HECTOR

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644052

Secure Portable USB Data Storage

HECTOR Demonstrator 2 platform

Marcel Kleja (1), Marek Laban (1,2), Viktor Fischer (3)

(1) MICRONIC a.s., Bratislava, Slovak Republic

(2) Technical University of Kosice, Slovak Republic

(3) Laboratoire Hubert Curien Saint-Etienne, France

HECTOR Outcomes in Demonstrator

- → Authenticated encryption
  - → CAESAR competition candidate - ASCON used
- → True Random Number generator
  - → PLL-TRNG with integrated embedded tests compliant with AIS 20/31 PTG.2
- → Physically unclonable function
  - →TERO PUF with postprocessing (32-bits of the 128-bit key)

Secure Portable Data Storage

- USB mass storage class flash drive with integrated HW cipher
- Designed to protect sensitive personal information
  - Protects data stored on it at rest
  - Target audience: lawyers, doctors, notaries...

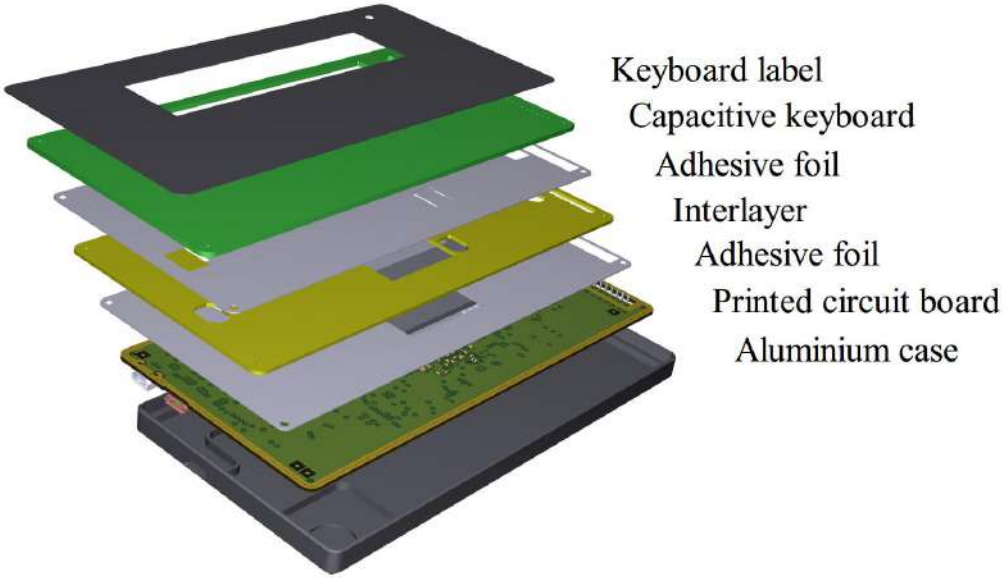
- Motivation for development of such a device:
  - Weaknesses have been discovered in similar secure solutions (key stored “securely” in the device)
  - Lack of trusted secure storage solutions engineered and manufactured in EU
  - To demonstrate HECTOR project outcomes

Secure Portable Data Storage

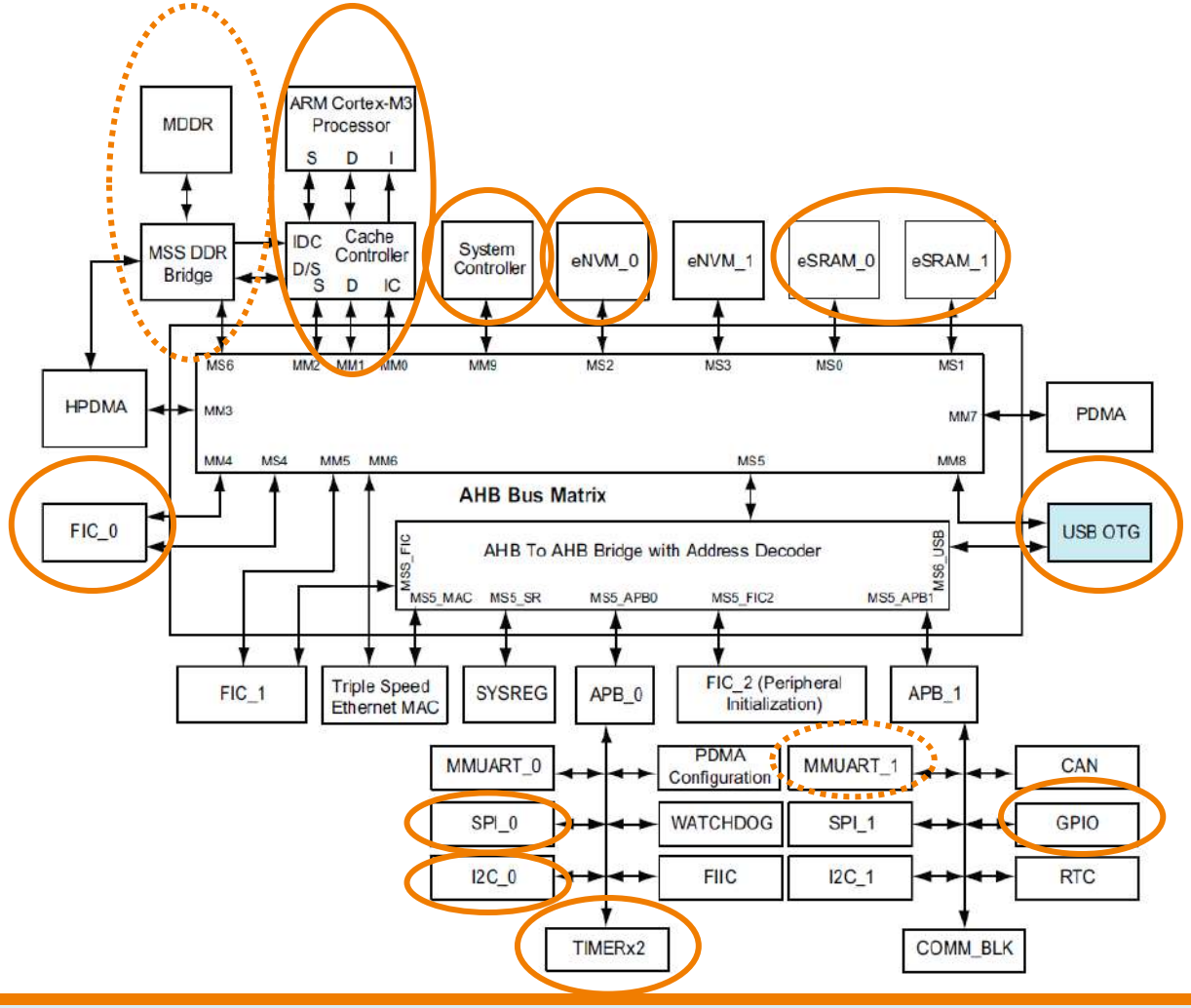
- Data are stored on a replaceable SD-card (up to 32 GB)
- Based on Microsemi SmartFusion2
- Passphrase entered directly on device – reduces risk of keylogger attacks
- The data throughput is >19MB/s for read and >13MB/s for write

Secure Portable Data Storage – HW Development

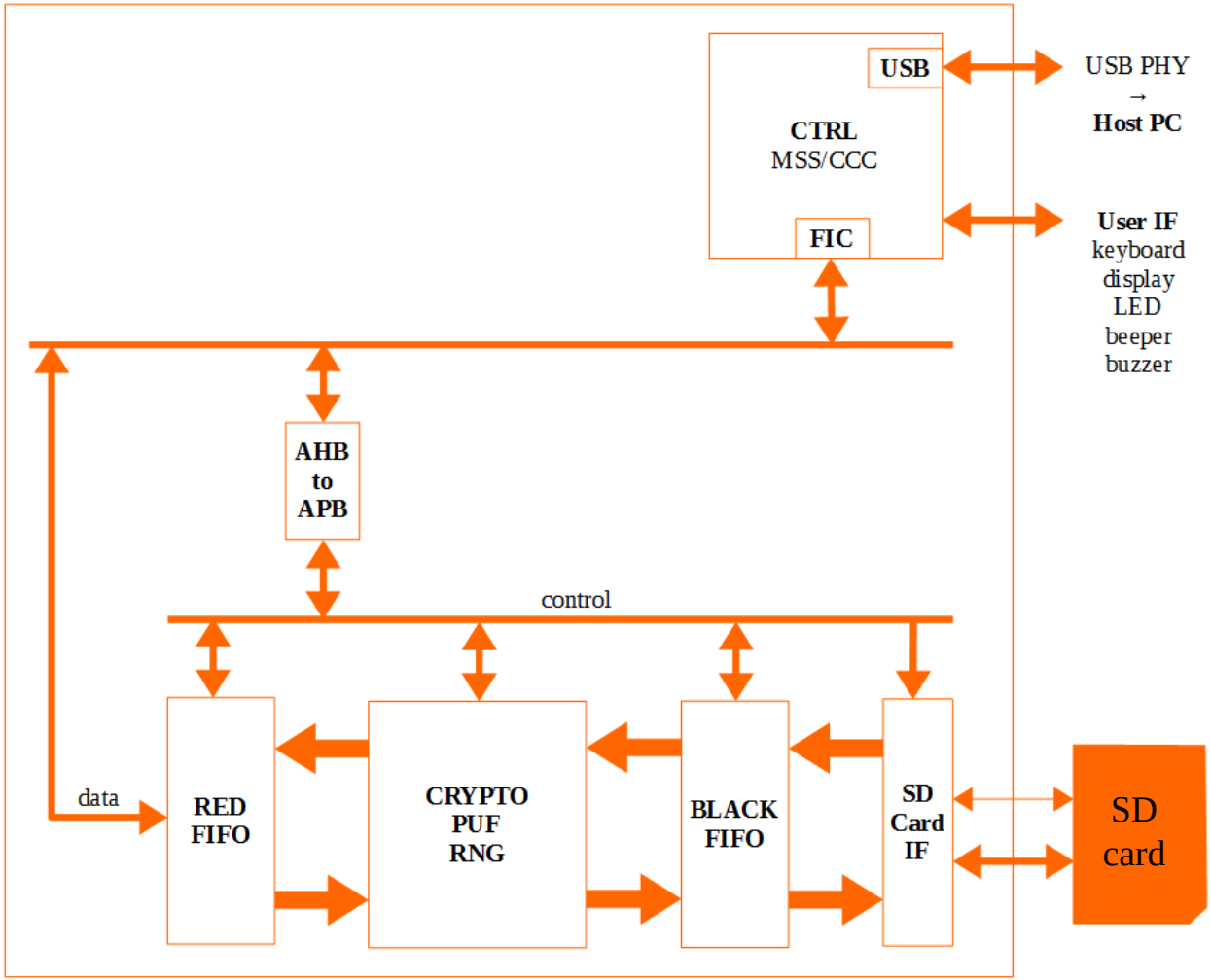
- Complex process – several versions developed
  - First version based on existing commercial evaluation boards
  - Second version on HECTOR evaluation boards
  - Final version:
    - Capacitive keyboard implemented
    - Custom case developed
    - Device is assembled using adhesive foils
    - Protected against disassembling by poured epoxy mass in the bottom case



Microsemi SmartFusion2 – MSS Utilization



Microsemi SmartFusion2 – FPGA Fabric



HECTOR Evaluation Platform

- Based on motherboard and daughter board modular system
- Developed for easy evaluation and development of cryptographic primitives

- Main advantages:
  - Low-cost, exchangeable daughter boards
  - Adapted to implementation of side-channel attacks
  - Support for daughter board remote connection via HDMI cable

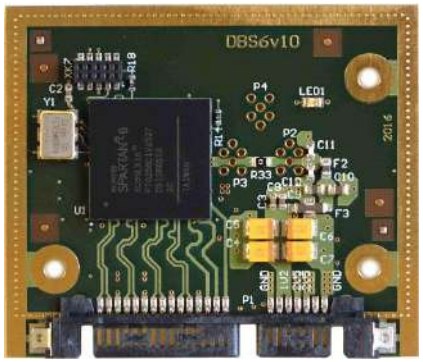
HECTOR Evaluation Platform – Motherboard

- Based on Microsemi SmartFusion2
- 64 MB of external RAM, USB interface
- Only low-noise linear regulators are used

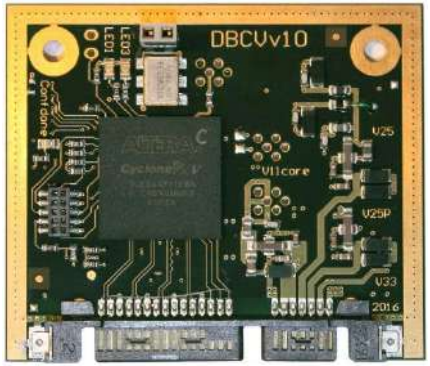
- Complex acquisition system implemented
- Controlled by the PC using a USB interface and TCL scripts

Development Process

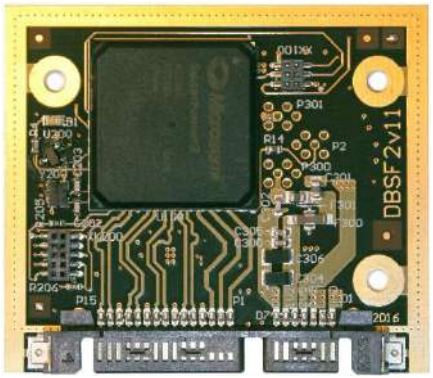
- Primitives examined on FPGAs of three different families
- Evaluated on many FPGAs in order to verify reproducibility and reliability
- Tested and measured in various environmental conditions using a remote connection of the module
- Evaluation platform – a step to demonstrator development



Xilinx Spartan 6

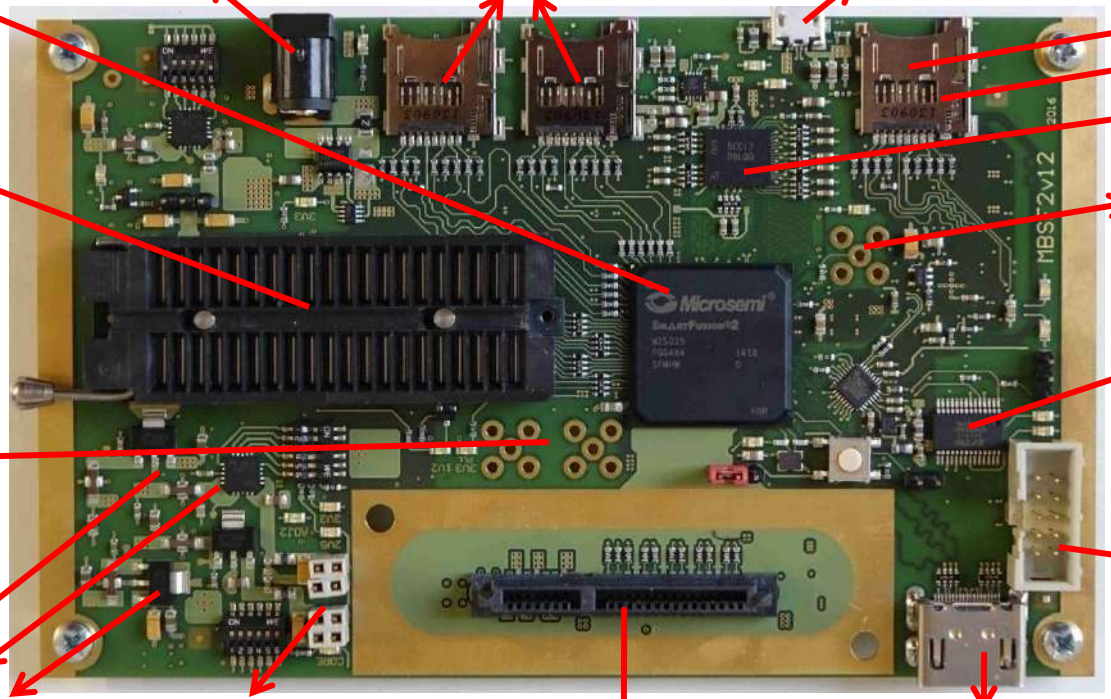


Altera Cyclone V

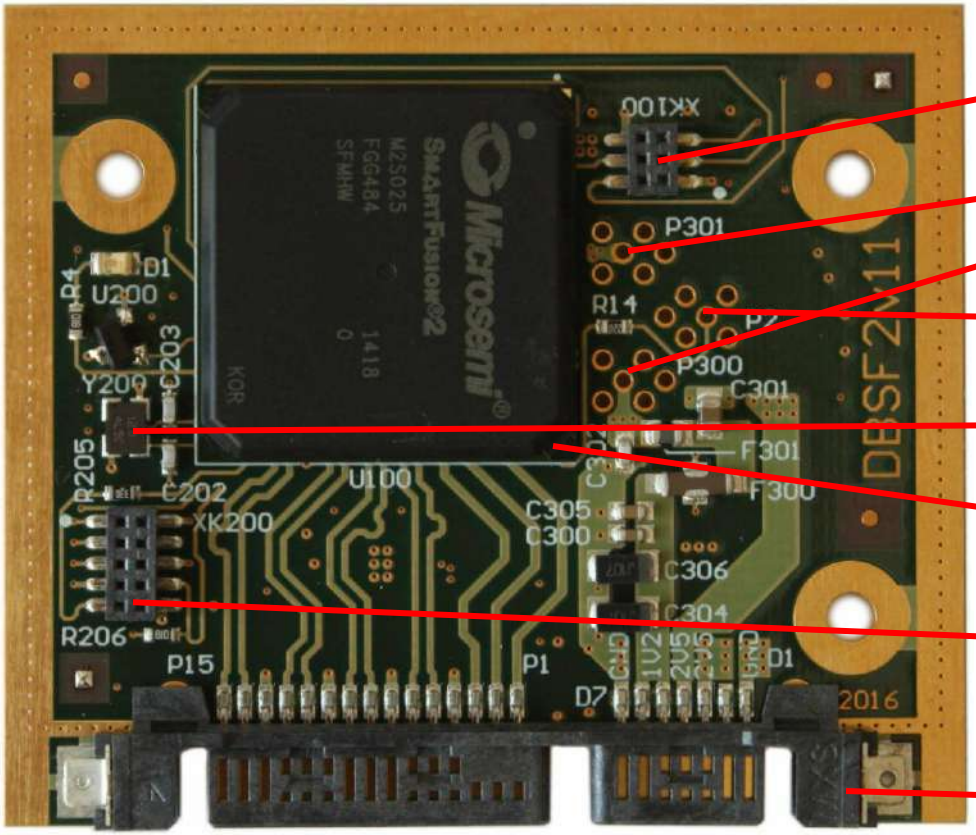


Microsemi SmartFusion 2

HECTOR Mother Board 1 – Microsemi SF2



HECTOR Microsemi SmartFusion 2 Daughter Board



Usage of the Device

- Empty
  - Security critical data zeroized
- Enrolled
  - Security critical data generated: helper data, data encryption key
- Once enrolled – user just enters his passphrase to generate 96 bits of the key (remaining 32 come from the PUF)

Demonstration

- Follows…

Conclusions

- The device demonstrates results of the HECTOR project
- It can be used as a secure HW storage of highly sensitive data
- Main advantages:
  - The confidential key is not stored in the device
  - A part of the key is device dependent but not reachable by the attacker (PUF)

"The **HECTOR** project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement number 644052."

If you need further information, please contact the coordinator:
TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55 Fax: +43 4242 233 55 77
E-Mail: coordination@hector-project.eu