SE*cube*™ Data Sheet
Introduction

August 2015 | Data Sheet DUI 15082DS

General Description

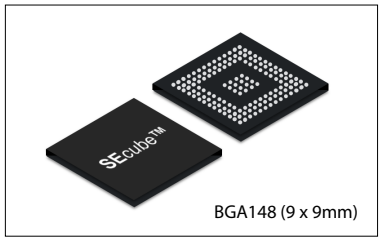
The SE*cube*™ (Secure Environment cube) is a powerful chip which integrates three key security elements in a single package. A fast floating-point Cortex-M4 CPU, a high-performance FPGA and an EAL5+ certified Security Controller (Smart Card).

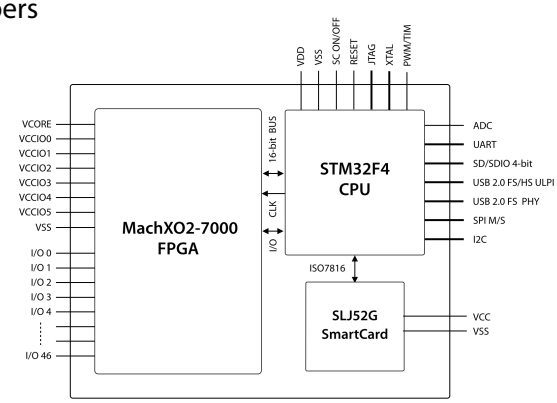
The result of this innovative combination gives an extremely versatile secure environment in a single SoC, in which developers can rapidly implement complex applications and appliances.

The SE*cube*™ chip has multiple embedded communication interfaces. In addition, the internal FPGA provides up to 47 fast I/O (100 MHz) for custom high-speed interface implementations.

This allows fast integration of the SE*cube*™ into any hardware design, while drastically reducing the final BOM.

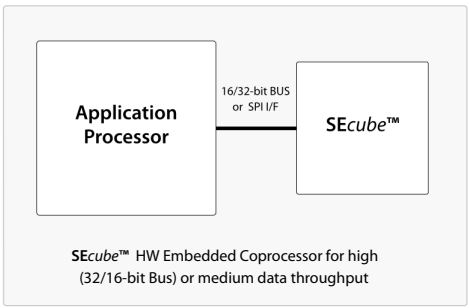
The SE*cube*™ is the ultimate solution for high-end design, delivering integration of a flexible, configurable and certified secure element.



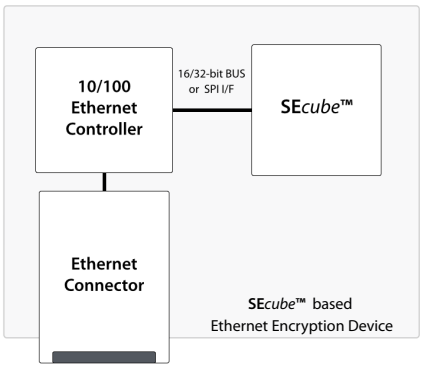


SE*cube*™ Block Diagram

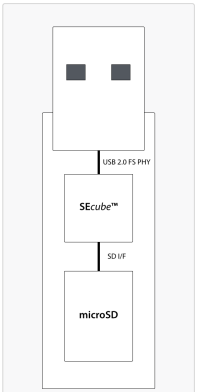
TYPICAL APPLICATION DIAGRAMS



SE*cube*™ HW Embedded Coprocessor for high (32/16-bit Bus) or medium data throughput



SE*cube*™ based Ethernet Encryption Device



SE*cube*™ based USB 2.0 Secure Token

SE*cube*™ Data Sheet Introduction

August 2015 Data Sheet DUI 15082DS

Main Features

Three powerful elements in one chip

■Embedded STM32F4 CPU

- •Core: ARM® 32-bit Cortex®-M4 CPU with FPU, Adaptive real-time accelerator (ART Accelerator™) allowing 0-wait state execution from Flash memory, frequency up to 180 MHz, MPU, 225 DMIPS/1.25 DMIPS/MHz (Dhrystone 2.1), and DSP instructions
- •Memories:
  - 2 MB of Flash memory organised into two banks allowing read-while-write
  - 256+4 KB of SRAM including 64-KB of CCM (core coupled memory) data RAM
- •Clock, reset and supply management:
  - 1.7 V to 3.6 V application supply and I/Os POR, PDR, PVD and BOR
  - 4-to-26 MHz crystal oscillator
  - Internal 16 MHz factory-trimmed RC (1% accuracy)
  - Internal 32 kHz RC with calibration
- •Low power
  - Sleep, Stop and Standby modes
  - VBAT supply for RTC, 20×32 bit backup registers + optional 4 KB backup SRAM
- •JTAG interface
- •1×12-bit, 2.4 MSPS ADC, 7.2 MSPS in triple interleaved mode
- •Up to 17 timers: up to twelve 16-bit and two 32- bit timers up to 180 MHz, 1 IC/OC/PWM or pulse counter and quadrature (incremental) encoder input
- •1xSPI (45 Mbits/s) Master/Slave configurable
- •1USART (11.25 Mbit/s, CTS,RTS RS232)
- •1 × I2C interface (SMBus/PMBus)
- •1 x SD/SDIO interface up to 48MHz (SD v4.2, SDIO v2.0), 1bit-4bit modes supported
- •True random number generator
- •CRC calculation unit
- •RTC: sub-second accuracy, hardware calendar
- •96-bit unique ID
- •USB Connectivity:
  - USB 2.0 full-speed device/host/OTG controller with on-chip PHY
  - USB 2.0 high-speed/full-speed device/host/OTG controller with dedicated DMA, on-chip full-speed PHY and ULPI
- Connections to SmartCard:
  - ISO7816 interface with Clock
  - 1 x GPIO to control external power supply
- Connections to FPGA:
  - 16-bit data, 6-bit address, 100MHz bus SRAM/PRAM mode, 2 x chip selects
  - Master Oscillator pin, up to 90 MHz
  - 5xGPIOs connected to the FGPA JTAG interface for bit-bending programming operations
  - 2xGPIOs for status/polling/interrupt signalling

■ Embedded MachXO2-7000 FPGA

- 6864 LUTs and 47 I/Os
- Ultra Low Power Device (65 nm process, 19 µW standby power, programmable low swing differential I/Os, Stand-by mode and other power saving options)
- Embedded and distributed memory
  - 240 Kbits SysMEM™ embedded blocks RAM
  - 54 Kbits distributed RAM
  - Dedicated FIFO control logic
- 256 Kbits On-Chip User Flash Memory
- Flexible I/O Buffers:
  - (LVCMOS 3.3/2.5/1.8/1.5/1.2, LVTTL, PCI, LVDS, Bus-LVDS, MLVDS, RSDS, LVPECL, SSTL 25/18, HSTL 18,Schmitt trigger input up to 0.5 V hysteresis, etc.)
  - On-chip differential terminations
- Wide Frequency range (10 MHz to 400 MHz)
- Non-Volatile infinitely reconfigurable
- In-field logic configuration while system operates

■ Embedded SLJ52G SECURITY CONTROLLER - SMART CARD

- JavaCard Platform, including ePassport and eSign applets
- ISO7816 Interface
- Supported standards: JC 3.0, GP 2.2, ICAO BAC, SAC, AA, BSI-TR03110 v1.11 EAC, ISO 18013 BAP, EAP config 1-4
- 128 KByte EEPROM
- DES, 3DES, AES up to 256-bit
- RSA up to 2048-bit, ECC up to 521-bit
- Certified Common Criteria CC EAL5+ high

SEcube™ is a Blu5 trademark. All other brand or product names are trademarks or registered trademarks of their respective holders.
The specifications and information herein are subject to change without notice.

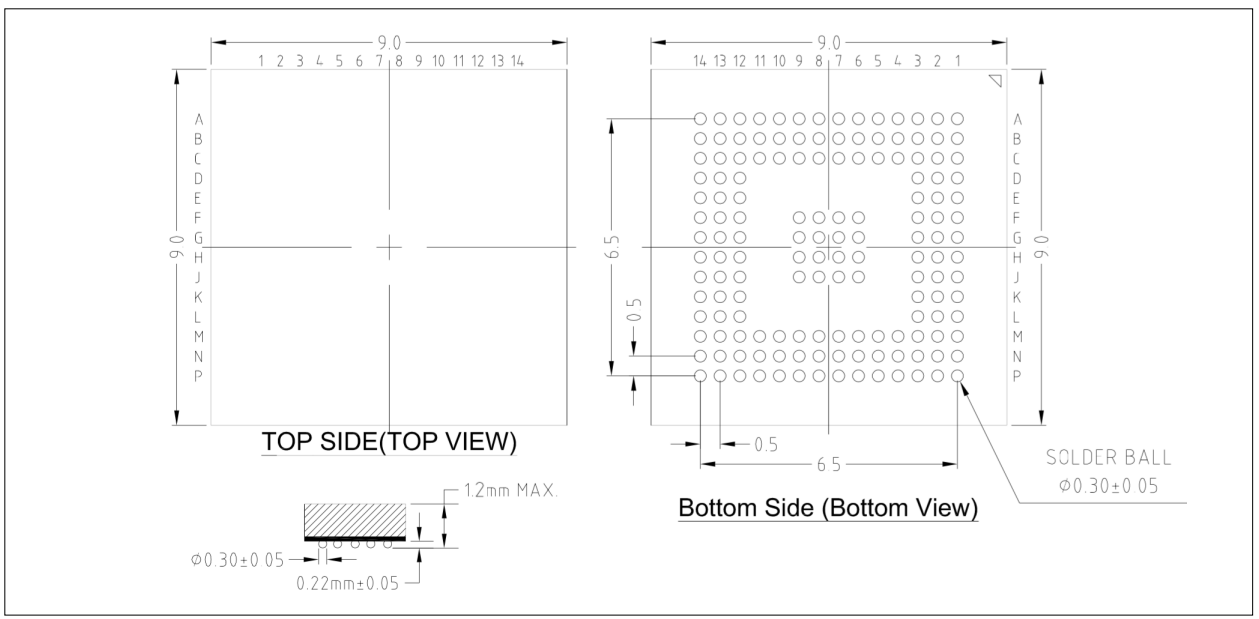
SE*cube*™ Data Sheet Introduction

August 2015 | Data Sheet DUI 15082DS

Pinout and Packaging

SE*cube*™ Pinout Table

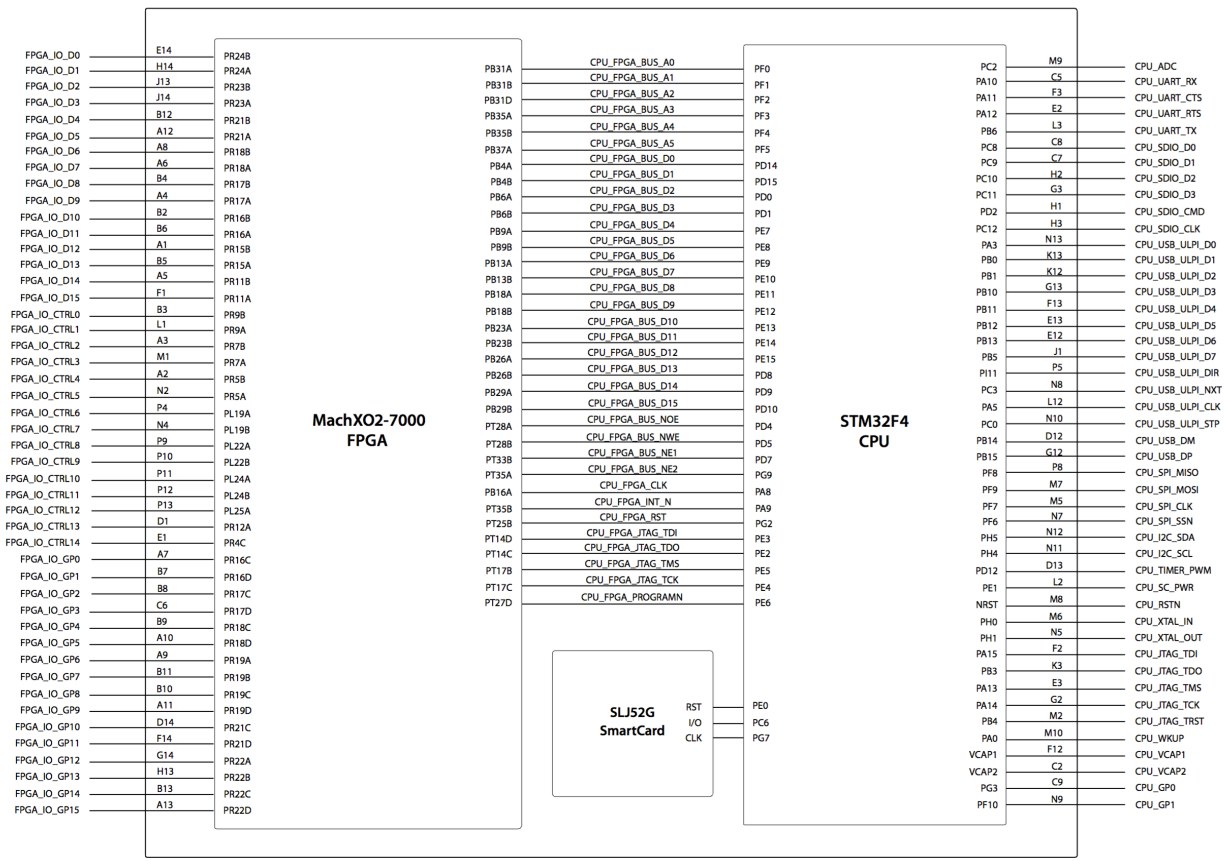
A1	FPGA_IO_D12	B12	FPGA_IO_D4	E3	CPU_JTAG_TMS	H2	CPU_SDIO_D2	L1	FPGA_IO_CTRL1	N6	FPGA_VCORE
A2	FPGA_IO_CTRL4	B13	FPGA_IO_GP14	E12	CPU_USB_ULPI_D6	H3	CPU_SDIO_CLK	L2	CPU_SC_PWR	N7	CPU_SPI_SSN
A3	FPGA_IO_CTRL2	B14	FPGA_VCORE	E13	CPU_USB_ULPI_D5	H6	VSS	L3	CPU_UART_TX	N8	CPU_USB_ULPI_NXT
A4	FPGA_IO_D9	C1	FPGA_VCCIO0	E14	FPGA_IO_D0	H7	VSS	L12	CPU_USB_ULPI_CLK	N9	CPU_GP1
A5	FPGA_IO_D14	C2	CPU_VCAP2	F1	FPGA_IO_D15	H8	VSS	L13	FPGA_VCORE	N10	CPU_USB_ULPI_STP
A6	FPGA_IO_D7	C3	CPU_VDD	F2	CPU_JTAG_TDI	H9	VSS	L14	FPGA_VCORE	N11	CPU_I2C_SCL
A7	FPGA_IO_GP0	C4	CPU_VDD	F3	CPU_UART_CTS	H12	CPU_VDD	M1	FPGA_IO_CTRL3	N12	CPU_I2C_SDA
A8	FPGA_IO_D6	C5	CPU_UART_RX	F6	VSS	H13	FPGA_IO_GP13	M2	CPU_JTAG_TRST	N13	CPU_USB_ULPI_D0
A9	FPGA_IO_GP6	C6	FPGA_IO_GP3	F7	VSS	H14	FPGA_IO_D1	M3	VSS	N14	VSS
A10	FPGA_IO_GP5	C7	CPU_SDIO_D1	F8	VSS	J1	CPU_USB_ULPI_D7	M4	CPU_VDD	P1	FPGA_VCCIO0
A11	FPGA_IO_GP9	C8	CPU_SDIO_D0	F9	VSS	J2	CPU_VDD	M5	CPU_SPI_CLK	P2	VSS
A12	FPGA_IO_D5	C9	CPU_GP0	F12	CPU_VCAP1	J3	CPU_VDD	M6	CPU_XTAL_IN	P3	FPGA_VCCIO5
A13	FPGA_IO_GP15	C10	FPGA_VCCIO1	F13	CPU_USB_ULPI_D4	J6	VSS	M7	CPU_SPI_MOSI	P4	FPGA_IO_CTRL6
A14	FPGA_VCCIO1	C11	CPU_VDD	F14	FPGA_IO_GP11	J7	VSS	M8	CPU_RSTN	P5	CPU_USB_ULPI_DIR
B1	FPGA_VCCIO1	C12	CPU_VDD	G1	FPGA_VCCIO0	J8	VSS	M9	CPU_ADC	P6	FPGA_VCORE
B2	FPGA_IO_D10	C13	FPGA_VCORE	G2	CPU_JTAG_TCK	J9	VSS	M10	CPU_WKUP	P7	FPGA_VCCIO4
B3	FPGA_IO_CTRL0	C14	FPGA_VCCIO2	G3	CPU_SDIO_D3	J12	CPU_VDD	M11	CPU_VDD	P8	CPU_SPI_MISO
B4	FPGA_IO_D8	D1	FPGA_IO_CTRL13	G6	VSS	J13	FPGA_IO_D2	M12	VSS	P9	FPGA_IO_CTRL8
B5	FPGA_IO_D13	D2	FPGA_VCORE	G7	VSS	J14	FPGA_IO_D3	M13	VSS	P10	FPGA_IO_CTRL9
B6	FPGA_IO_D11	D3	FPGA_VCORE	G8	VSS	K1	FPGA_VCORE	M14	FPGA_VCCIO2	P11	FPGA_IO_CTRL10
B7	FPGA_IO_GP1	D12	CPU_USB_DM	G9	VSS	K2	FPGA_VCORE	N1	SC_VCC	P12	FPGA_IO_CTRL11
B8	FPGA_IO_GP2	D13	CPU_TIMER_PWM	G12	CPU_USB_DP	K3	CPU_JTAG_TDO	N2	FPGA_IO_CTRL5	P13	FPGA_IO_CTRL12
B9	FPGA_IO_GP4	D14	FPGA_IO_GP10	G13	CPU_USB_ULPI_D3	K12	CPU_USB_ULPI_D2	N3	VSS	P14	FPGA_VCCIO3
B10	FPGA_IO_GP8	E1	FPGA_IO_CTRL14	G14	FPGA_IO_GP12	K13	CPU_USB_ULPI_D1	N4	FPGA_IO_CTRL7		
B11	FPGA_IO_GP7	E2	CPU_UART_RTS	H1	CPU_SDIO_CMD	K14	FPGA_VCCIO2	N5	CPU_XTAL_OUT		



SE*cube*™ Packaging information

Embedded Components Cross-Connections

Refer to the specific component's data sheets for further details.
Power supply signals are directly connected to the relating components.

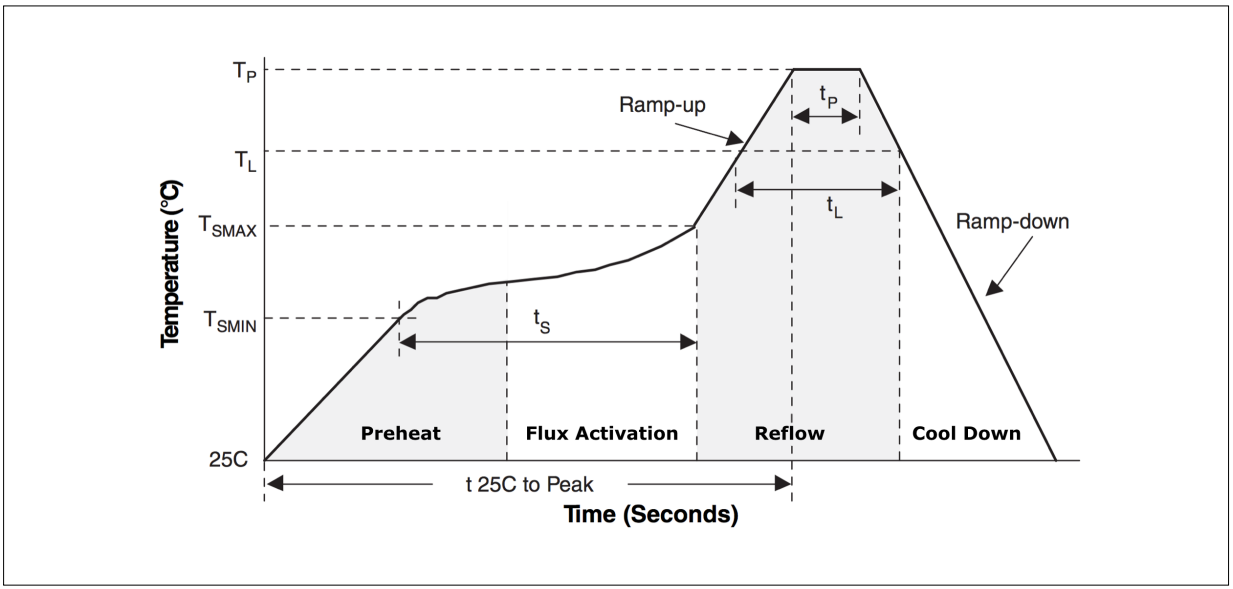


SE*cube*™ Internal Connections

Reflow Profiles

SE*cube*™ Reflow Table

Parameter	Description	Pb-Free and Halogen-Free Packages
Ramp-Up	Average Ramp-Up Rate (T_{SMAX} to T_P)	3 °C/second max.
T_{SMIN}	Preheat Peak Min. Temperature	150 °C
T_{SMAX}	Preheat Peak Max. Temperature	200 °C
t_S	Time between T_{SMIN} and T_{SMAX}	60 seconds–120 seconds
T_L	Solder Melting Point	217 °C
t_L	Time Maintained above T_L	60 seconds–150 seconds
t_P	Time within 5 °C of Peak Temperature	30 seconds
Ramp-Down	Ramp-Down Rate	6 °C/second max.
t 25 °C to T_P	Time from 25 °C to Peak Temperature	8 minutes max.



SE*cube*™ Termal Reflow Profile