ASSURED

SECURITY CONSULTANTS

Cryptech

The Open Hardware Security Module Platform

::1

Joachim Strömbergson
Assured AB
https://github.com/secworks

IT security
- Embedded systems
- ASIC, FPGA
- Biometrics

Open Crypto Hardware
CPU design
Assembly hacking

Hardware Security Modules

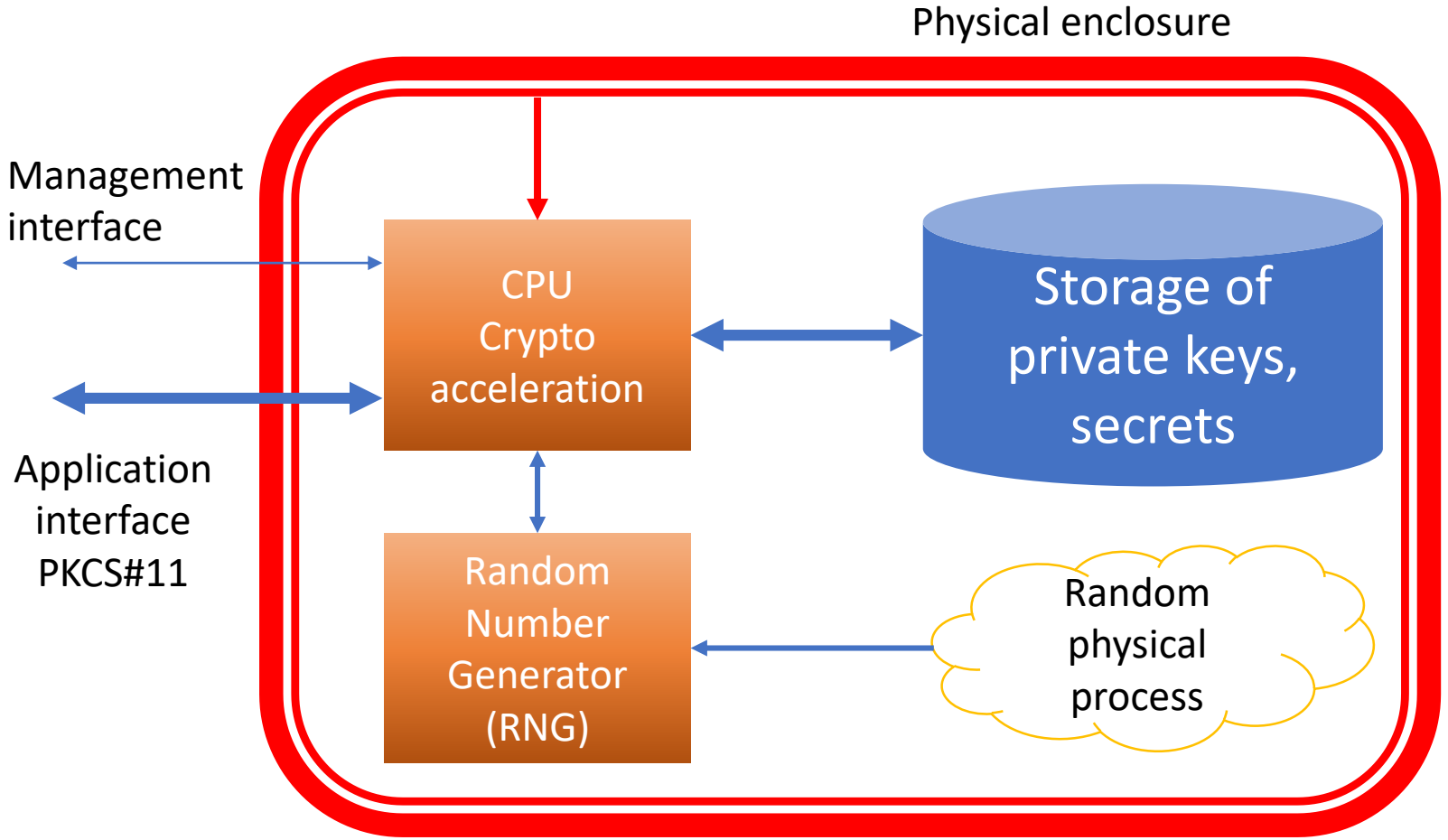
Black Boxes FTW

Hardware Security Module (HSM)

- Dedicated appliance for cryptographic operations
- Generate, use and store secrets (private keys in PKI)
  - Protect secrets
- Offload sensitive operations from general systems
  - Crypto acceleration

- Very expensive
- Very few vendors
- National interests – strong connections to agencies

Hardware Security Module (HSM)



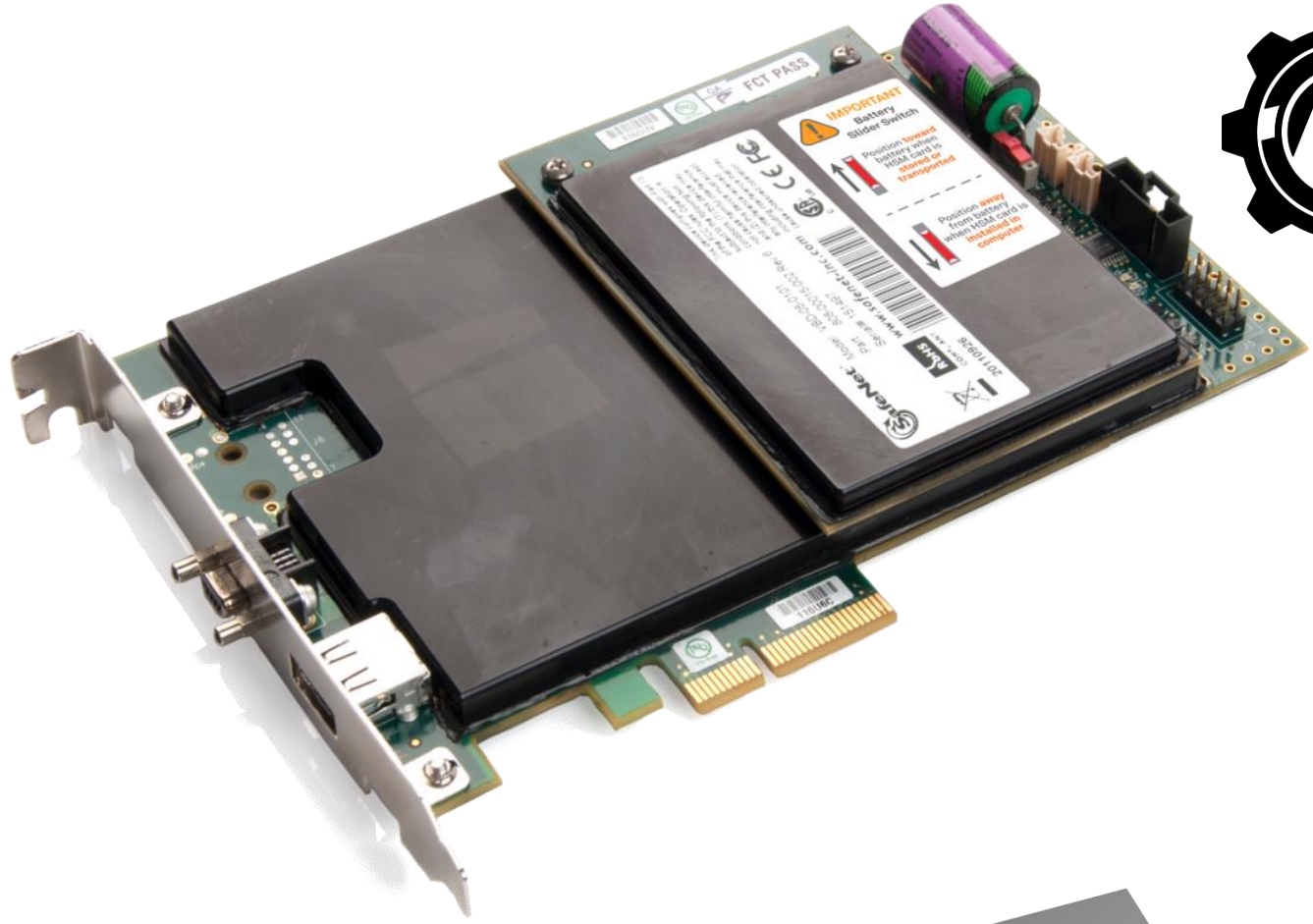

Authentication
Acceleration
UAF
Cerificates
Gambling
Banking
SAML
Gaming
VPN
BGPSEC
OTR
RND
U2F
Keywrap
HSM
OTP
OpenID
PIN
PGP
TLS
RPKI
S/MIME
Payments
OAUTH
DNSSEC
PKI
Passports
Storage
Encryption
IPsec
Ecommerce
Lottery
Signing
eGov
Key_generation
ID-cards

Hardware Security Module (HSM)

- PKCS#11
  - Public Key Crypto Standard. And API
  - Object types for RSA keys, X.509 Certificates
    - Generate, Sign, Seal, Verify, Export
  - RSA Security, now OASIS

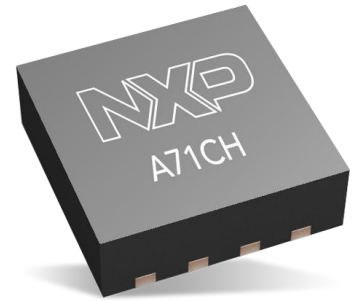
- NIST FIPS 140-2, 140-2, Common Criteria, NIST SP 800-90, BSI AIS31


AEP systems

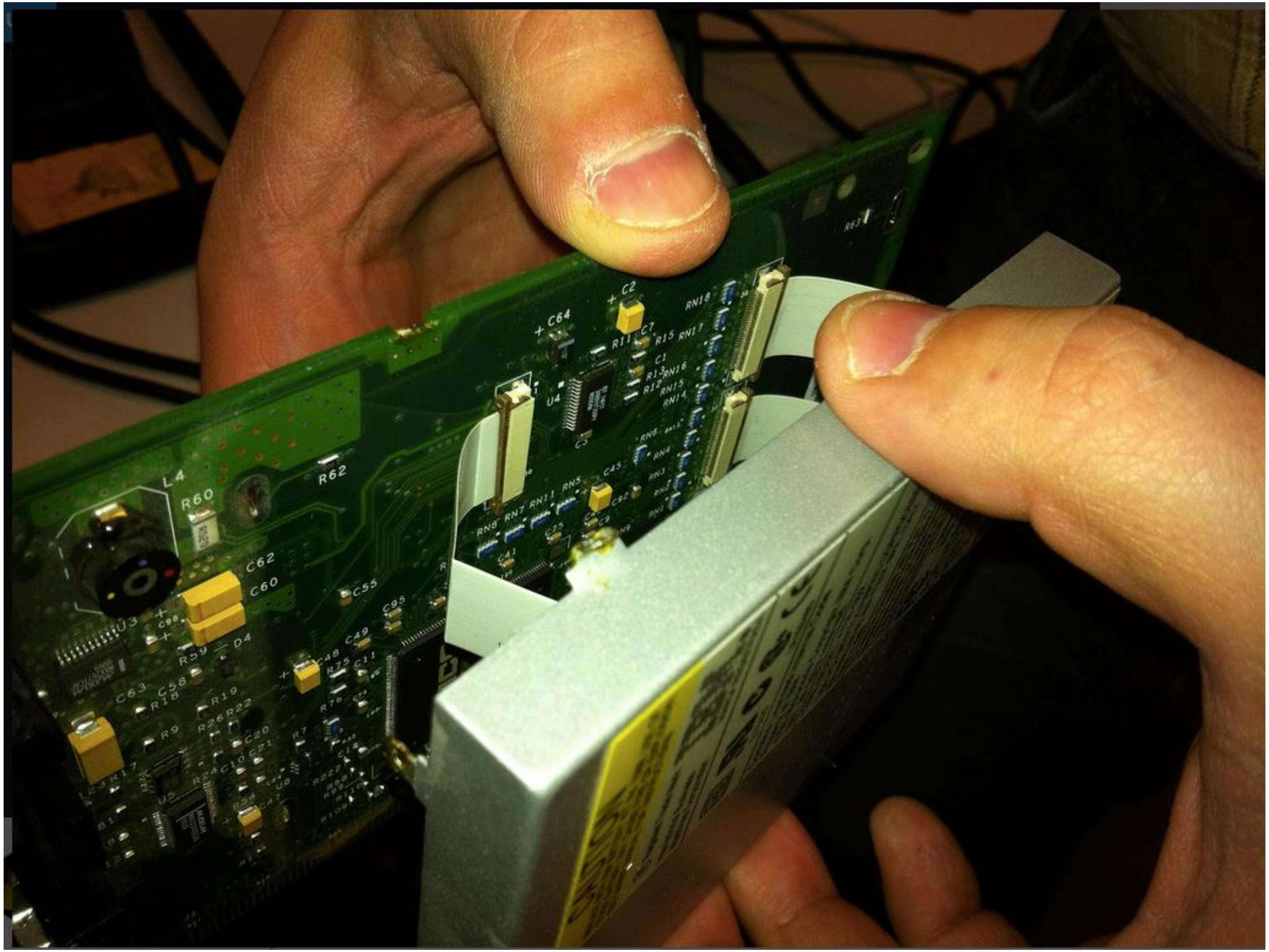

FCT PASS
IMPORTANT
Battery
Slider Switch

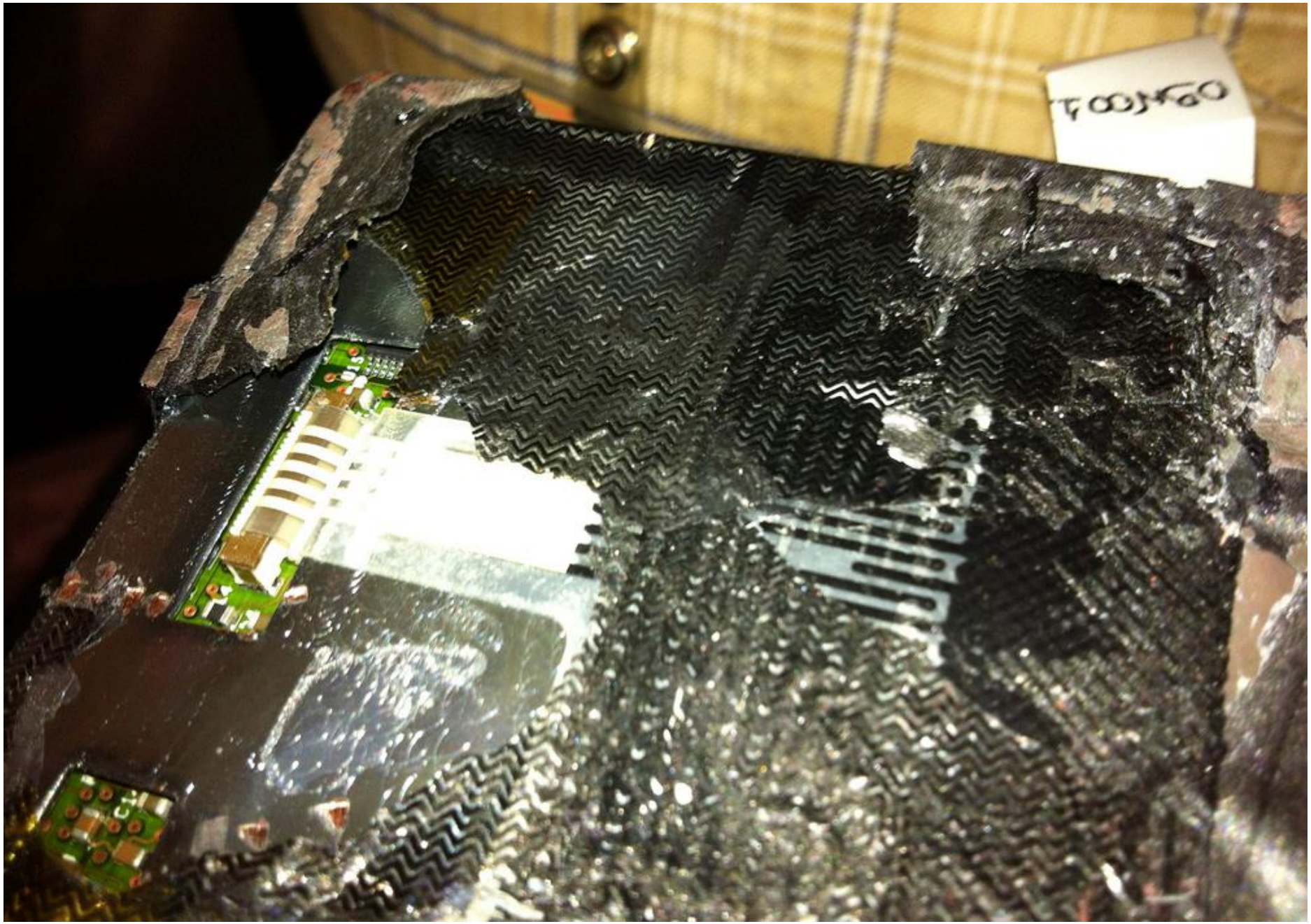

Infineon
TPM1.2
SLB 9635 TT 1.2


THALES


NXP
A71CH


IBM 4758 PCI HSM
CAUTION
REPLACE WITH IBM BATTERY KIT No. 1008. USE OF OTHER BATTERY MAY CAUSE FIRE OR EXPLOSION. SEE OWNER MANUAL FOR INSTRUCTIONS
Registed Trade Mark
International Business Machines Corporation
IBM
MARCA REGISTRADA
E178428
LR102480
Contains Licensed Internal Code
Property of IBM
4758 Microcode Copyright IBM Corp. 1997. All rights reserved.
TYPE-MODEL 4758-002
Type: PCI CRYPTOGRAPHIC COPROCESSOR
Manufactured by IBM ITALY SPA, ITALY
Made in Italy
This device complies with Part 15 of FCC Rules Operation is subject to the following two conditions (1) this device may not cause harmful interference and (2) this device must accept any interference received including interference that may cause undesired operation
Tested To Comply With FCC Standards
FOR HOME OR OFFICE USE
Canada ICES/NMB-003, Class/Class B
+12V : 0,1A
5V : 1,4A
FRU P/N 10J0077


C64
C2
C7
R11
R15
RN18
RN17
RN16
RN15
RN14
C1
U4
C3
RN6
RN4
RN3
RN2
RN1
C45
RN8
RN7
RN11
RN5
C75
C9
C41
L4
R60
R62
C62
C60
C55
C95
C49
U3
D4
R59
C48
R75
C11
C63
C58
R18
R19
R22
R26
R9
C20
R7
R17
U5
U8




1306
AMD
Altera
ATMEL
AT89S8515A
24C
9639

The random-number generators used for key generation are fatally flawed,
and have generated real certificatescontaining keys that provide no security whatsoever.

Dual_EC_DRBG in SP 800-90

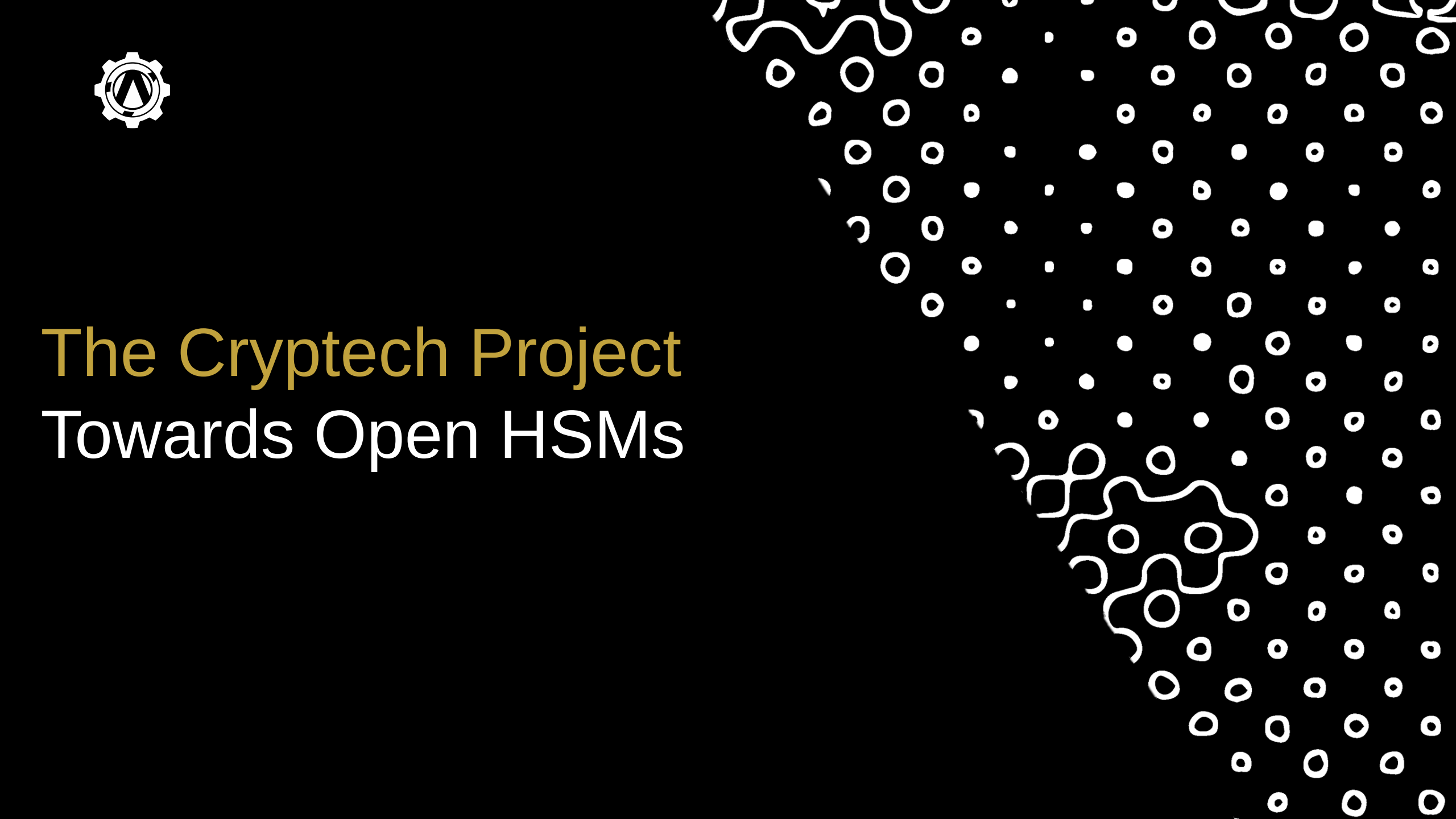
THE ESTONIAN ID CARD: A UNIQUE PLATFORM

- **1,295,844** valid ID cards, of which 26,199 e-residency cards in a total 142 countries (2018)
- First document signed with ID card on **7 October 2002**
- Almost 500 million digital signatures and over 670 million authentications as of May 2018
- **747,580** ID cards are used electronically at least once a year; about 42,000 people use their ID card digitally at least one hundred times in a three-month period
- The Estonian Information System Authority (RIA) is responsible for the digital elements on the ID card since 2016. As an identity document, the card remains in the jurisdiction of the Police and Border Guard Board. The certificates for the ID card are issued by SK ID Solutions AS
- The 2017 Emergency Act specifies authentication by ID card and digital signature as a **vital services**
- Estonia was notified of a cryptographic weakness in late summer 2017; it made the ID card theoretically vulnerable and affected approximately **800,000 cards** issued since October 2014
- The (remote) **updating** of the ID card – the replacement of the certificates with new ones – became possible on 25 October 2017
- The faulty certificates were **suspended** on 3 November 2017
- The faulty certificates were **revoked** on 1 April 2018 and could no longer be updated. **94%** of ID-cards that had been electronically used were updated; of the 494,000 ID cards that were renewed, 354,000 were updated remotely
- As of the end of 2017, 160,000 people were using mobile ID and 140,000 were using Smart-ID

Faulty RSA key generation (ROCA) in Secure Element chips from Infineon. >1 Billion(!) devices affected globally

HSM Vulnerabilities

- CVE-2015-5464: SafeNet Luna remote key export restriction bypass
- CVE-2015-1878: Thales nShield arbitrary sign, key extract



The Cryptech Project

Towards Open HSMs

The Cryptech Project

- Multi-year effort to move towards an open HSM platform developed using open, auditable and trusted tools.
- Started at the suggestion of Russ Housley, Jari Arkko, and Stephen Farrel of the IETF to meet the assurance needs of supporting IETF protocols in an open and transparent manner.
- Composable, e.g. "Give me a key store and signer suitable for DNSsec“
- Reasonable assurance by being open, diverse design team
  - Core team from Sweden, Russia, USA, Germany, Japan, Ireland
  - Open development, signed commits to Git repos etc

The Cryptech Project

- 2-clause BSD license for all SW, FPGA source code
  - All cores for crypto acceleration in HW (AES, SHA-256, RSA, EC)
- Creative Commons for all drawings, documents
  - PCB layout, Bill of Materials (BoM)

- Repos accessible via trac: https://trac.cryptech.is/'
- Maillists: https://trac.cryptech.is/wiki/MailingLists

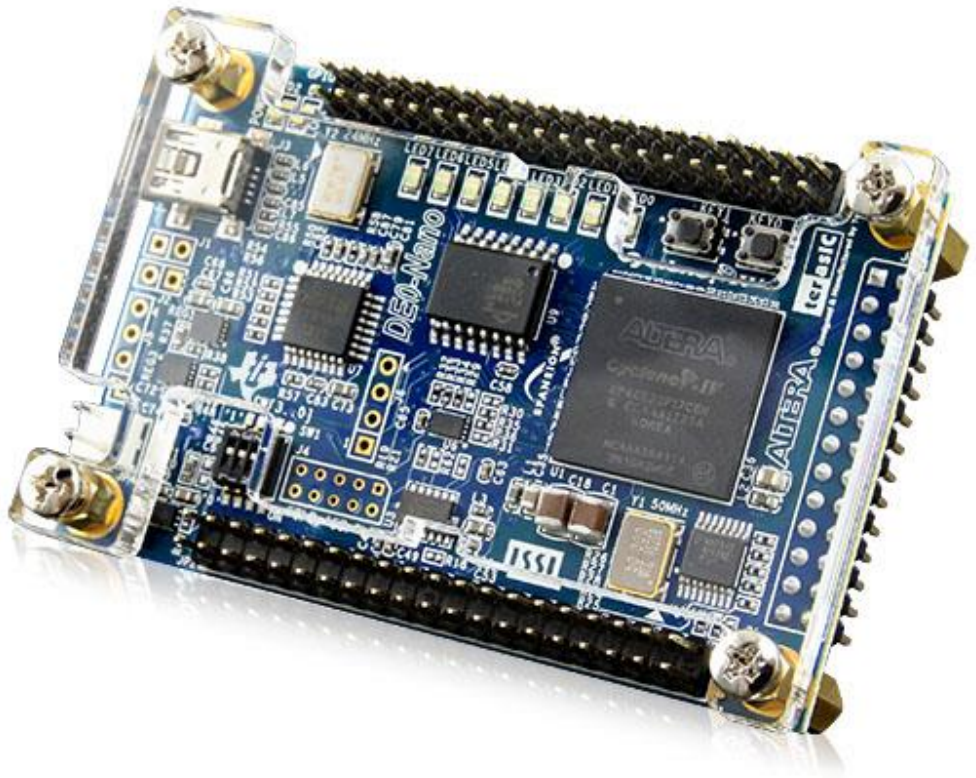
- Step by step towards open toolchain
- Goal is to be able to do reproducible builds, traceable builds

The Cryptech Project

- Verilog (2001) for all FPGA cores
  - Functional models in C, Python, Verilog
  - Icarus Verilog, Verilator used for simulations, linting
- C, asm, Python, Bash, Make for SW and integration
  - Mainly GCC. Some Clang/llvm for static analysis etc
  - OpenOCD for debug, FW download etc

Terasic DE0-Nano

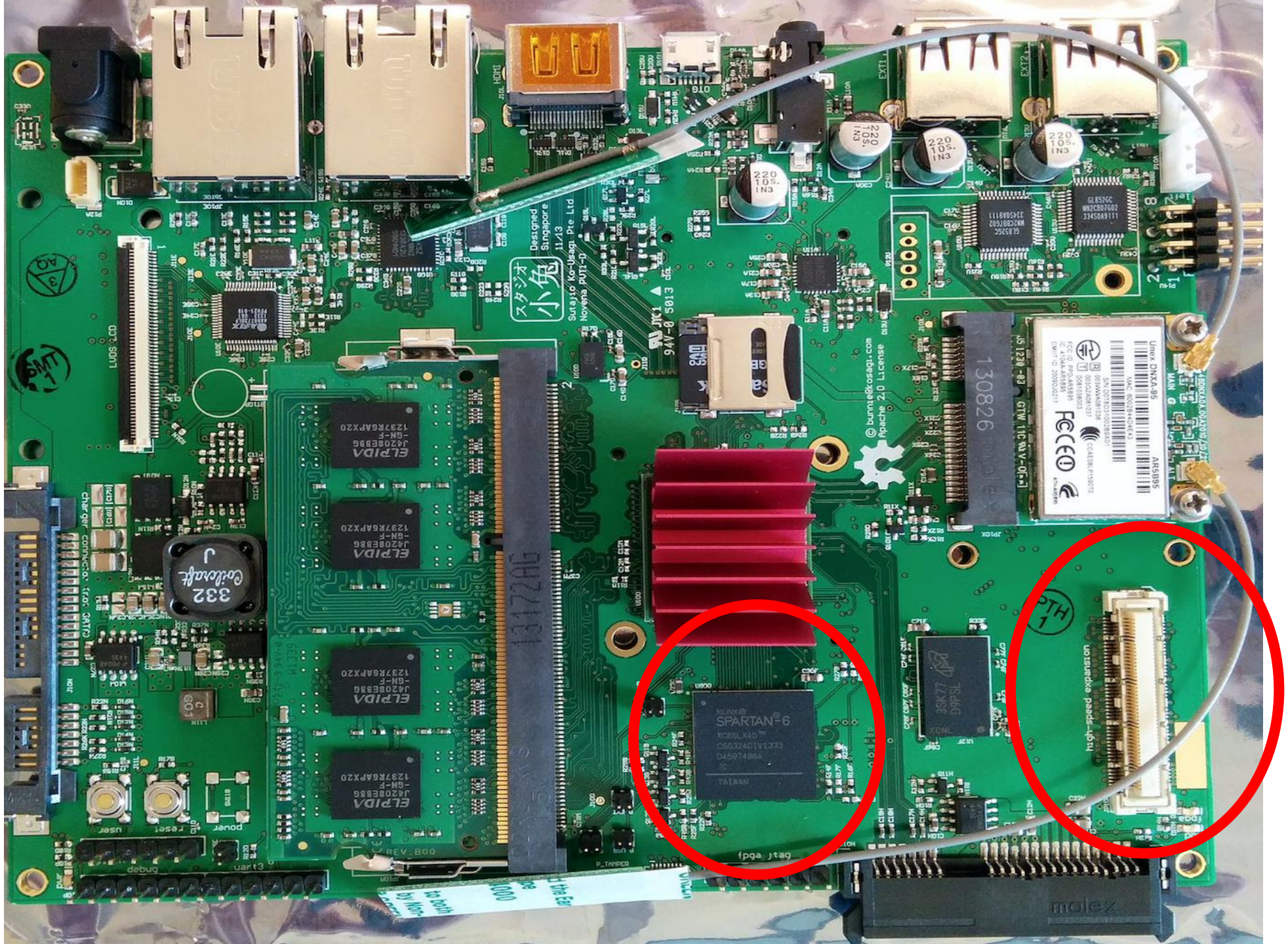
- Very simple, cheap FPGA with Altera/Intel Cyclone device
  - Cheap and easy to use.
  - Used to develop first cores and core
  - Slow and not very open platform
    - Intel/Altera tools required



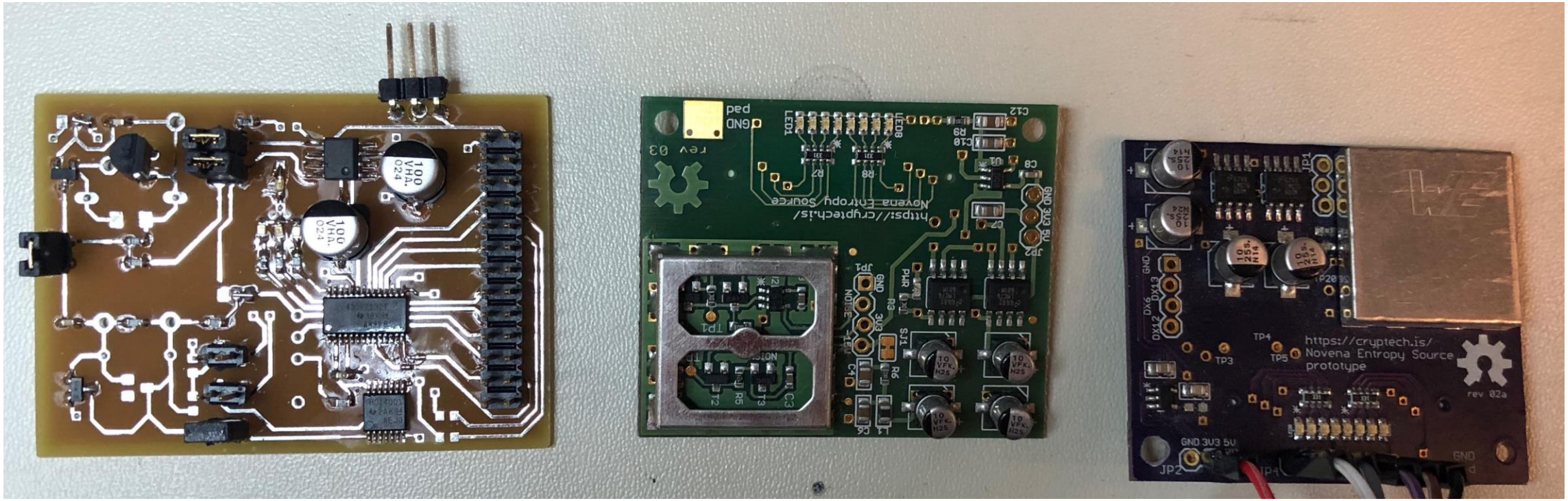
The Novena Open Laptop by Bunnie Huang

- Quad Core Cortex A9 MCU @ 1.2 GHz
- BLOB-free firmware and SW
- Xilinx Spartan-6 FPGA
- **Huge number of interfaces, peripherals**

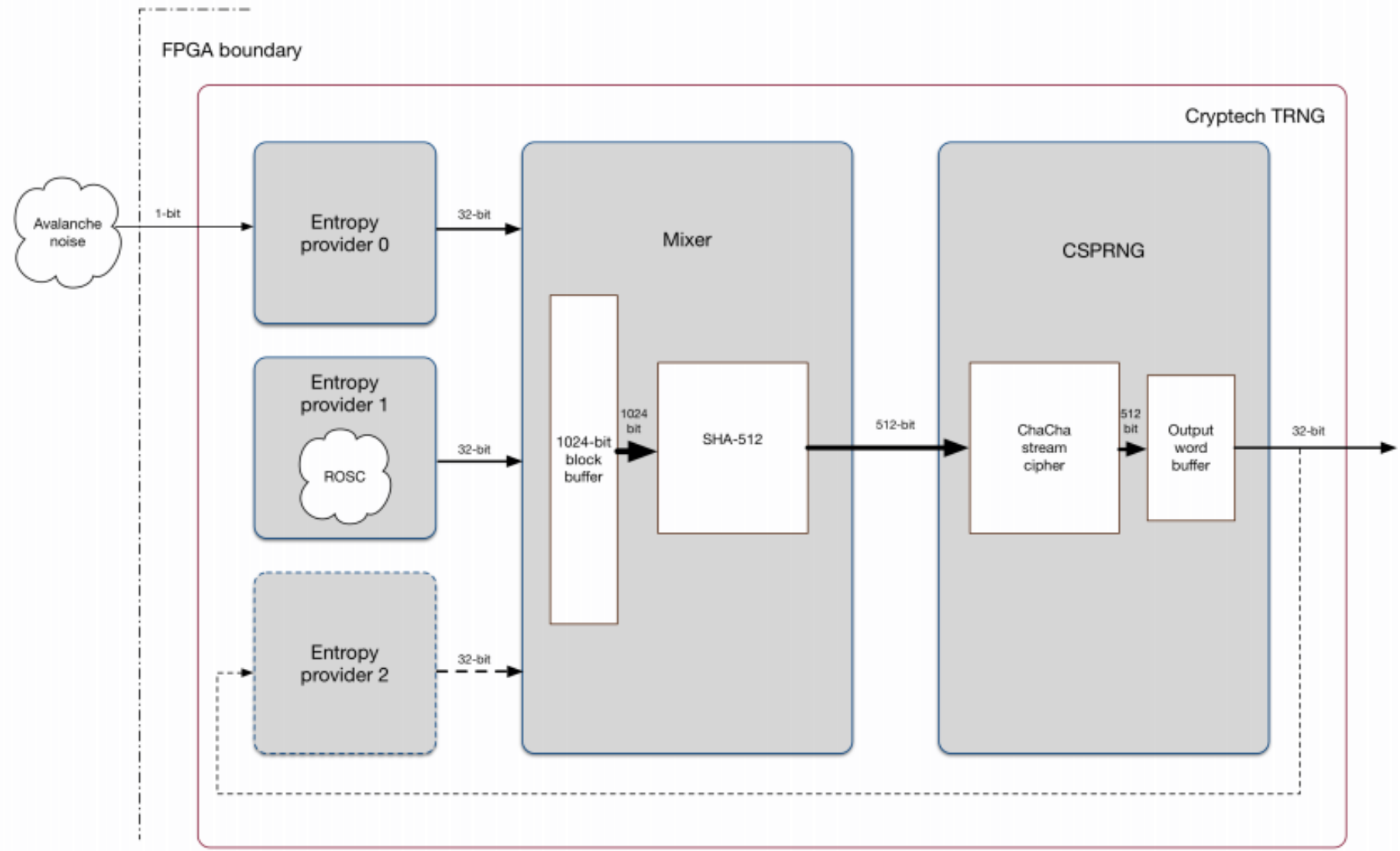
http://www.kosagi.com/w/index.php?title=Novena_Main_Page


SPARTAN-6
fpga jtag
high-speed expansion
debug
uart3
power
reset
user
charger connector (for SATA)
molex

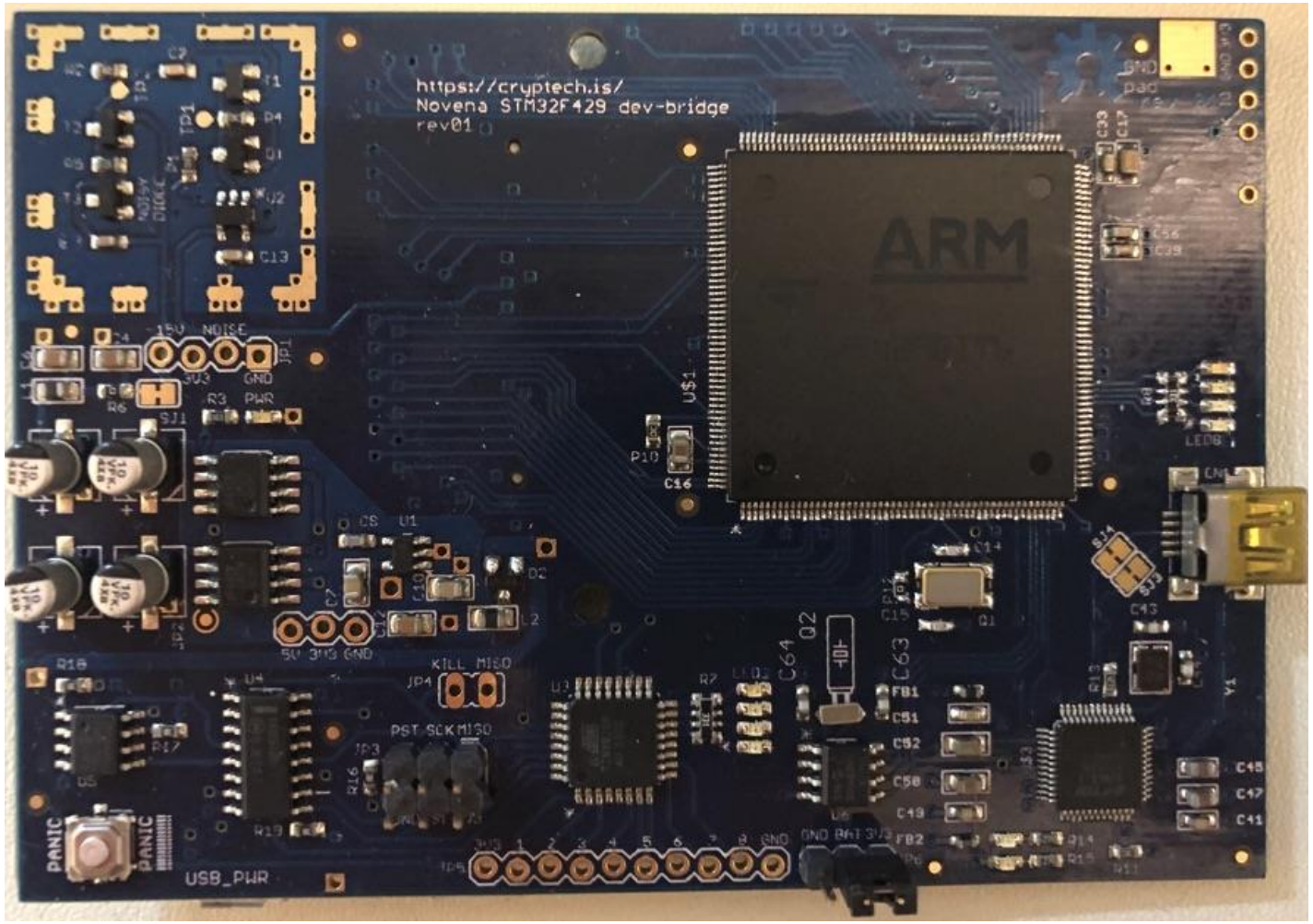
CrypTech Noise Boards



The Cryptech TRNG



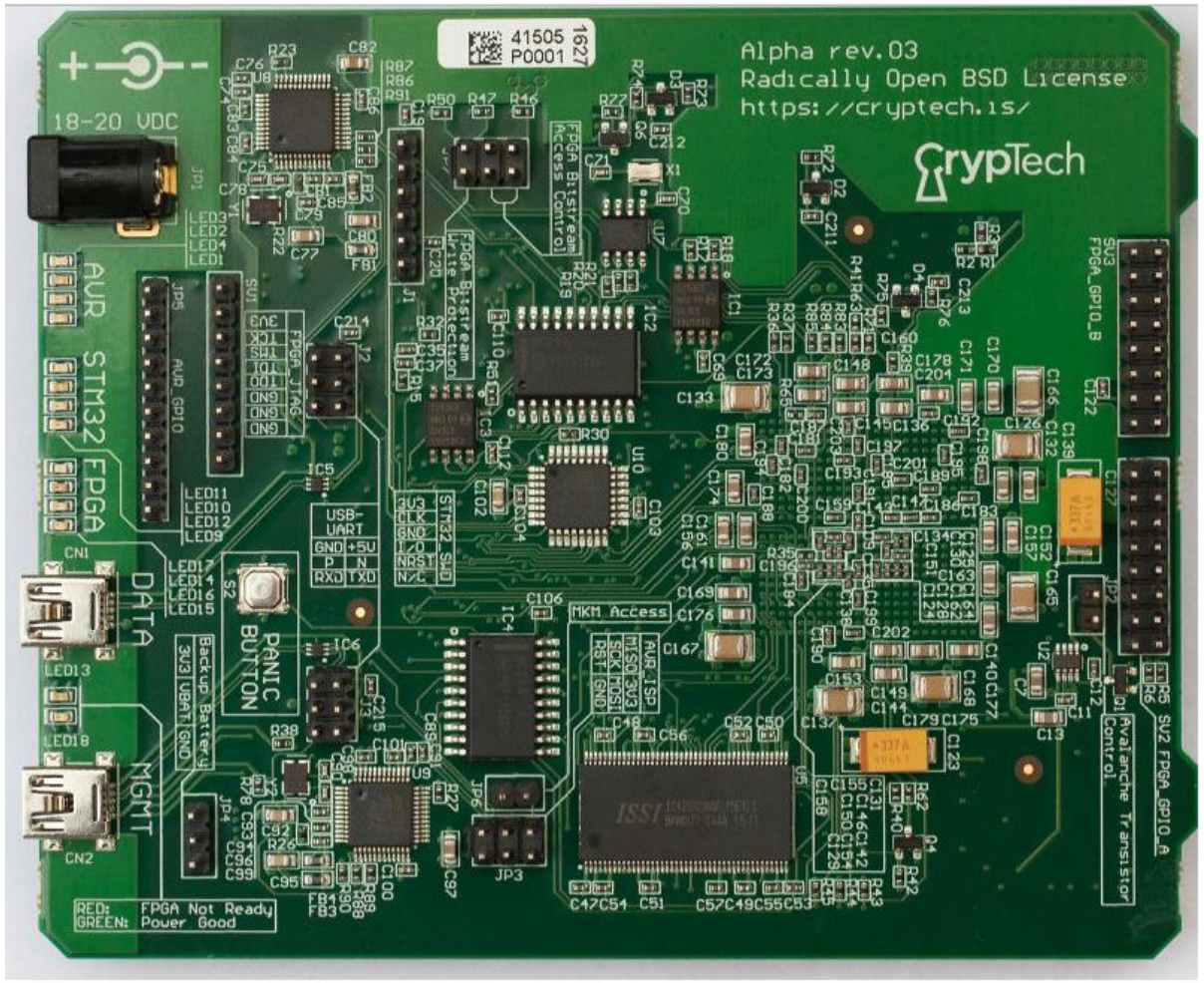
CrypTech Bridge Board



The Cryptech Alpha board

Our current platform

The Cryptech Alpha Board



The CrypTech Alpha Board

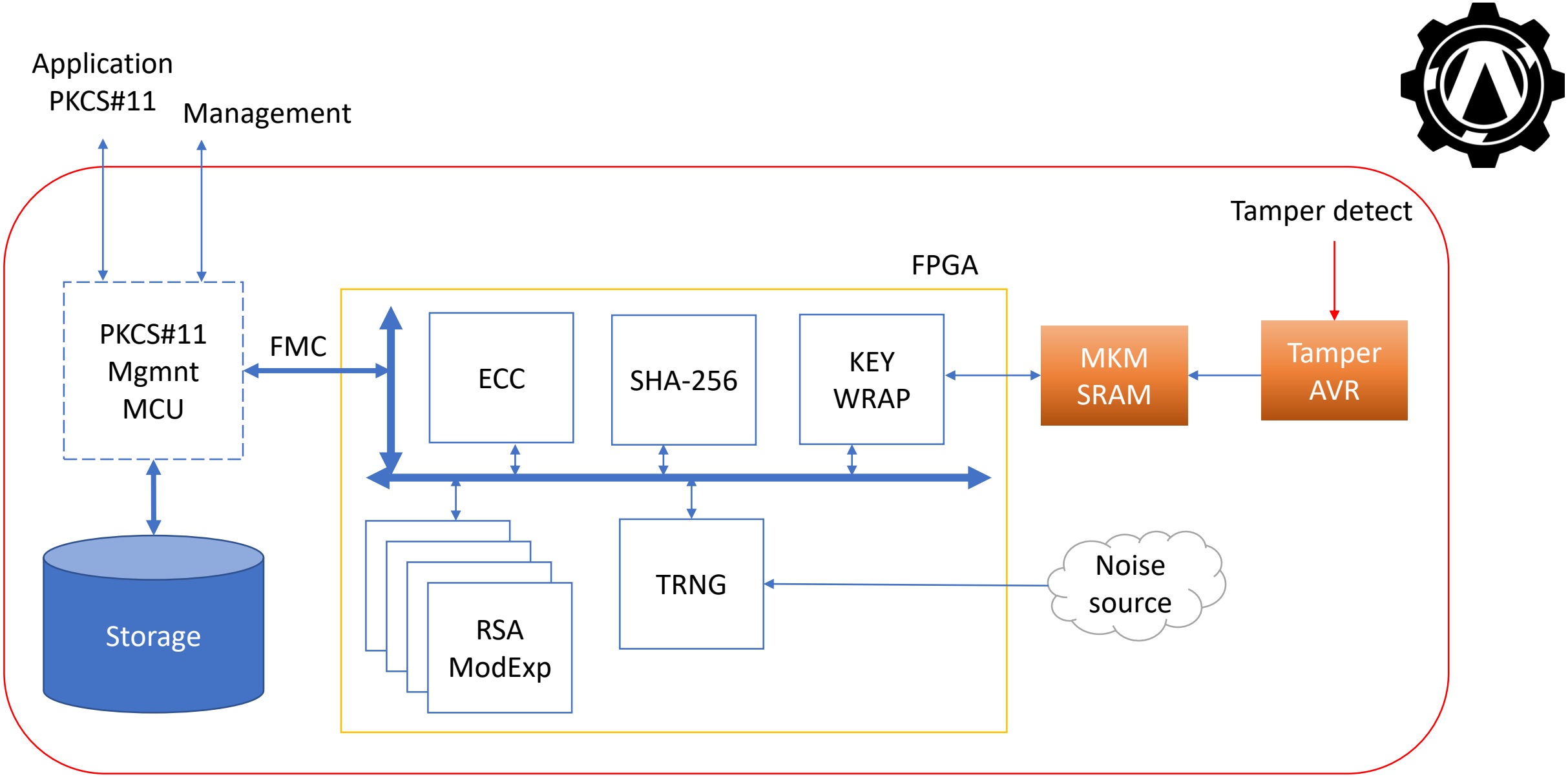
- ARM Cortex M4F based main CPU (STM32F429)
- Xilinx Artix-7 T200 FPGA
- AVR 8-bit MCU for tamper protection

- PKCS#11 and management SW developed by the project
- Comprehensive set of FPGA cores developed by the project
  - RSA, EC, AES, ChaCha
  - SHA-1, SHA-2, SHA-3
  - Keywrap, TRNG
  - SPI master, external interfaces, GPIOs

The CrypTech Alpha Board

- Complete HSM design usable for PKCS#11 applications
  - Usable for people that are used to handle PCBs, like electronics
- Really good random number generator
  - Extensively evaluated (in-house, Cisco etc)
- FPGA development requires tools from FPGA vendor Xilinx
  - Free as in beer, but not open, not auditable
  - FPGA core simulation done using open tools
    - Icarus Verilog, Verilator
- PCB design using commercial tool from Altium
  - Design has been converted to KiCAD after Alpha completion
- All SW developed using open tools
  - GCC, Clang/LLVM, OpenOCD etc

The Xilinx Vivado IDE is 20 GBytes


Application
PKCS#11
Management
Tamper detect
FPGA
PKCS#11
Mgmnt
MCU
FMC
ECC
SHA-256
KEY
WRAP
MKM
SRAM
Tamper
AVR
Storage
RSA
ModExp
TRNG
Noise
source

The CrypTech Alpha Board

- The MCU – FPGA bus FMC is a performance bottleneck
  - Long latency and low capacity (clock speed, data width)
  - All cores are slaves. CPU needs to do R-W to move data (over FMC)

- A lot of crypto functionality still in the MCU
  - Chinese Remeinder Theorem (CRT) for RSA key generation
  - Secrets are exposed in the MCU, secrets move across the FMC

- The MCU is not an open design
  - A lot of kitchen sinks (peripherals, functionality) not needed, not trusted

Performance, security and openess can be improved

Master Key Memories

Your black box has black boxes inside

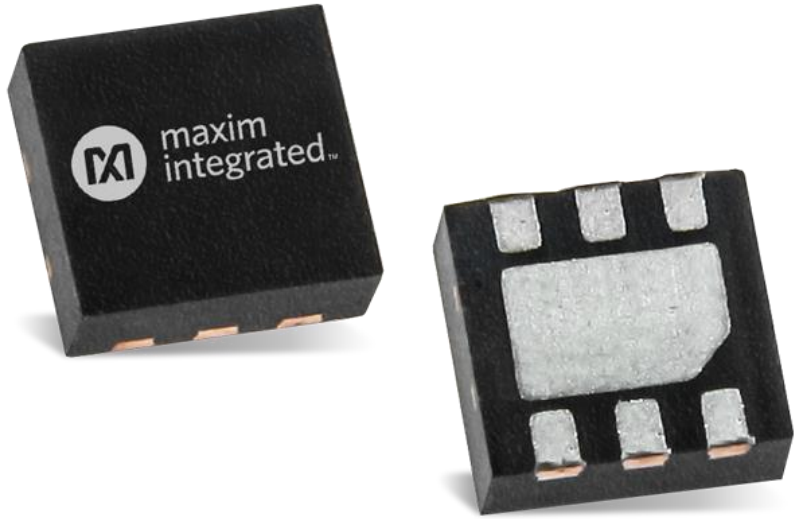
Tamper response, root of trust

- Secrets are stored in flash memory
- Keys in storage are encrypted (wrapped)
  - RFC 5649 AES-KEYWRAP, RFC 5297 AES-SIV-CMAC
- The key used to wrap secrets is called Master Key or Key Encryption Key (KEK)

- Single point of failure – Losing the KEK means that secrets are lost
  - Used to implement rapid tamper response
  - KEK is zeroised when a tamper event is detected
  - Master Key Memory and detection circuit is powered by battery

KEK storage – Security Managers

- Specialized, low power chips
  - BGAs, no external components, internal clocks
- Implements functions for detection of tamper events
  - Switches, Íight sensors, movement, temperature
- RAM based key storage with imprinting, remanence protection
  - Key rotation, key inversion
- Often combined with authentication, root of trust functions
  - HMAC-SHA256 or PKI based
- Commercial devices with few vendors
  - Maxim DeepCover
  - NDAs required, info hard to get
  - **They are black boxes too!**



KEK storage in Cryptech

- The KEK is the key to the protection of stored secrets
  - Having a black box as the fundamental part of the security is **NOT** accepted
- Master Key Memory is a standard, serial SRAM
  - Power supply connected to tamper switches
- Tamper control is a low power, 8-bit AVR processor
  - Can be powered by a battery
  - Tamper FW developed by the Cryptech project using open tools (AVR-GCC)
  - Not very fast, not integrated with the memory – but open

We are working on a much better solution

Cryptech Status

What we do right now

What we will do

Accomplishments 2018

- Performance Improvements
  - Revising and updating implementation to improve performance
  - Steps towards improved security. FPGA implementation of RFC 5649 AES-KEYWRAP

- Hash-based Signatures
  - Implementation of David McGrew's hash-based signature draft: https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs/?include_text=1
  - Quantum resistant signature scheme with potential uses in signing code updates

- Ed25519 HW core
  - Edwards-curve signature algorithm
  - Crypto implementation done, working on drivers
  - Could implement x25519 without a lot of additional effort if needed

Accomplishments 2018

- External Security Code Audit
  - Completed in September of this year
  - Cure53 report is on our website: https://cryptech.is/2018/10/external-security-audit-completed/
  - No critical vulnerabilities
  - Identified vulnerabilities fixed by year-end

Having said that, the results in the cryptographic realm are outstandingly positive. Not only there were no security issues found, but also the overall design has been evaluated as excellent. This especially holds for the *TRNG*, which displays many strengths despite its simple architecture. The testing team is happy to report that the cryptographic aspects connected to the tested items are well under-control.

Ongoing developments

- Performance Improvements
  - Totally new RSA core architecture is being developed (10x – 20x seems possible)
  - Hunting latencies for FPGA – SW communication
    - Endian conversion in SW being moved to HW in the FPGA
      - We can do **memcpy()** now  **Committed last night**
  - Improving FPGA clock speed through floorplanning
    - 100+ MHz

Ongoing developments

- Security improvements
  - Moving SW crypto processing into the FPGA
    - PKCS#11 and management still in the STM32 MCU
  - Adding DMA engine inside FPGA for core – core transfer
    - Eliminate transfer of sensitive data across the FMC bus
  - Reproducible builds for releases
    - MCU, FPGA, Tamper

Open Master Key Memory

- Develop an open MKM, implemented in a FPGA
  - Lattice iCE40 – no external config mem, very lower power consumption
  - BGA device that can be mounted on PCB back to back with main FPGA
  - Active tamper detection with ns tamper response time
  - Zeroisation of KEK with remanence/imprinting protectior
  - **Open toolchain and auditable FPGA bitstream**
  - http://www.clifford.at/icestorm/

Alpha v2, Alpha NG, Beta - something

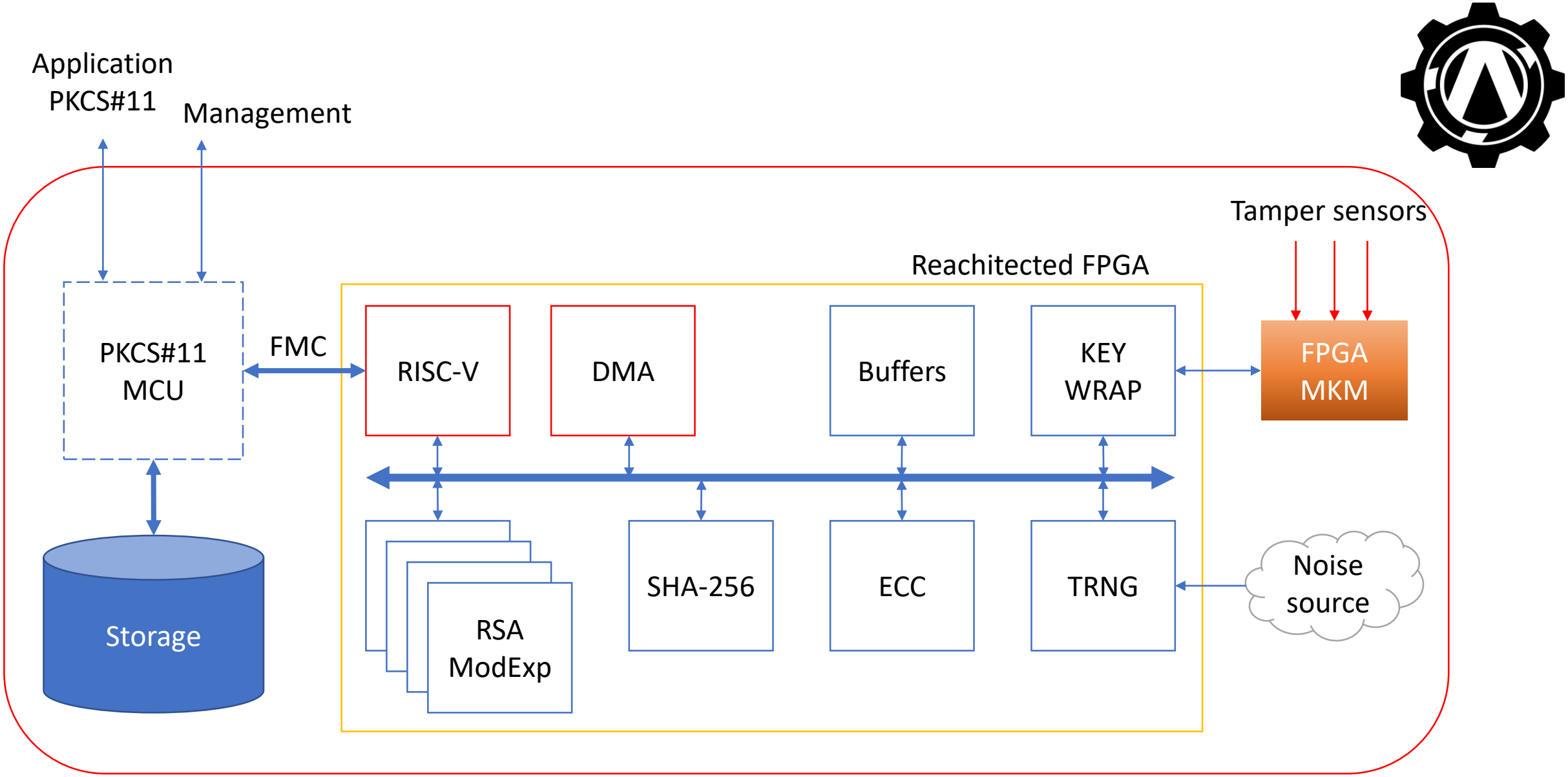
- Integrate the MCU into the FPGA – **using open RISC-V cores**
  - Looking at ***VexRisc*** and Western Digital ***Swerv*** cores
- Rearchitect the FPGA DMA engine to allow core-core transfers
- Integrate new RSA cores when completed
- Integrate FPGA based MKM with no exposed wires to the main FPGA.
- Integrate small **RISC-V** in FPGA based Master Key Memory to add tamper functionality, root of trust (PicoRV32)

Alpha v2, Alpha NG, Beta - something

- Openness Improvements
  - No proprietary MCU – RISC-V is the open future
  - Open Master Key Memory, root of trust
  - We still need use proprietary tools for the main FPGA

- Cost and size improvements
  - Remove several components (the MCU being most costly)
  - Reduce the PCB dimensions
  - Cost reduction probably used to buy FPGA with better speed grade

http://www.clifford.at/papers/2018/nextpnr/slides.pdf - **NextPnR FOSS FPGA Place & Route**
https://symbiflow.github.io/ - **SymbiFlow - open source FPGA tooling for rapid innovation**


Application
PKCS#11
Management
Tamper sensors
Reachitected FPGA
PKCS#11
MCU
FMC
RISC-V
DMA
Buffers
KEY
WRAP
FPGA
MKM
Storage
RSA
ModExp
SHA-256
ECC
TRNG
Noise
source

Cryptech as an open platform

- Diamond-HSM
  - First commercial HSM based on Cryptech
  - Developed, manufactured by Diamond Key Security (DKS)
    - Founded by people from Internet orgs. Focus on Internet infrastructure, research
  - First machines delivered. Used for DNSSEC, Federated Identity Management

- TorHSM
  - Developing dedicated Tor Directory Authorities (DAs) based on the Cryptech Alpha
  - Adding PCIexpress – USB bridge
  - Board 1mm smaller to fit inside a host PC
  - Removing tamper-MCU, current FTDI interface chips, headers, power supply
  - https://trac.cryptech.is/wiki/ExternalProjectsTorHSM

Diamond-HSM™

- Trustworthy Hardware Security Module
  - Low cost, open-source solution utilizing two CrypTech modules for speed and redundancy
  - High entropy, True Random Number Generator (TRNG) for secure cryptography
  - Rugged, tamper-resistant housing
- 1U 19” rack-mountable network appliance with USB and Ethernet interfaces
- Two (2) embedded CrypTech modules
- PKCS#11 API implementation supporting standard applications e.g. OpenDNSSEC and BIND for DNS zone signing for DNSSEC
- Product availability 1H 2019

Thanks to the Cryptech Funders!

вопросы

ASSURED

SECURITY CONSULTANTS

www.assured.se

Tack!

ASSURED

SECURITY CONSULTANTS

www.assured.se