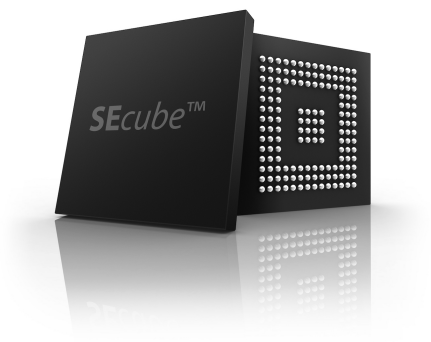
SE*cube*™

Reconfigurable Silicon



SE*cube*™ - Secure Environment cube - is the open hardware and software platform for your own security and application developments.

Powerful and security-oriented, SE*cube*™ is easy to integrate and capable of hiding all the complexity behind a simple set of APIs.

In a single-chip design, SE*cube*™ embeds three main cores: a highly powerful processor, a Common Criteria certified security controller and a high-performance FPGA.

The result of this innovative combination delivers an extremely versatile secure environment in a single SoC (System-On-Chip), in which developers can rapidly implement their complex applications with and deploy into various ICT devices.

SE*cube*™ platform provides many functional entry levels, ranging from hardware to software APIs amenable to become service-ready applications. Whilst easy-to-use and high-security abstraction layer are availed to developers, security experts are now capable of building their system from ground up, starting from the elementary low-level blocks.

Suitable for demanding security projects, SE*cube*™ chip has multiple embedded communication interfaces. In addition, the internal FPGA provides up to 47 fast I/O for custom high-speed interface implementation. This allows fast integration of SE*cube*™ chip into any hardware design, while drastically reducing the final BOM (bill of material).

SE*cube*™ provides several communication interfaces for the integration into any kind of device, as well as multi-level, open source libraries. Blu5 Optimised and GovMil Libraries are available to realise high-grade security services and applications minimising the development effort and reducing drastically the time-to-market.

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

Blu5 Group
info@blu5group.com
www.blu5group.com

SE*cube*™

Reconfigurable Silicon

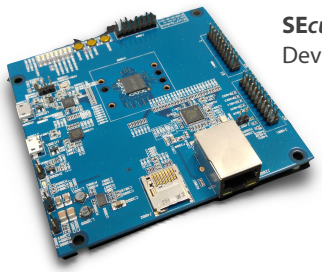
*Technical Specifications**

SE*cube*™ Secure Environment

- STM32F4 - 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 - FLASH 2 MB - RAM 256 KB
- Security Controller SLJ52G - JavaCard Platform, including ePassport and eSign applets
- 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
- Space resilient for LEO satellite applications
- FPGA - MachXO2-7000 - 6864 LUTs - 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
- Wide Frequency range (10 MHz to 400 MHz)
- Non-Volatile infinitely reconfigurable
- In-field logic configuration while system operates
- Interfaces
  - USB 2.0 high-speed/full-speed device/host/OTG controller with dedicated DMA, on-chip full-speed PHY and ULPI
  - 47 FPGA I/Os

SE*cube*™ DevKit - Development Board

- Two USB 2.0 interfaces (Full Speed, High Speed)
- MicroSD card interface
- 10/100Mb Ethernet interface
- 8 User LED, 2 general purpose buttons, 1 reset
- Expansion connectors (GPIOs, SPI, I2C, PWM, ADC, etc.)
- 20-pin JTAG interface
- Powered by USB cable



SE*cube*™ DevKit
Development Board

Open Source Firmware & Libraries

- 10Mbps USB and SDCard communication drivers
- AES256, SHA256, CMAC-AES256
- HW AES256, single session, 100 Mbps
- SE*file*™ basic libraries, for data at rest protection
- SE*link*™ basic libraries, for data in motion protection

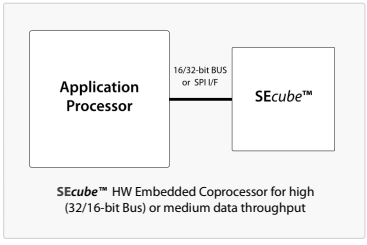
Enhanced/Optimised Firmware & Libraries

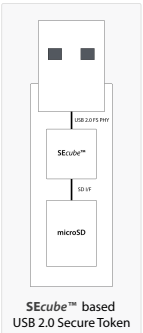
- Smart Boot-loader, multi interface, fast and safe FW injection
- 100Mbps USB and SDCard communication drivers
- Low power management libraries (dynamic, stop, standby)
- Key Management libraries (generation, update, storage, etc.)
- Communication libraries (vocoders, negotiation, etc.)
- SHA256, CMAC-AES256, Elliptic Curves (up to 521-bit), RSA (up to 2048-bit)
- JavaCard Blu5 Crypto Applet (based on EAL5+ security chip)
- Ultra Fast, Configurable HW AES256 ECB/CBC/CFB/OFB/CTR
  - 1.6 Gbps, 6 pipeline levels
  - 8 independent sessions, 8 SBOX
  - enhanced CTR mode (customisable polynomials)
  - SE*file*™ high speed libraries, for data at rest protection2 cache levels, ultra-low overhead
  - SE*link*™ libraries, for data-in-motion protection unlimited sessions, full set of security policies

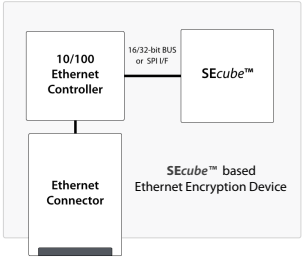
GovMil Firmware and Libraries

Full set of hardware & firmware security functions and libraries for Military and Government users, including specific libraries to allow cryptographic flexibility and full customisation with exclusive additional security mechanisms.

Typical Application Diagrams







Blu5 Group
info@blu5group.com
www.blu5group.com