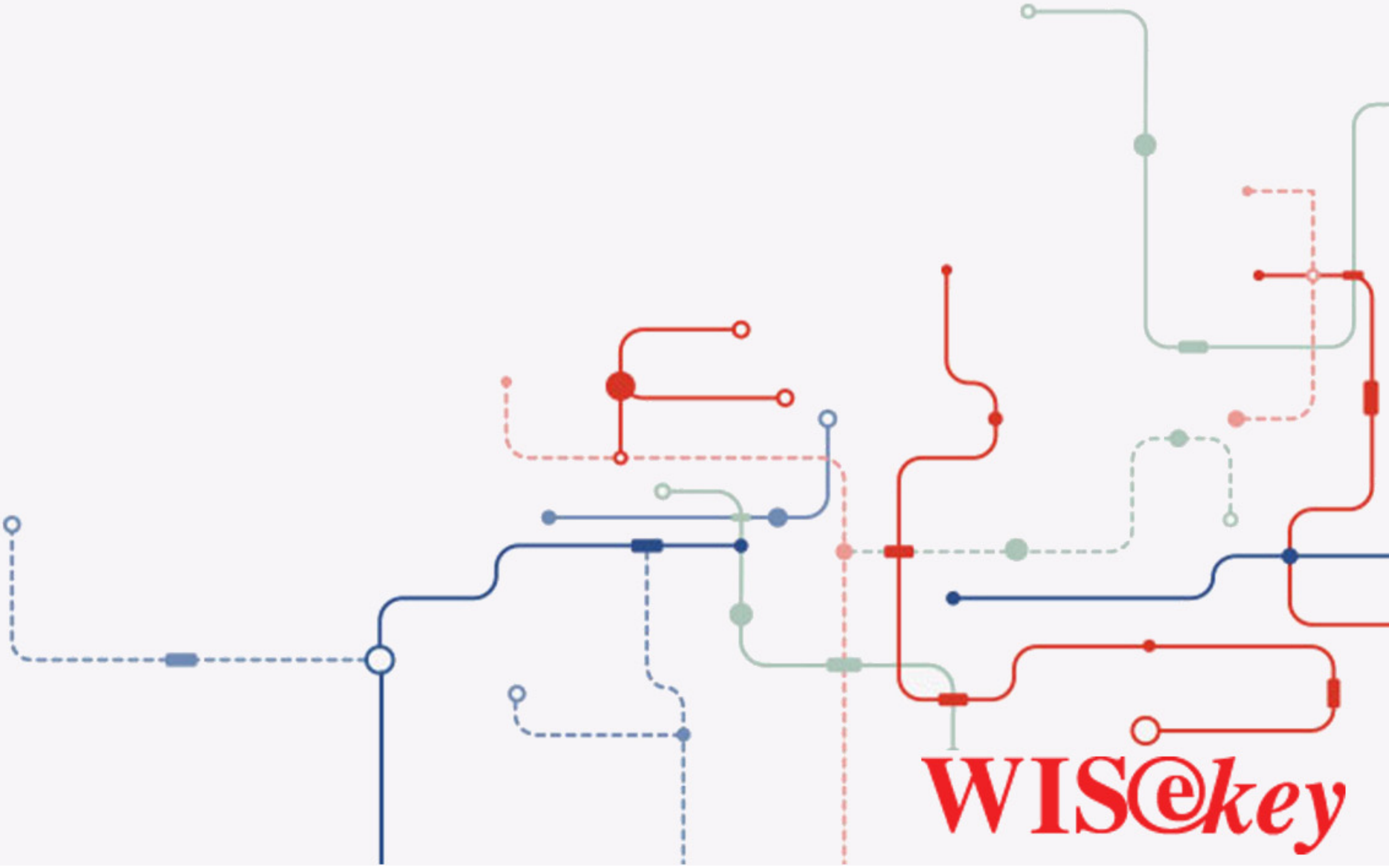
MS6003

Summary Datasheet



WISekey

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
- Low power modes
- Operating range:
  - From 2.70V to 5.5V
  - From -40°C to 105°C
- **8kV contact IEC 61000-4-2 ESD protection (USB)**
- Available in wafers,waffle packs and QFN20 4x4

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
- I^{2}C Interface up to 1Mbits/s
- USB 2.0 Full Speed Interface
  - 8 Programmable Endpoints with IN or OUT Directions for Bulk, Interrupt or Isochronous Transfers (4 end-points with double buffering of 64x2 bytes)
  - DMA Controller for fast transfers between internal DPRAM and RAM
  - Internally generated 48 MHz clock **(no need for an External Crystal)**
- 8 GPIOs (including IO0 and IO1)
- Hardware Communication Interface Detection
- One 32-bit timer and one 16-bit timer with wtachdog capability
- SysTick 24-bit timer, part of the SC300
- True Random Number Generator (RNG)
- Hardware DES/TDES
- Hardware AES 128/192/256
- 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
- Real Time Clock (RTC)
  - requires an external 32.768KHz crystal
  - VBAT : 2.4V to 3.6V
  - **Power consumption < 300nA (typical)**

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

- USB 2.0
- AIS-31
- CC EAL5+
- FIPS 140-3

[1] Licence not included - contact IAR

Description

The MS6003 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 MS6003 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 MS6003 is dedicated to perform fast encryption or authentication functions. Thanks to the built-in MPU of the SC300, the MS6003 can enforce privilege rules, separate processes, enforce access rules over the entire 4GB addressing space.

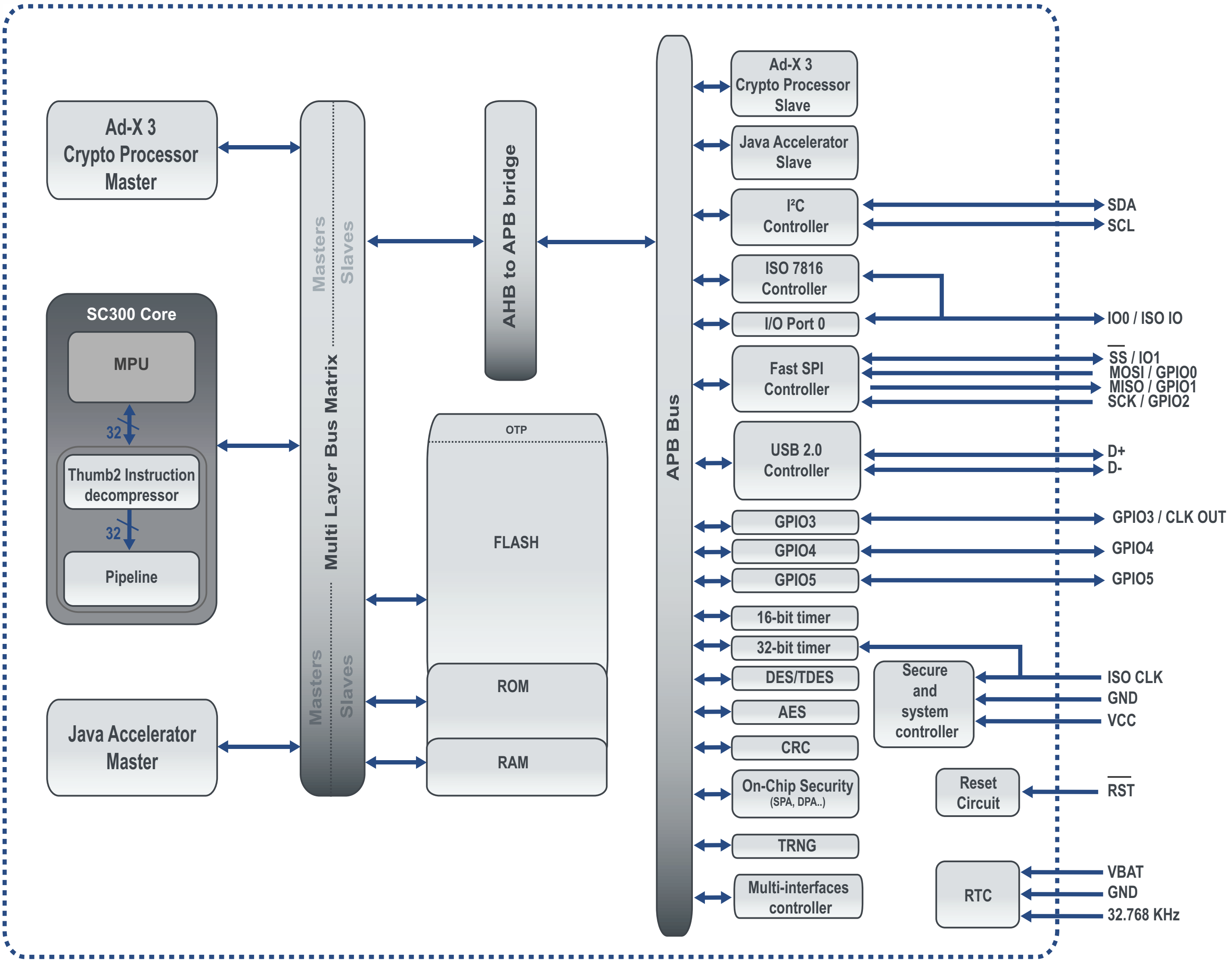
Additional security features include fault injection resistance, hardware shield, scrambling of program, data and addresses, power analysis countermeasures and memory accesses controller by privileged modes.

The USB V2.0 Full Speed controller provides a dynamic pull-up attachment/detachment and a host detection mechanism. Eight SW configurable data transfer endpoints are available, each with its own DPRAM. A DMA controller allows a fast transfer between the CPU RAM and the DPRAM banks. When configured as a master, the High Speed SPI, provides a clock up to 20MHz thanks to the dedicated internal VFO clock system. A specific DMA controller allows a fast transfer between the CPU RAM and the DPRAM banks. The internal DPRAM memory provides 4 DPRAM buffers of 16 bytes each. The SPI controller features three sources of interrupt (Byte Transmitted, Time-out and Reception Overflow), a programmable clock and interbyte (guardtime) delays. The I²C interface interconnects components on a unique two-wire bus, made up of one clock line and one data line with speeds of up to 1 Mbits per second, based on a byte-oriented transfer format. It is programmable as a master or a slave with sequential or single-byte access. Multiple master capability is supported. Arbitration of the bus is performed internally and puts the I²C in slave mode automatically if the bus arbitration is lost.

The built-in 8kV contact IEC 61000-4-2 ESD protection on USB pins, self-generated 48MHz and embedded RTC tremendously decrease the bill of material.

Thanks to its dedicated set of peripherals, the MS6003 is an ideal product for applications such as Strong Authentication USB Tokens and Embedded Systems.

Figure 1 MS6003 Core Architecture



AC/DC Characteristics - Preliminary

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 (2.7V - 5.5V range; T= -40°C to +105°C)

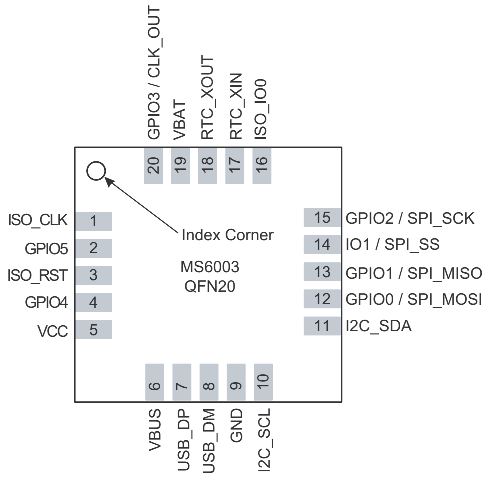
Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
V_{CC}	Supply Voltage		2.7		5.5	V
F_{VFO}	Processor Clock Input Frequency			50		MHz
$F_{peripheral}$	Peripheral Clock Frequency			25		MHz
V_{MAX}	Voltage Monitor: High Level Detection		6.1	6.3	6.5	V
V_{MIN}	Voltage Monitor: Low Level Detection		2.1	2.3	2.5	V
T_{MAX}	Temperature monitor High Level Detection		105			°C
T_{MIN}	Temperature monitor Low Level Detection				-40	°C
t_{FLASHW}	FLASH Write Time	per word	50	55	60	µs
t_{FLASHE}	FLASH Erase Time	erase+verify	2		10	ms
RST I_{IL}	Leakage Current RST	V_{IN}=0V (highZ)	-1		1	µA
RST I_{IH}	Leakage Current RST	V_{IN}=Vcc (highZ)	-1		1	µA
RST V_{IH}	Input High Voltage, RST signal		0.7xVcc		Vcc+0.3	V
RST V_{IL}	Input Low Voltage, RST signal		-0.3		0.2 x Vcc	V
CLK I_{IL}	Leakage Current CLK	V_{IN} = 0 (highZ)	-1		1	µA
CLK I_{IH}	Leakage Current CLK	V_{IN} = Vcc (highZ)	-1		1	µA
CLK V_{IH}	Input High Voltage, CLK signal		0.7xVcc		Vcc+0.3	V
CLK V_{IL}	Input Low Voltage, CLK signal		-0.3		0.2 x Vcc	V
I/O I_{IL}	Leakage Current, I/O signal	V_{IN}=0 (highZ)	-1		1	µA
I/O I_{IH}	Leakage Current, I/O signal	V_{IN}=Vcc (highZ)	-1		1	µA
I/O V_{IH}	Input High Voltage, I/O signal		0.7xVcc		Vcc+0.3	V
I/O V_{IL}	Input Low Voltage, I/O signal		-0.3		0.2 x Vcc	V
I/O V_{OH}	Output High Voltage, I/O signal	I_{OH}=20µA R_{PULLUP}=20K	0.97		1	x Vcc
I/O V_{OL}	Output Low Voltage, I/O signal	I_{OL}<1mA, ClassA	0		0.15	x Vcc

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
I/O V_{OL}	Output Low Voltage, I/O signal	I_{OL}<0.5mA, ClassB	0		0.15	x Vcc
I/O I_{OL}	Current output low, I/O signal	V_{OL} = 0.4V			8	mA
I/O I_{OH}	Current output high, I/O signal	V_{OH} = 0.7xVcc			8	mA
I/O Tr	Output Rise Time, I/O signal	C_{out} = 30 pF, R_{PULLUP} = 220K	9	12	19	ns
I/O Tf	Output Fall Time, I/O signal	C_{out} = 30 pF	10	13	21	ns
$R_{I/O\ PULLUP}$	RST Pin Pullup IO0, IO1, GPIO0 to GPIO5 Pin Pullup			220 220		kΩ
$R_{I/O}$ PULLDOWN	RST Pin Pulldown IO0, IO1, GPIO0 to GPIO5 Pin Pulldown			1000 1000		kΩ

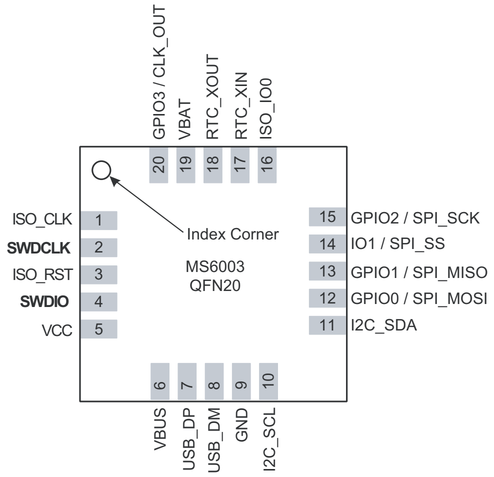
Pin and Packages Configurations

QFN20

GND	Ground (reference voltage)
V_{CC}	Power supply input
VBUS	USB Power supply input
ISO CLK	ISO CLK ISO 7816 input clock
ISO RST	ISO Reset signal input
ISO IO / I/O0	ISO IO or IO0
I/O1 / $\overline{SS}$	IO1 or SPI Slave Select
GPIO0 / MOSI	GPIO0 or SPI MOSI
GPIO1 / MISO	GPIO1 or SPI MISO
GPIO2 / SCLK	GPIO2 or SPI clock
GPIO3 / CLK_OUT	GPIO3 or USB clock Out
GPIO4	General Purpose Input Output
GPIO5	General Purpose Input Output
SDA	I2C SDA
SCL	I2C SCL
DP	USB D+ differential data
DM	USB D- differential data
VBAT	Power supply for RTC
RTC_XIN	Resonator signal input to generate RTC internal clock
RTC_XOUT	Resonator signal output to generate RTC internal clock



Volume configuration

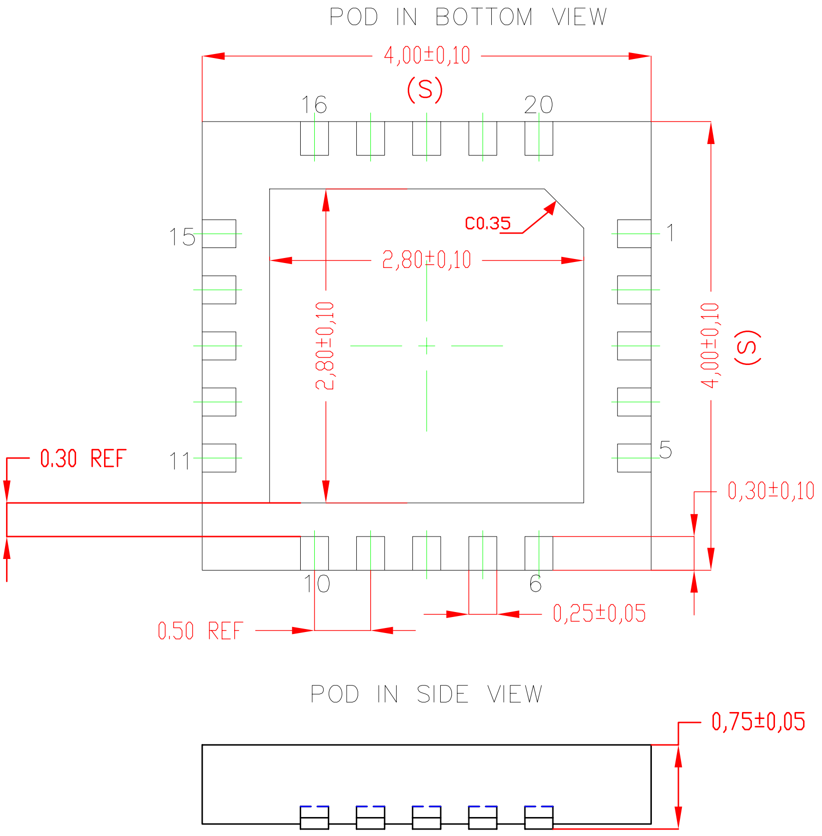


Engineering samples only

Configuration	Interfaces Available	Package
QFN20 volume	SPI (or 4 GPIO) + ISO (or 1 GPIO) + 3 GPIO + I2C + USB	QFN20 (4*4)
QFN20 engineering	SPI (or 4 GPIO) + ISO (or 1 GPIO) + 1 GPIO + debug interface + I2C + USB	QFN20 (4*4)

Package outline

PACKAGE OUTLINE DRAWING		
Package name	R-QFN020_J	
Package description	Quad Flat No Lead Package, 20 Leads, 4x4x0.75mm, Pitch 0.5mm	
Reference doc	POD_PPT_F15_702	Rev. 1.0
Date	Jun 16, 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.

The photographs and information contained in this document are not contractual and may be changed without notice. Brand and product names may be registered trademarks or trademarks of their respective holders.
Note: This is a summary document. A complete document will be available under NDA. For more information, please contact your local WiseKey sales office.