CrypTech Open Source Cryptography Project – 2020 Update

October 2020

Phil Roberts: phil@robertskeys.net

Hardware Security Module

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

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

Hardware Security Module

VPN

E-commerce

Certificates

RPKI

DNSSEC

TLS

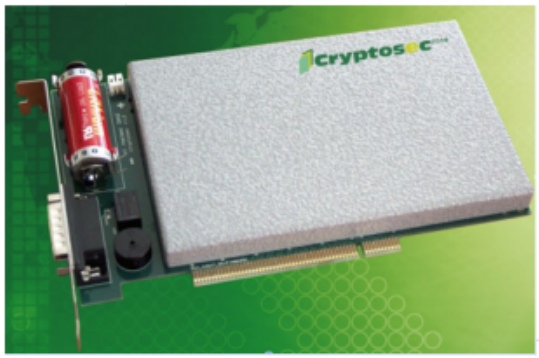
E-gov

Gaming

Banking

Where Keys Go to Hide

Many Flavors and Sizes



CrypTech Project

- Multi-year effort to move towards an open HSM platform developed using open, auditable, and trustable tools
- Started at the suggestion of Russ Housley, Jari Arkko, and Stephen Farrell 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 a signer suitable for DNSsec”
- Reasonable assurance of being open:
  - Core team from Sweden, Russia, USA, Germany, Japan, and Ireland
  - Open development: signed commits to Git repos, etc.

CrypTech Project

- 3-clause BSD license for all SW, FPGA code
  - All cores for crypto acceleration in HW (AES, SHA-256, RSA, EC)
- Creative commons for all documents
  - PCB layouts, BOMs

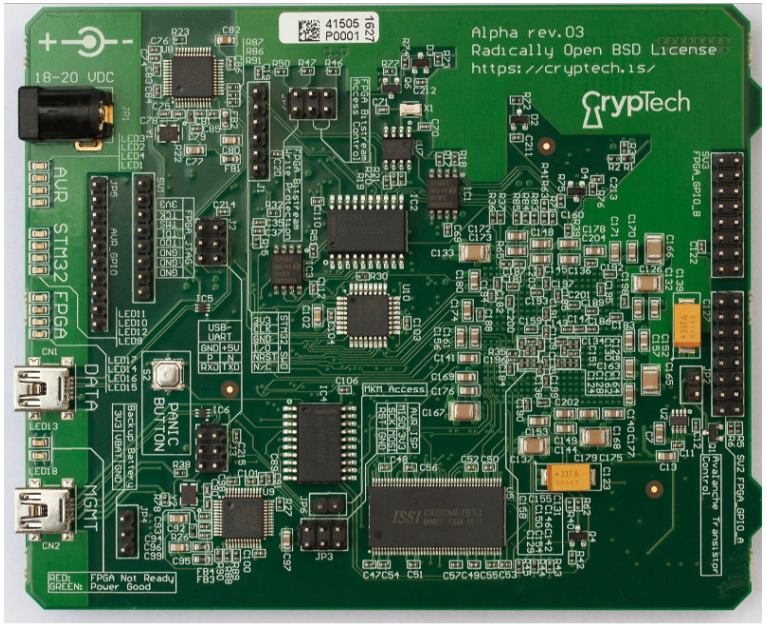
- Repos accessible via trac: https://trac.cryptech.is
- Maillists: https://trac.cryptech.is/wiki/MailingLists

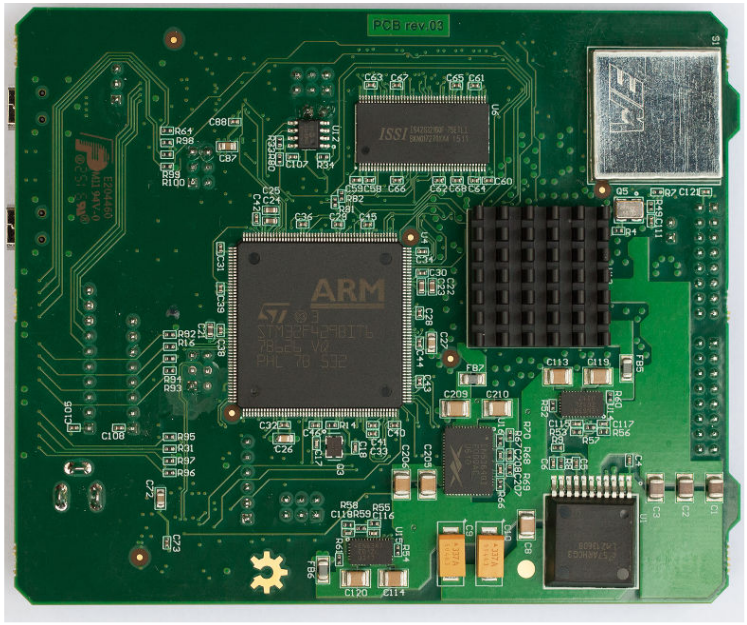
- Step-by-step towards an open toolchain
- Goal is to be able to do reproducible builds, traceable builds

CrypTech: Thanks to our Funders:

DuckDuckGo

CrypTech Alpha Board





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 software developed by the project
- Comprehensive set of FPGA cores developed by the project
  - RSA, EC, AES, ChaCha
  - SHA-1, SHA-2, and SHA-3
  - Keywrap, TRNG

DNSsec use case

- DNSSEC signer
  - Works with OpenDNSSEC, BIND, Knot, and PowerDNS
  - Supports both RSA and EC
  - Available soon as a product offering through Diamond Key Security

CrypTech Resources

- Website: https://cryptech.is
- Wiki: https://trac.cryptech.is/wiki
- Git repositories: https://trac.cryptech.is/wiki/GitRepositories
- Mailing lists: https://trac.cryptech.is/wiki/MailingLists
- CrowdSupply for buying Alphas: https://www.crowdsupply.com/cryptech

Project Accomplishments

- Open Source Hardware and Software Published
  - RSA signing mains the main use case (80 sigs/sec RSA-2048) (part of ARIN grant)
  - Release 4 of the software just became available
- 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
  - Edwards-curve signature algorithm
  - Crypto implementation done, working on drivers
  - Could implement x25519 without a lot of additional effort if needed

2018 Accomplishments

- 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 were fixed by year-end

The results in the cryptographic realm are outstandingly positive. Not only were there 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.

Open Master Key Memory

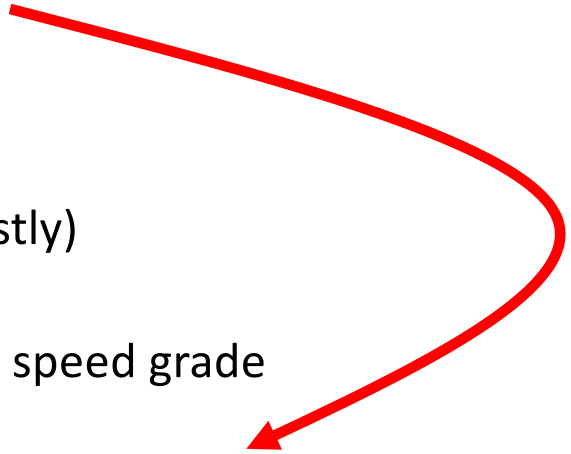
- Develop an open MKM, implemented in a FPGA
  - Lattice iCE40 – no external config mem, very lower power consumption
  - BGA device that can be mounted on PCB back to back with main FPGA
  - Active tamper detection with ns tamper response time
  - Zeroisation of KEK with remanence/imprinting protectior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

Alpha v2, Alpha NG, Beta - something

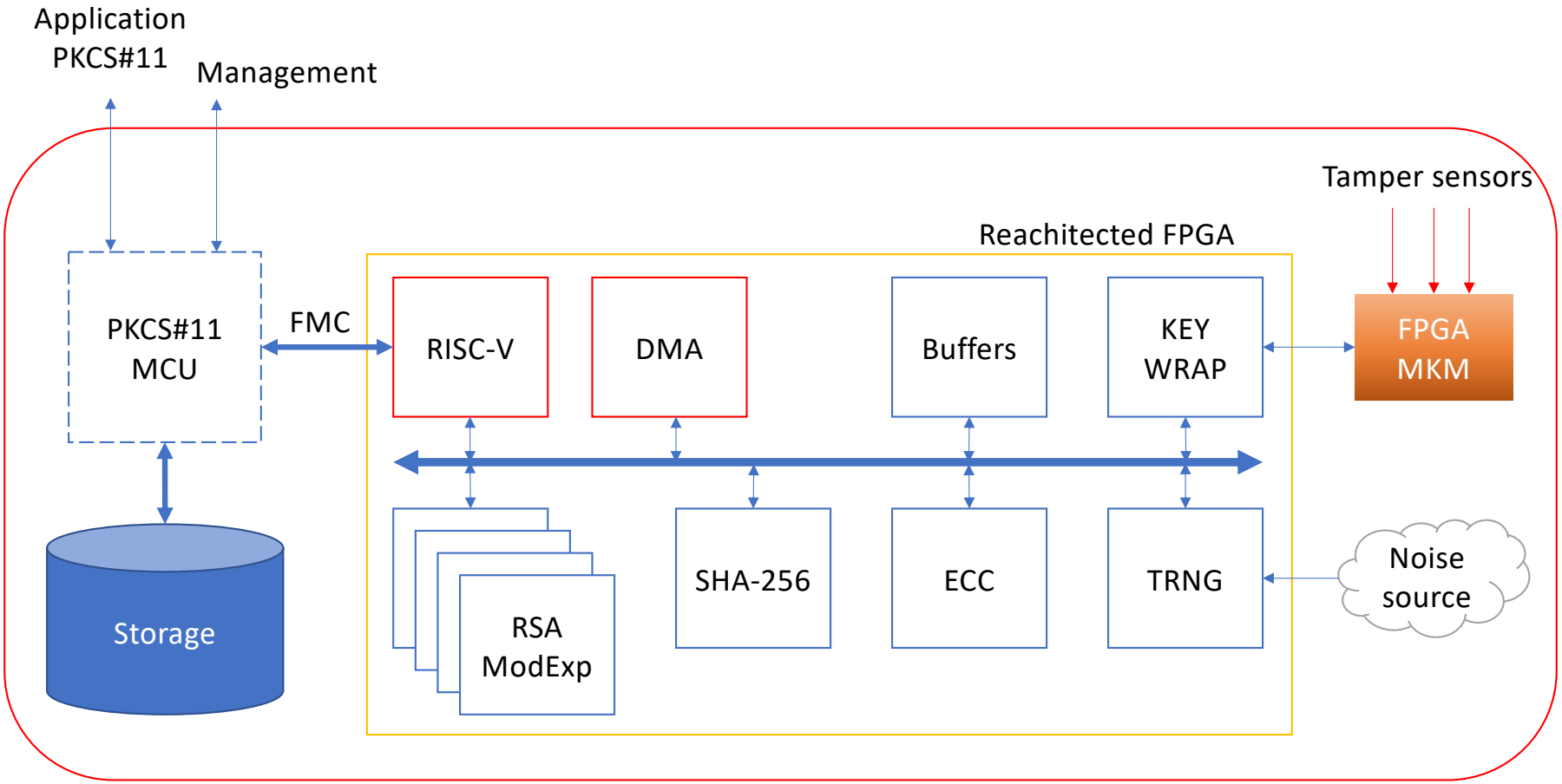
- Integrate the MCU into the FPGA – **using open RISC-V cores**
  - Looking at ***VexRisc*** and Western Digital ***Swerv*** cores (delayed)
- Rearchitect the FPGA DMA engine to allow core-core transfers (in progress)
- Integrate new RSA cores when completed (done)
- Integrate FPGA based MKM with no exposed wires to the main FPGA (done)
- Integrate small **RISC-V** in FPGA based Master Key Memory to add tamper functionality, root of trust (PicoRV32) (in progress)
- Board designs moved to KiCAD (done)
- Ready for new prototype board run (funding)

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

CrypTech thanks the ARIN community for its support!

October 2020

Phil Roberts: phil@robertskeys.net