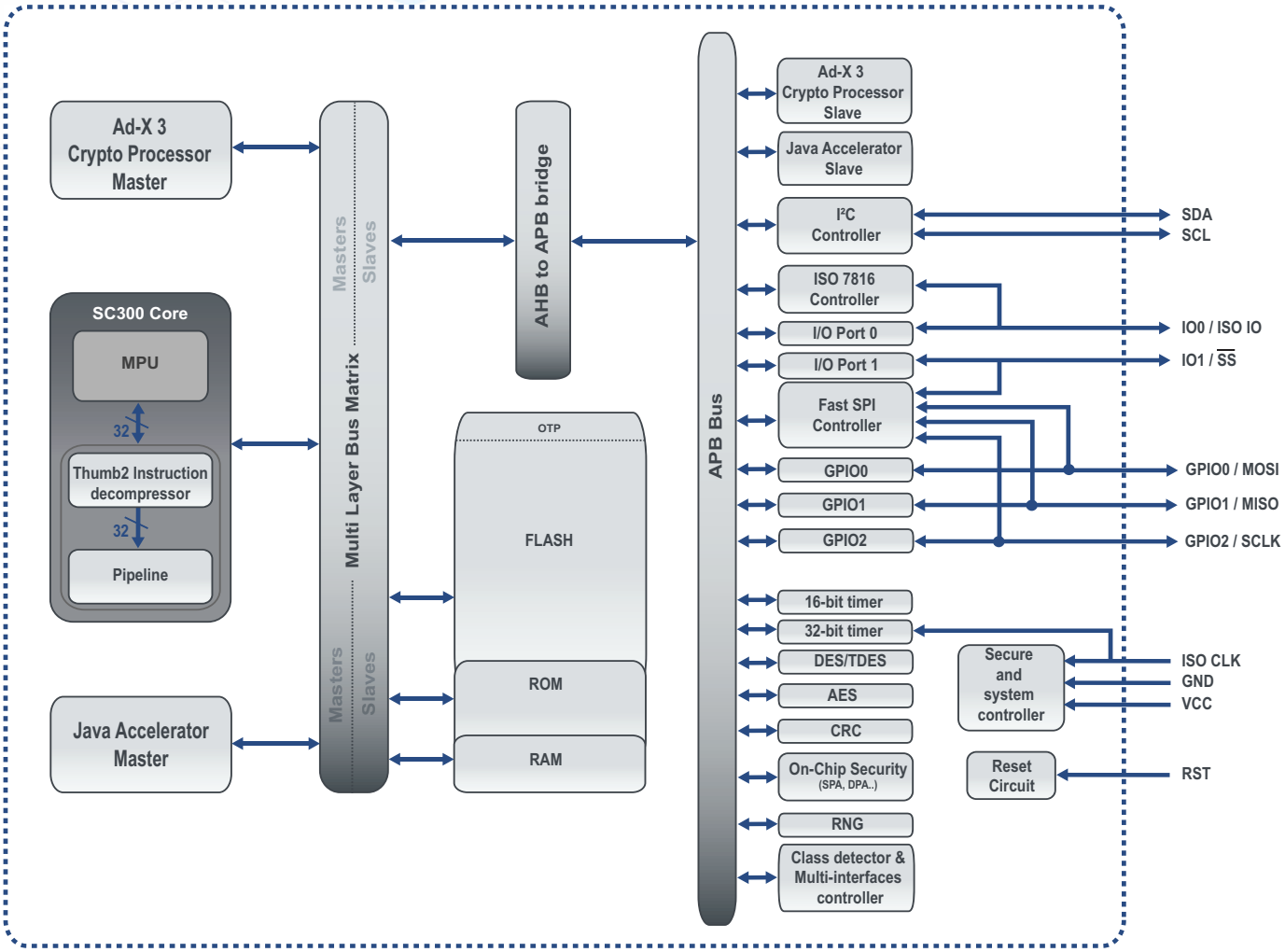
Thanks to the built-in MPU of the SC300, the MS6001 can enforce privilege rules, separate processes, enforce access rules over the entire 4GB addressing space.

Additional security features include fault injection resistance, hardware shield, scrambling of program, data and addresses, power analysis countermeasures and memory accesses controller by privileged modes.

Thanks to its dedicated set of peripherals, the MS6001 is an ideal product for application such as a Secure Element.

6631JS – 24Feb23

Figure 1 MS6001 ARM CPU Core Architecture



AC/DC Characteristics

Maximum Ratings

Parameter	Symbol	Min.	Max.	Unit
Supply Voltage	V_{CC}	-0.3	7	V
Operating Temperature	T_A	-40	+105	°C

AC/DC Characteristics (1.62V - 5.50V range; T= -40°C to +105°C)

Symbol	Parameter	Conditions	Min.	Typ.	Max.	Units
V_{CC}	Supply Voltage		1.62		5.5	V
F_{VFO}	Processor Clock Input Frequency	with Vcc=4.5V config 20MHz config 50MHz	 18 46	 20 50	 24 61	MHz
$F_{peripheral}$	Peripheral Clock Frequency	with Vcc=4.5V	18	22	24	MHz
V_{MAX}	Voltage Monitor: High Level Detection		6.1	6.3	6.4	V
V_{MIN}	Voltage Monitor: Low Level Detection		1.1	1.2	1.6	V
T_{MAX}	Temperature monitor High Level Detection			110		°C
T_{MIN}	Temperature monitor Low Level Detection			-40		°C
V_{POR}	Power-on Reset Voltage		1	1	1.45	V
t_{POR}	Power-on Reset Period	V_{CC}=5V V_{CC}rise time=10µs LowPowerStartup=0 LowPowerStartup=1		 112 226		µs
t_{TOUT}	Reset Delay Time-out Period	warm reset ISO400 fuse = 0		523		t_{CYC}
		warm reset ISO400 fuse = 1	the longest of 523 t_{CYC} or 7 t_{CYC}+ 403 t_{isoclk}			
		POR (cold reset) LowPowerStartup=0 LowPowerStartup=1		 980 2549		t_{CYC}
t_{FLASHW}	FLASH Write Time	per word	50	55	60	µs
t_{FLASHE}	FLASH Erase Time	per 2Kbytes sector	2	2+0.5	10	ms
t_{CYC}	CPU Cycle Time	LowPowerStartup=0 LowPowerStartup=1		$4.10^9/F_{VFO}$ $10^9/F_{VFO}$		ns
RST I_{IL}	Leakage Current RST	V_{IN}=0V		0		µA
RST I_{IH}	Leakage Current RST	V_{IN}=Vcc		0		µA
RST V_{IH}	Input High Voltage, RST signal		0.7xVcc	NA	Vcc+0.3	V
RST V_{IL}	Input Low Voltage, RST signal		-0.3	NA	0.2 x Vcc	V
CLK I_{IL}	Leakage Current CLK	V_{IN} = 0		0		µA
CLK I_{IH}	Leakage Current CLK	V_{IN} = Vcc		0		µA
CLK V_{IH}	Input High Voltage, CLK signal		0.7xVcc	NA	Vcc+0.3	V

Symbol	Parameter	Conditions	Min.	Typ.	Max.	Units
CLK V_{IL}	Input Low Voltage, CLK signal		-0.3	NA	0.2 x Vcc	V
I/O I_{IL}	Leakage Current I/O	V_{IN}=0		0		µA
I/O I_{IH}	Leakage Current I/O	V_{IN}=Vcc		0		µA
I/O V_{IH}	Input High Voltage, I/O signal		0.7xVcc	NA	Vcc+0.3	V
I/O V_{IL}	Input Low Voltage, I/O signal		-0.3	NA	0.2 x Vcc	V
I/O V_{OH}	Output High Voltage, I/O signal	I_{OH}=20µA R_{PULLUP}=20K	0.7 x Vcc			V
I/O V_{OL}	Output Low Voltage, I/O signal	I_{OL}<1mA, ClassA			0.08 x Vcc	V
I/O V_{OL}	Output Low Voltage, I/O signal	I_{OL}<0.5mA, ClassB			0.15 x Vcc	V
I/O V_{OL}	Output Low Voltage, I/O signal	I_{OL}<0.5mA, ClassC			0.15 x Vcc	V
Tr	I/O Output Rise Time	C_{out} = 30 pF, R_{PULLUP} = 220K	9.2	12.1	18.3	ns
Tf	I/O Output Fall Time	C_{out} = 30 pF	10.1	13.0	20.1	ns
$R_{I/O\ PULLUP}$	RST Pin Pullup IO0, IO1, GPIO0 to 2 Pin Pullup SCK Pin Pullup			220 220 220		kΩ
$R_{I/O\ PULLDOWN}$	RST Pin Pulldown IO0, IO1, GPIO0 to 2 Pin Pulldown SCK Pin Pulldown			1000 1000 1000		kΩ

Note: 1. In deep sleep Mode, the external clock can be stopped. The Frequency and temperature Monitors are switched off

6631JS – 24Feb23

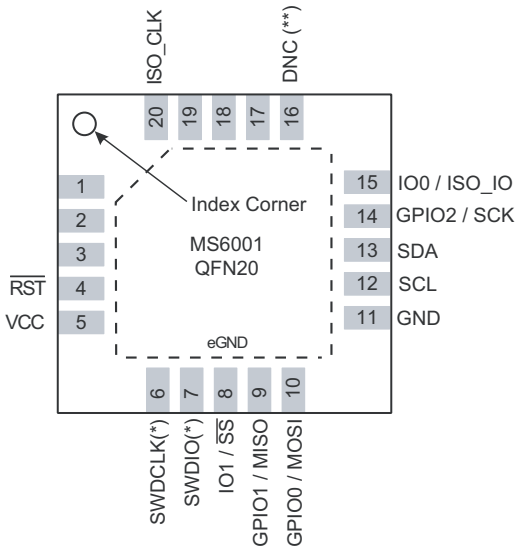
Typical power consumption.

Symbol	Parameter	Conditions	Min.	Typ.	Max.	Units
I_{PDN-T}	IDD total in Power down mode	config 20MHz 4.5V < VCC < 5.50V 2.7V < VCC < 4.5V 1.62V < VCC < 2.7V config 50MHz 4.5V < VCC < 5.50V 2.7V < VCC < 4.5V 1.62V < VCC < 2.7V		 97 86 80 121 105 98		µA
I_{RUN}	IDD when CPU runs	config 20MHz 4.5V < VCC < 5.50V 2.7V < VCC < 4.5V 1.62V < VCC < 2.7V config 50MHz 4.5V < VCC < 5.50V 2.7V < VCC < 4.5V 1.62V < VCC < 2.7V		 5.1 4.6 4.4 8.6 7.9 7.6		mA
I_{Ad-X3}	IDD when Ad-X3 runs	config 20MHz 4.5V < VCC < 5.50V 2.7V < VCC < 4.5V 1.62V < VCC < 2.7V config 50MHz 4.5V < VCC < 5.50V 2.7V < VCC < 4.5V 1.62V < VCC < 2.7V		 6.3 5.9 5.7 12 11.3 11.0		mA
I_{Worst}	IDD when all features run	config 20MHz 4.5V < VCC < 5.50V 2.7V < VCC < 4.5V 1.62V < VCC < 2.7V config 50MHz 4.5V < VCC < 5.50V 2.7V < VCC < 4.5V 1.62V < VCC < 2.7V		 8.8 8.3 8.1 17.9 17.2 16.8		mA

Pin and Packages Configurations

QFN20

GND	Ground, mandatory to connect it
eGND	Exposed pad unconnected internally, connect to ground recommended
VCC	Power supply input
IO1 / $\overline{SS}$	IO1 or SPI Slave Select
GPIO0 / MOSI	GPIO0 or SPI MOSI
GPIO1 / MISO	GPIO1 or SPI MISO
GPIO2 / SCK	GPIO2 or SPI clock
SDA	I2C SDA
SCL	I2C SCL
IO0 / ISO_IO	IO0 or ISO IO
ISO_CLK	ISO CLK ISO 7816 input clock
$\overline{RST}$	Reset
SWDCLK(*)	Single Wire Debug Clock
SWDIO(*)	Single Wire Debug IO



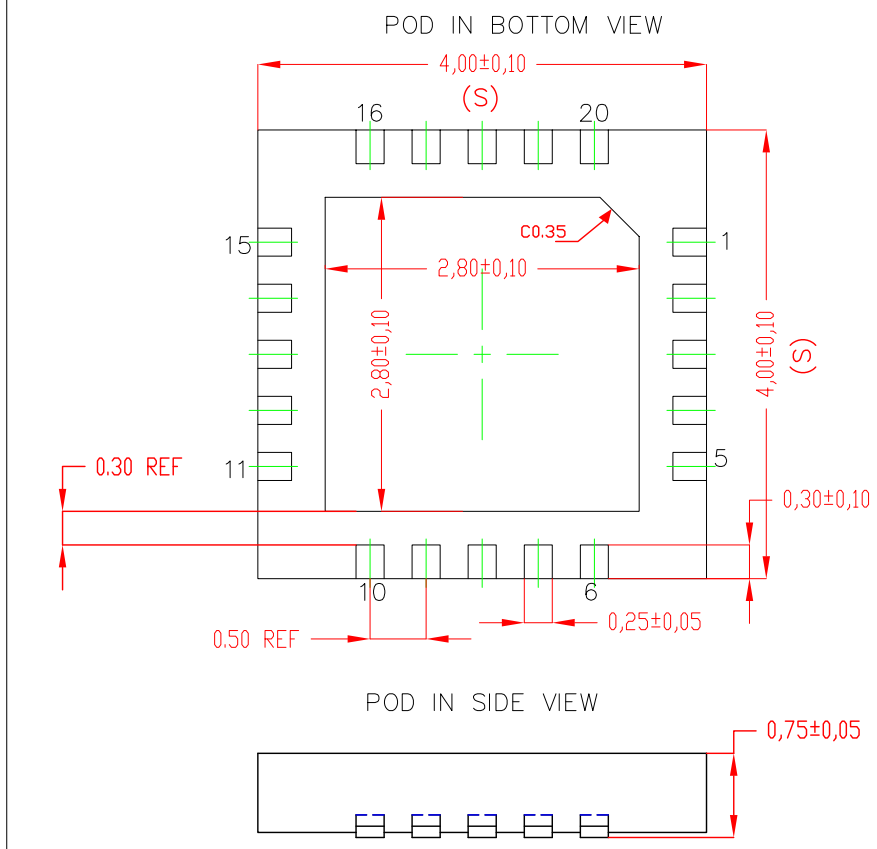
(*) only for engineering sample
(**) Do Not Connect

Configuration	Interfaces Available	Package
QFN20	**ISO (or 1 GPIO) + I2C + SPI (or 4 GPIO)**	QFN20 (4*4)

6631JS – 24Feb23

Package outline

PACKAGE OUTLINE DRAWING		
Package name	R-QFN020_G	
Package description	Quad Flat No Lead Package, 20 Leads, 4x4x0.75mm, Pitch 0.5mm	
Reference doc	POD_PPT_B13_401	Rev. 2.1
Date	Jun 01, 2015	



NOTES:

1. ALL DIMENSIONS ARE IN mm. ANGLES IN DEGREES
2. COPLANARITY APPLIES TO THE EXPOSED PAD AS WELL AS THE TERMINALS. COPLANARITY SHALL NOT EXCEED 0.08 mm.
3. WARPAGE SHALL NOT EXCEED 0.10 mm.
4. PACKAGE LENGTH/ PACKAGE WIDTH ARE CONSIDERED AS SPECIAL CHARACTERISTIC.(S)
5. REFER JEDEC MO-220.