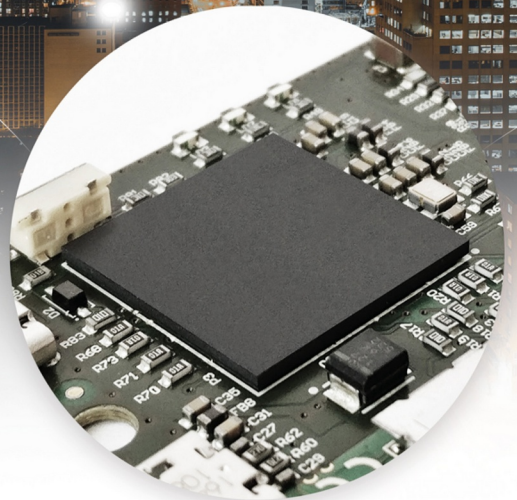
SKUDO



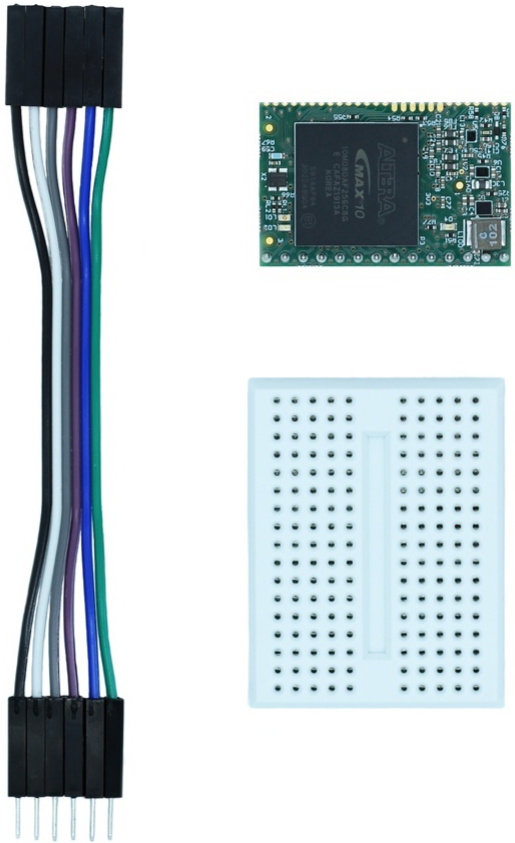
Innovative hardware-based encryption for
secure data communication

MADE IN EUROPE

www.skudo.tech

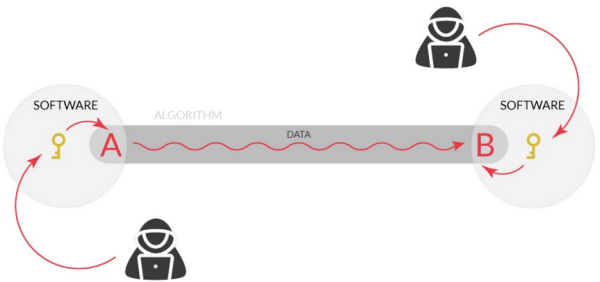
Agenda

- Why Skudo HSM
- The solution
- Inside the FPGA chip
- Applications
- Demo in “space”



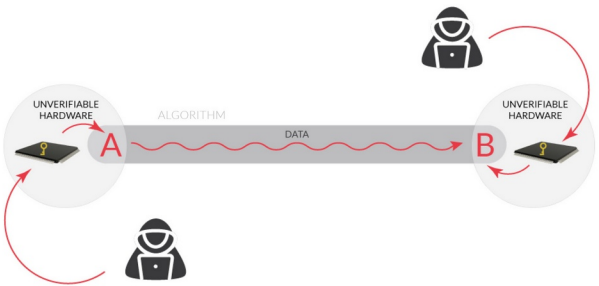
Your data is as safe as the place where you store your encryption keys

SOFTWARE ENCRYPTION



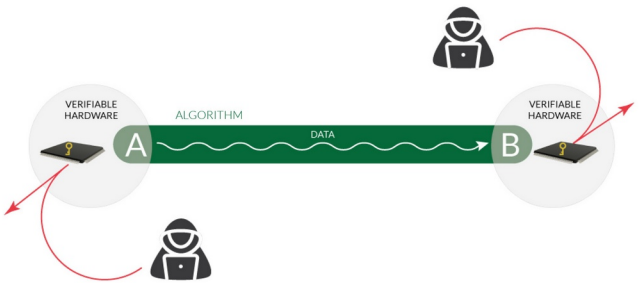
Encryption keys are stored in a software

UNVERIFIED HARDWARE ENCRYPTION



Encryption keys are stored in an harware (chip) which might have backdoors

VERIFIABLE, TRANSPARENT, EUROPEAN HARDWARE ENCRYPTION



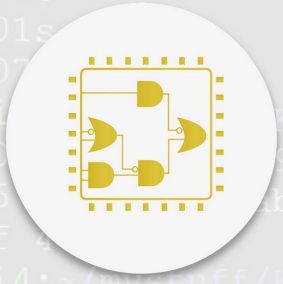
Encryption keys are stored in a verifiable harware (chip)

Our solution

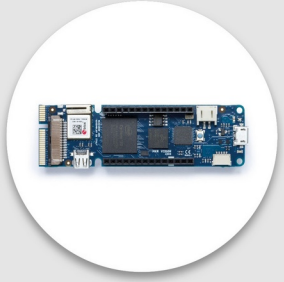
We have developed our own Hardware Security Module (HSM) on a chip, using the FPGA technology.

- Hardware based encryption
- European design and production
- Third party verifiable, no backdoors
- Open source algorithms
- Customizable FPGA technology
- Easy to use and integrate
- Highly optimized softcores

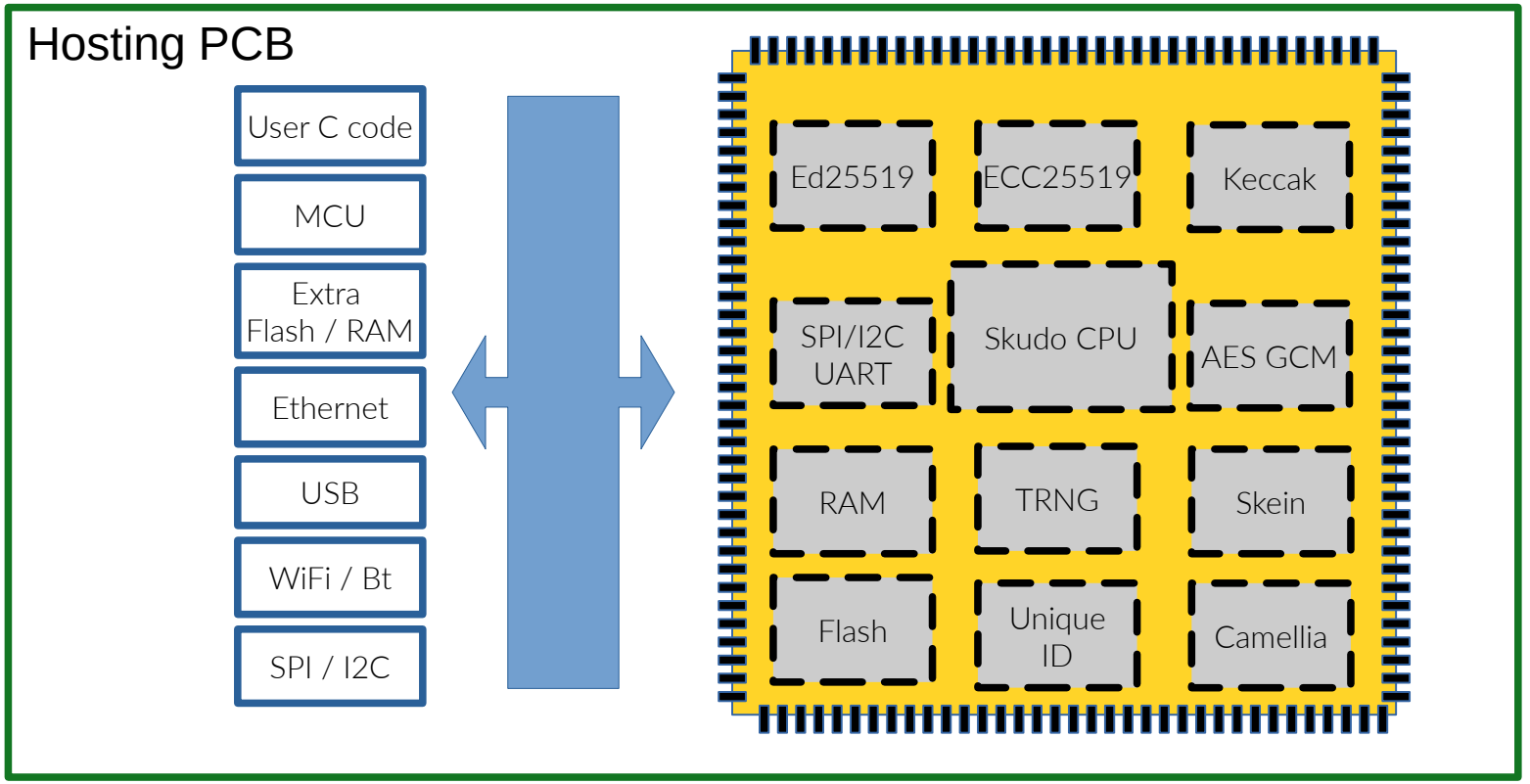
Skudo Softcores



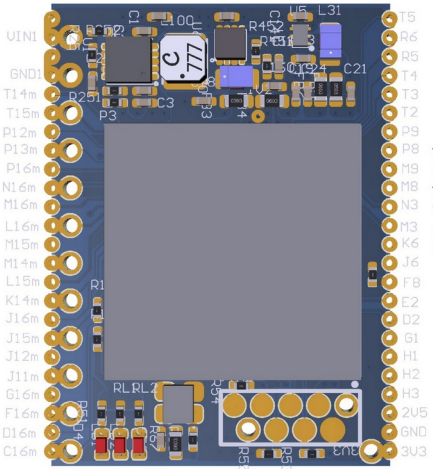
- Symmetric encryption: Camellia, AES GCM
- Asymmetric encryption: Curve25519 (ECDH), Ed25519 (signature)
- Hashing: Skein, SHA3-512 (Keccak) and SHA512
- True Random Number Generator: FIGARO
- Double SPI (users+admin), UART and I2C
- “Skudo-ino” - the porting of our full HSM softcore into the Arduino Vidor4000 FPGA board.*

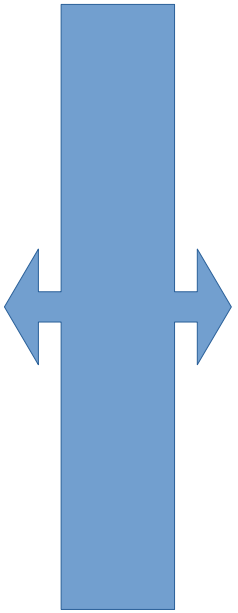


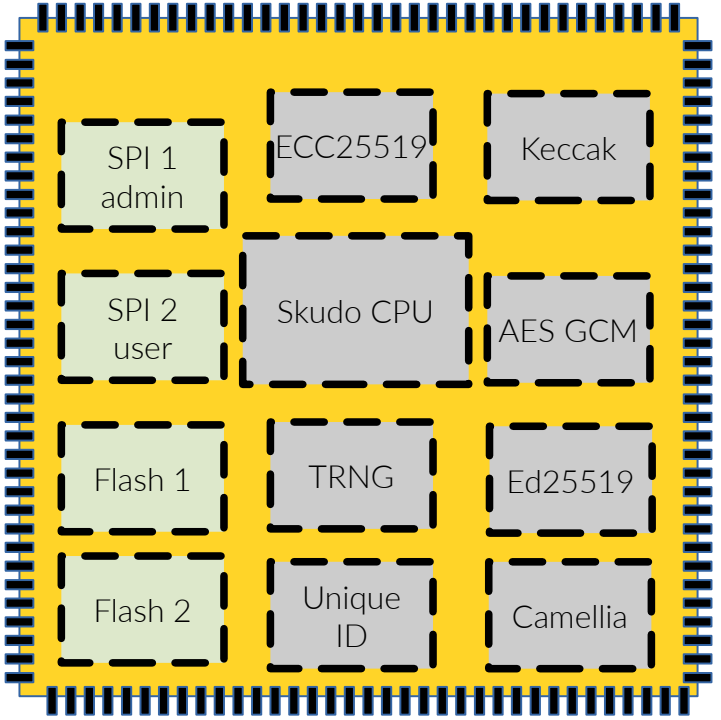
Custom PCB module (HSM + ext MCU) / Skudo



HSM with dual SPI and separate storages







Skudo custom solutions

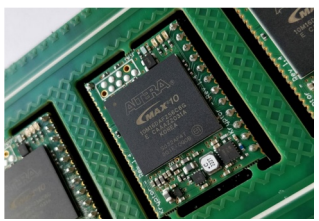
BLACK AND SHIELD

A communication solution that works with a hardware portable device “Black” and software Android app „Shield”.

BLUE

A development board that allows easy testing and integration of the customer’s solution with Skudo encryption chip.
Read more

KRYPTOR



Hardware Security Module (HSM) running on a FPGA chip designed for makers communities.
Read more

Custom solutions for ESA

ESA HAPS

Skudo is carrying out the development of a PKI (CCSDS compatible) within the scope of an ESA procurement contract. It also includes the technical demonstration of the custom built asymmetric End2End encryption (based on that PKI) on a HAPS (High Altitude Pseudo Satellite) by encrypting a Telemetry data stream.

SUPERNOVA

Skudo is designing and developing the consumer hardware product device “Supernova”. It can be used to secure the wireless Telemetry link (MAVlink protocol) of any drone using the Pixhawk autopilot and a Holibro wireless radio link (a widely used combination). The novel asymmetric encryption architecture will be based on the ESA PKI, and will be eventually also tested on a space craft.

Skudo Kryptor HSM on CS

CROWD SUPPLY BROWSE LAUNCH ABOUT US Search

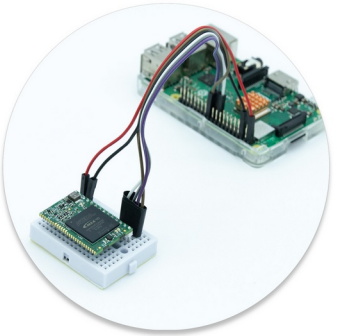
professional European encryption solution to the IoT developer and maker communities with an easy plug-and-play module.

Technical Specifications

- **FPGA**: Intel/Altera MAX10 8K LE (10M08DAF256C8G)
- **Dimensions**: 23x35 mm
- **Internal flash**: 1376 Kb
- **Internal RAM**: 378 Kb total
- **GPIO**: 250 available from the FPGA (fewer accessible via board)
- **Operating frequency**: 100 MHz
- **Control**: API / encrypted command line interface (CLI)
- **Platform compatibility**: Linux, RPi, Arduino, etc.
- **Duplication protection**: Anti-piracy duplication protection via chip ID
- **Encryption speed**: symmetric encryption speed up to 108 Mbps on a single core (SPI link speed capped at 2 Mbps)
- **Power consumption**: ~58 mAh (idle state) to ~65 mAh (constant operations)

Kryptor HSM for CrowdSupply

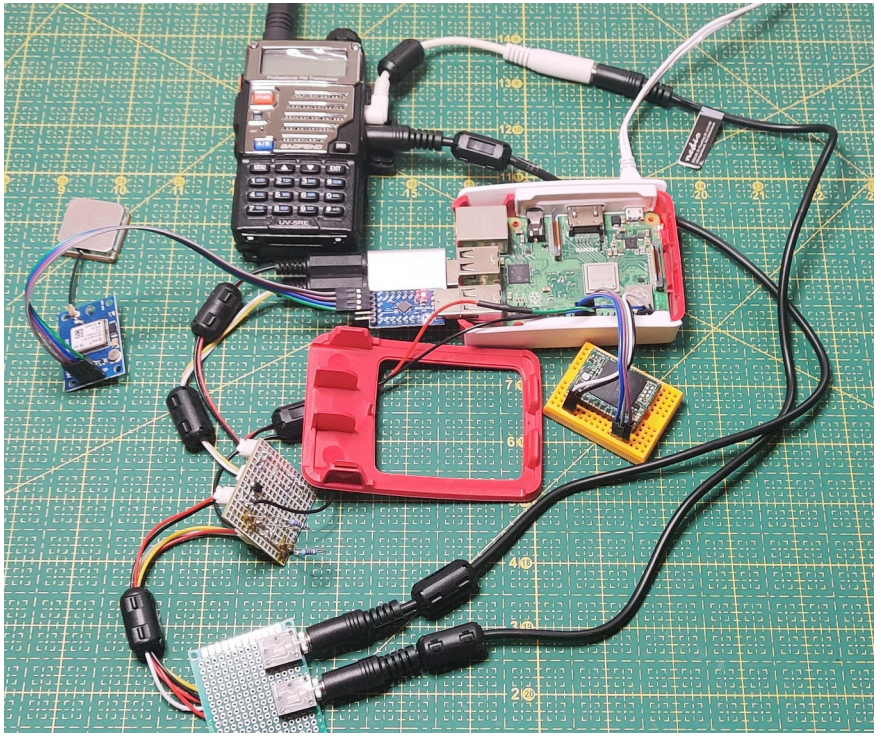
B2C / B2B2C



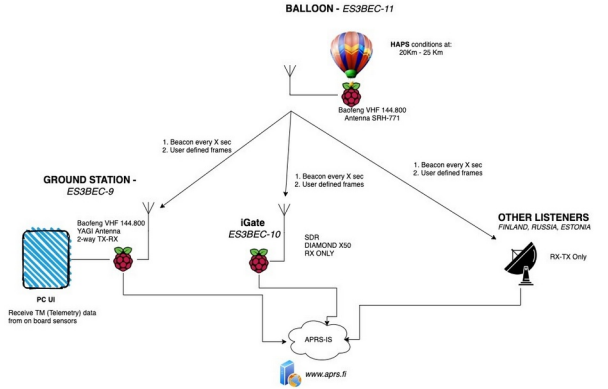
Makers / System integrators via CROWD SUPPLY platform

The board is available at: https://skudo.tech/kryptor

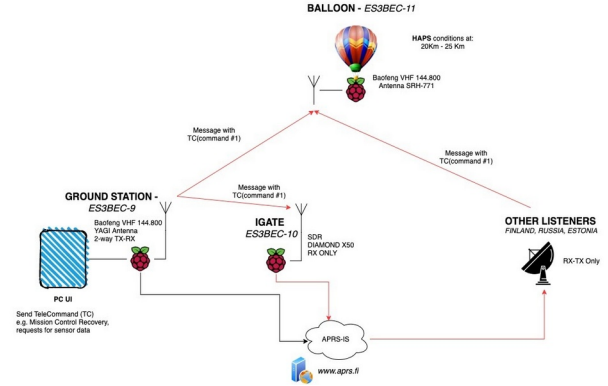
ESA PoC in HAPS conditions



DOWNLINK



UPLINK



t0 Beacon Reserv.	t5 UL SDLS	t10 DL SDLS	t15 UL SDLS	t20 DL SDLS	t25 UL SDLS	t30 DL Report	t35 UL SDLS	t40 DL SDLS	t45 UL SDLS	t50 DL SDLS	t55 UL SDLS

Innovation research

business incubation centre Estonia

- Symmetric Key Infrastructure (SKI)[1]
- Public Key Infrastructure (PKI) [2]
- Physical Unclonable Functions (PUF) [3]
- Elliptic Curve Integrated Encryption Scheme ECIES [4]
- Post Quantum Cryptography (PQC) [5]

1. https://en.wikipedia.org/wiki/Symmetric-key_algorithm
2. https://en.wikipedia.org/wiki/Public_key_infrastructure
3. https://en.wikipedia.org/wiki/Physical_unclonable_function
4. https://en.wikipedia.org/wiki/Integrated_Encryption_Scheme
5. https://en.wikipedia.org/wiki/Post-quantum_cryptography

SKUDO OÜ

www.skudo.tech

STEFANO ALBERICO

Stefano@skudo.tech

PGP keyID: 46020FD9

Twitter: @SkudoTech

Telegram: http://bit.ly/skudo-tg

esa business incubation centre Estonia

SKUDO OÜ is participating in the ESA Business Incubation Centre Estonia

SKUDO OÜ is an European company, based and operating from Estonia

October 2020

Extra slides

Business model

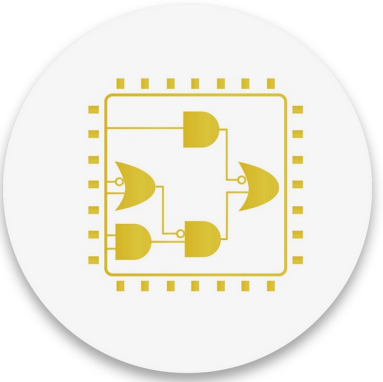
Custom Projects

Space, IoT, Critical Infrastructure, Drones etc.

Physical Products

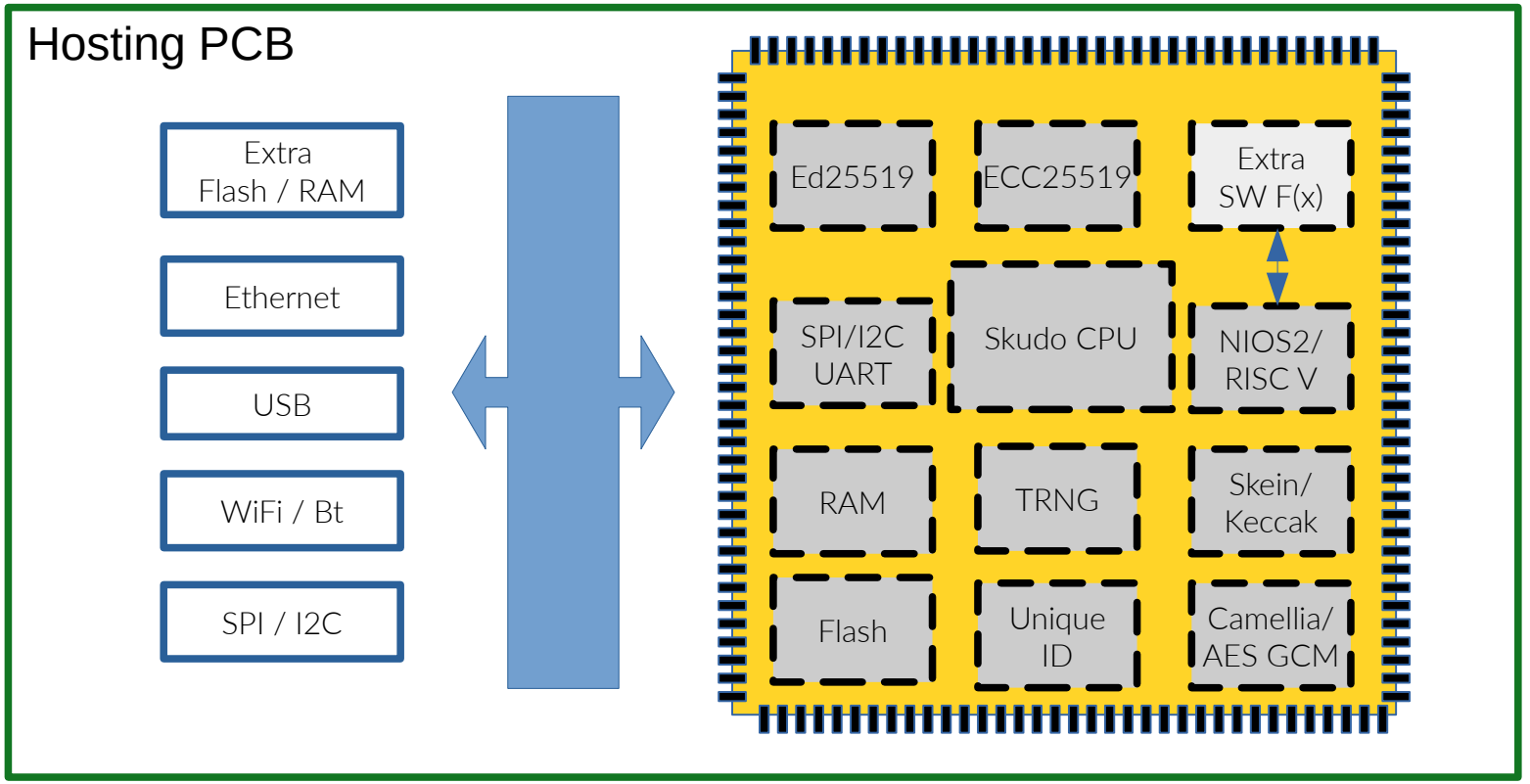
Supernova - encrypted data transfer for drones

FPGA SOFTCORES

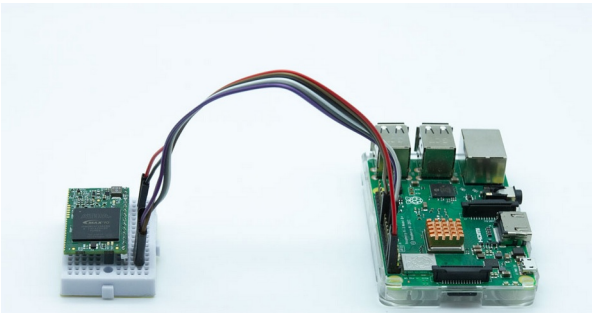


Licenses

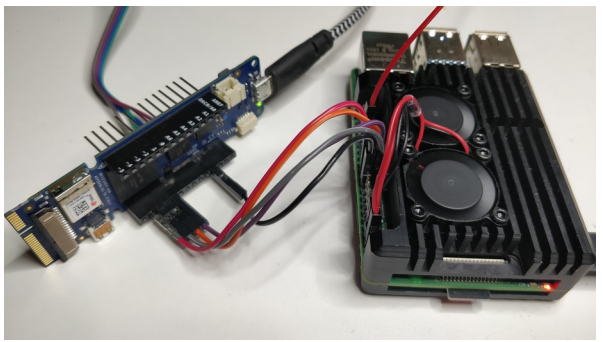
Custom PCB module (HSM + internal CPU)



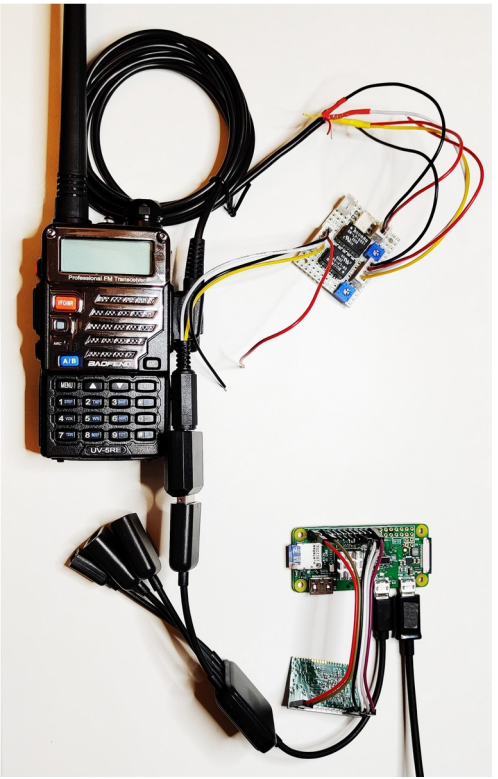
Different setups



RPi3 + Kryptor HSM



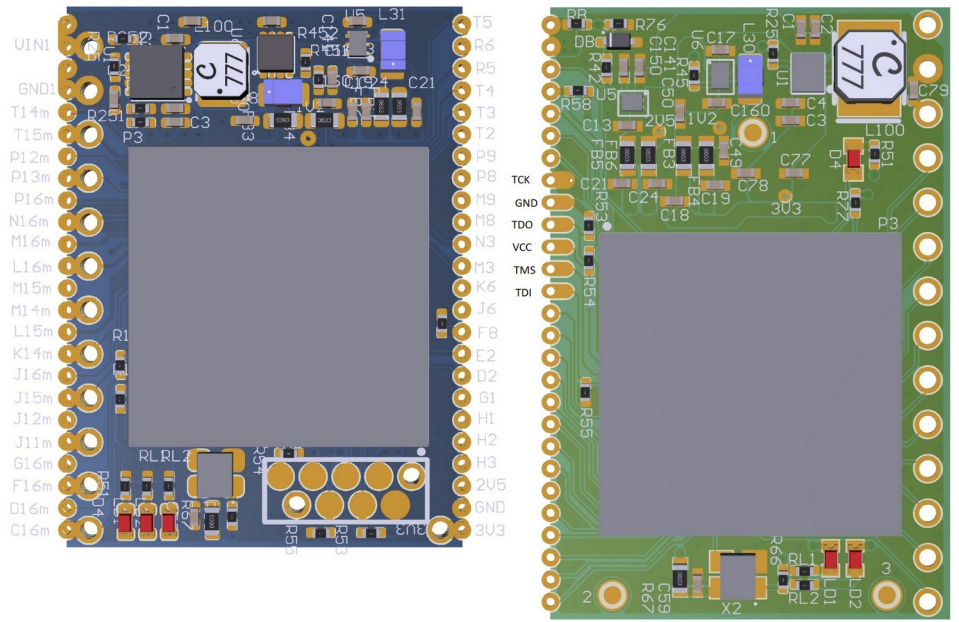
Arduino Vidor4000 +
Skudo HSM softcore



Packet radio setup +
Kryptor HSM (ESA)

Kryptor PCB evolution

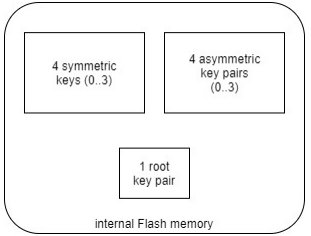
Latest Kryptor HSM

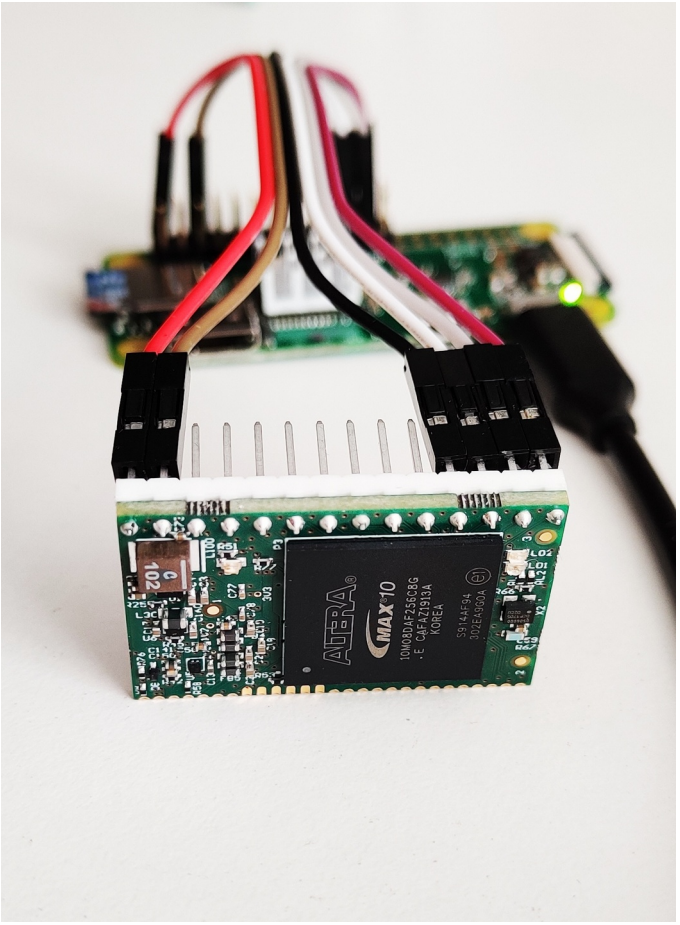


Previous version
of Kryptor HSM

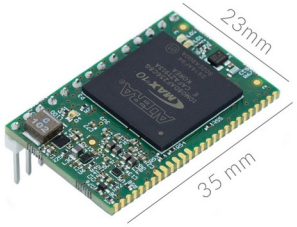
Skudo Kryptor HSM - CS

- Kryptor HSM (8K LE)
- Camellia, Skein, ECDH, TRNG
- Raspberry Pi Zero W
- LiPo battery
- SPI connection (4 wires) at 2 Mbps
- Skudo CLI (Linux SDK)
- SSH Terminal via WiFi





Skudo HSM PCBs

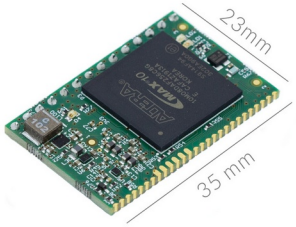


KRYPTOR

- Model: MAX10 8K LE
- 1376 Kbits of internal Flash
- 378 Kb of total internal RAM
- up to 50 GPIO

- Runs at 100 MHz

- SPI link speed up to 2 Mbps
- UART speed up to 921.6 Kbps
- API / encrypted command interface
- Anti piracy duplication protection (via chip ID)

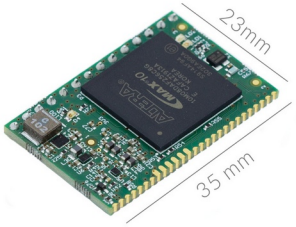


PRO

- Model: MAX10 8K LE
- 1376 Kbits of internal Flash
- 378 Kb of total internal RAM
- up to 50 GPIO

- Runs at 100 MHz

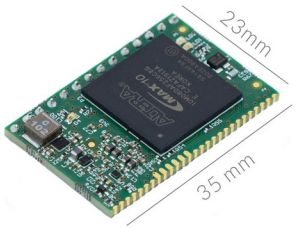
- SPI link speed up to 10 Mbps
- UART speed up to 921.6 Kbps
- API / encrypted command interface
- Anti piracy duplication protection (via chip ID)



ULTIMATE

- Model: MAX10 8K LE
- 1376 Kbits of internal Flash
- 378 Kb of total internal RAM
- up to 250 GPIO

- Runs at 100 MHz
- Symmetric encryption speed up to 108 Mbps (can be increased with multiple cores)
- SPI link speed up to 90 Mbps (can be increased with quad SPI)
- API / encrypted command interface
- Anti piracy duplication protection (via chip ID)



OTHER

custom built solutions:

- Model: MAX10 up to 50K LE
- up to 5888 Kbits of internal Flash
- up to 1638 Kb of total internal RAM
- up to 500 GPIO

- Runs at 100 MHz
- Symmetric encryption speed up to 108 Mbps (can be increased with multiple cores)
- SPI link speed up to 90 Mbps (can be increased with quad SPI)
- API / encrypted command interface
- Anti piracy duplication protection (via chip ID)