CrypTech Open Source Cryptography Project – 2021 Update

October 2021

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

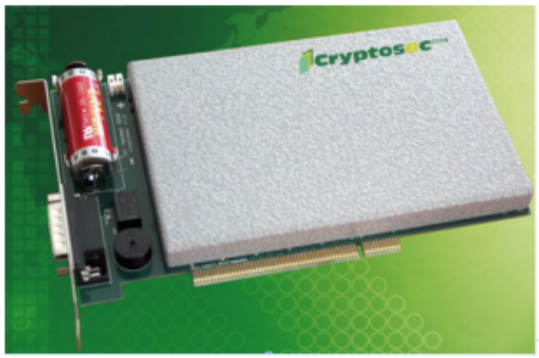
E-gov

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.

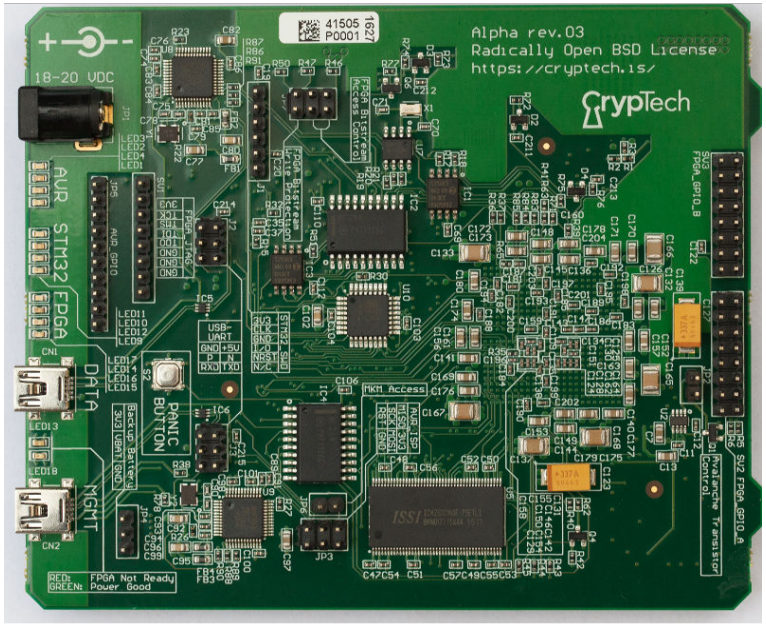
CrypTech Project

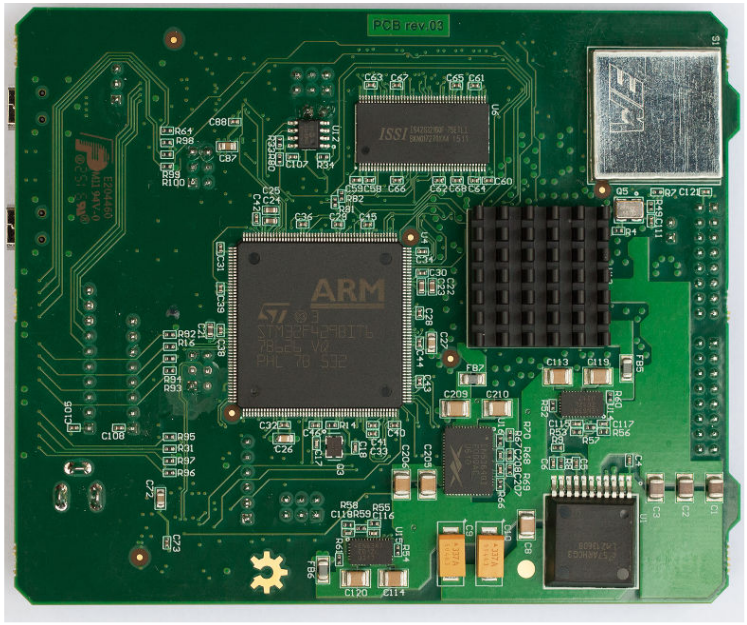
- 3-clause BSD license for all SW, FPGA code
  - All cores for crypto acceleration in HW (AES, SHA-256, RSA, EC)
- Creative commons for all documents
  - PCB layouts, BOMs

- 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 Alpha Board





Project Accomplishments

- Open Source Hardware and Software Published
  - RSA signing remains the main use case (80 sigs/sec RSA-2048) (part of 2020 ARIN grant)
  - Release 4 of the software, will be updated when testing of new board design is complete
- 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
- External Security Code Audit
  - Cure53 report is on our website: https://cryptech.is/2018/10/external-security-audit-completed/
  - No critical vulnerabilities

2020-21 Accomplishments

- There seems to be some kind of virus going around….
- Board designs moved to KiCAD and verified
- New board design complete (new MKM, new FPGAs, tighter security embedded in the physical layer)
- 6 new prototype boards fabricated, debugging in progress
- Testing is underway on new components

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 small **RISC-V** in FPGA based Master Key Memory to add tamper functionality, root of trust (PicoRV32) (in progress)

CrypTech: Thanks to our Funders:

DuckDuckGo

CrypTech thanks the ARIN community for its support!

October 2021

Phil Roberts: phil@robertskeys.net