Why sponsor CrypTech?

the DNS perspective

What is cryptech.is?

The Snowden and subsequent revelations have called into question the integrity of some of the implementations of basic cryptographic functions and of the cryptographic devices used to secure applications and communications on the Internet. There are serious questions about algorithms and about implementations of those algorithms in software and particularly in hardware. The algorithmic issues are in the domain of cryptographic research, but we must also address the implementation issues that have arisen.

To fill this need the cryptech.is project is developing an open-hardware and open source cryptographic hardware engine design that meets the needs of high assurance Internet infrastructure systems that rely on cryptography. The open-hardware and open source cryptographic engine will be of general use to the wider Internet community, covering needs such as securing email, web, DNSsec, PKIs, etc.

Why should a TLD care about cryptech?

The introduction of DNSSEC and the signing of the root zone almost 5 years ago meant that key management became a part of the operational considerations of most TLDs. In some cases TLDs have even begun to consider trust management as part of their business development strategy.

Multiple studies and surveys of the Internet have shown that there is ample room for improvement in the global deployment of technologies such as TLS, RPKI and DNSSEC. This means that trustworthy key management is going to become even more of an issue than it is today, and for even more organizations.

With wider adoption of DNSSEC, it also becomes possible to enable other forms of technical trust using DNSSEC as a foundation (eg DANE) and even though DANE has been largly abandoned for use on the web, its becoming more wide spread for other in other applications.

As DNSSEC is becoming an important foundation for trust, the practice and policies applied to key management for DNSSEC below the TLD will become more important and will be subject to scrutiny by relying parties. This change presents an oportunity and a challenge for a TLD: how to help your customers ”level up” their key management operations in order to be able to support new applications.

One important aspect of key management is the use of HSMs as bearers of cryptograpic key material. The problems involved in deploying the leading commercial HSMs is mostly one of *trust* and *cost* , but not always in that order.

Do you trust your HSMs?

The commercial market for HSMs is exceedingly small. Only a handful of vendors – most in countries in the five eyes community, control the entire market which has seen several M&As lately. Anyone who wants to deploy an HSM today is thus left with very few options.

Recently (and independently from the Snowden revelations) some have come to question the trustworthyness of a closed platform HSM but to date there has not been an alternative for high-assurance applications. The cryptech.is reference design has the potential to change that by making it possible for almost anyone to buy or build an HSM that has been developed in a completely open and transparent way.

Can your customers afford an HSM?

A typical HSM that can support high performance signing, costs around 10k-30k USD. With the need for redundancy and backup this quickly becomes a forbidding cost for many organizations.

The cryptech.is reference design will make it possible for new vendors to enter the HSM market by elliminating the development costs. These vendors will base their product on a completely open design and will therefore be much better placed to deliver higher quality at a much lower price point.

The cryptech.is design can be built and sold at a fraction of the cost of current HSM solutions. The ”build it yourself” HSM is however not just a question of cost but also one of trust.

Budget & Timeline

The project is currently one year into a 2-3 year arc with the aim to develop a reference architecture and a prototype HSM implementing this architecture. All results are published under BSD or Creative Commons license (as applicable).

The **total budget** is estimated at around **2M USD**. The project is being run using agile project management methods and planning is done continuously. The project dashboard page [https://wiki.cryptech.is/wiki/Dashboard] reflects the current state of work and can also serve as a point of reference for specific work items of possible interest to sponsors. Currently the **monthly operating cost** for the project is around **50-70k USD**.

We solicit sponsorship and collaborative funding up to a maximum of 100k USD per donor per year as the project is trying to avoid any one sponsor having too much influence over the project. We gladly accept any amount either as a one-time or recurring donation.

Why is this so expensive?

The cryptech.is project is trying to produce a complete and fully tested design for an HSM. Among other things, this involves establishing trust in the implementations of cryptographic functions such as true random number generators (TRNG), digital signature algorithms and stream ciphers as well as technical controls such as tamper detection, master key

protection etc.

In order to establish ultimate trust in the deliverables, the project cannot rely on (say) the AES implementation bundled with a CPU but must implement all such functions from scratch. In order to reduce the attack surface of the HSM, most cryptographic functions are executed inside a Field Programmable Gate Array (FPGA). Implementing cryptographic primitives in an FPGA is both hard and expensive but the end result should be both secure and highly trustworthy.

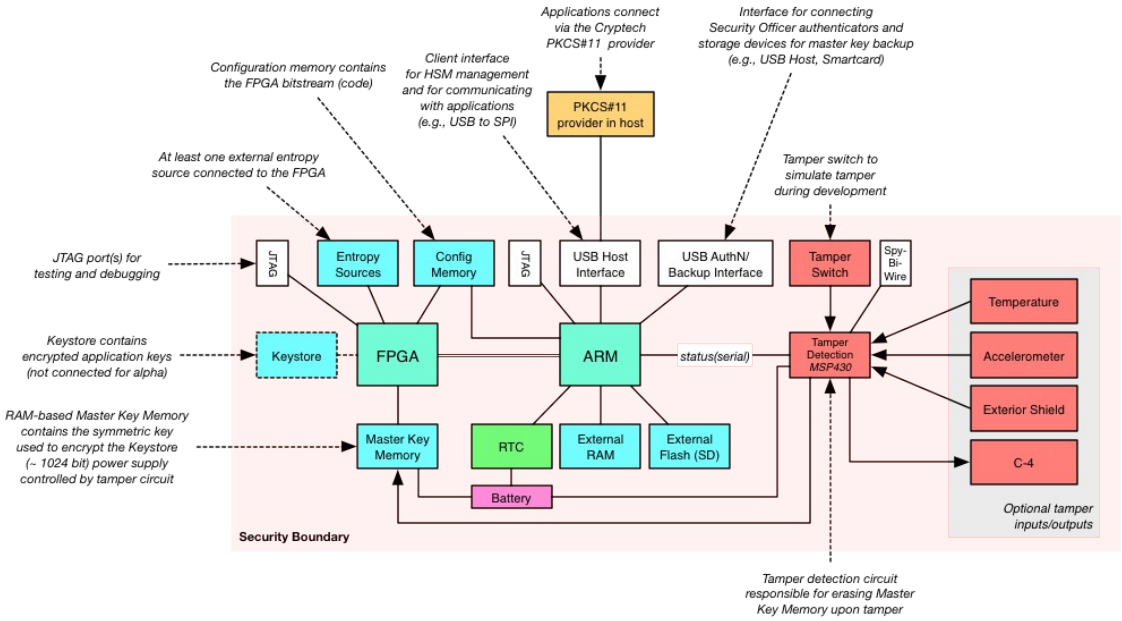
In order to further increase trust in the project deliverables, the project is making an effort to be culturally and geographically diverse, This means engaging FPGA programmers, software developers, electronics designers from different parts of the world and with different backgrounds. The core team today includes individuals from the United States, Sweden, and Russia, and this of course contributes to increase overall project costs.

Designing an HSM in this way is expensive but will hopefully yield a design that can support even the most sensitive applications.

We need your support!

The cryptech.is project is a major undertaking which requires access to experts in electronics, trust management, application integration, embedded systems design, FPGA programming etc making this a non-trivial and a much more expensive undertaking than (say) producing a library of cryptographic functions to be run on a general purpose computer.

In order to become a success, the cryptech.is project needs your help and support! With support and funding the project can deliver a foundational component which will help reestablish trust in some of the most important parts of Internet infrastructure.


Applications connect via the Cryptech PKCS#11 provider
Interface for connecting Security Officer authenticators and storage devices for master key backup (e.g., USB Host, Smartcard)
Configuration memory contains the FPGA bitstream (code)
Client interface for HSM management and for communicating with applications (e.g., USB to SPI)
PKCS#11 provider in host
At least one external entropy source connected to the FPGA
Tamper switch to simulate tamper during development
JTAG port(s) for testing and debugging
JTAG
Entropy Sources
Config Memory
JTAG
USB Host Interface
USB AuthN/ Backup Interface
Tamper Switch
Spy-Bi-Wire
Temperature
Accelerometer
Exterior Shield
C-4
Keystore contains encrypted application keys (not connected for alpha)
Keystore
FPGA
ARM
status(serial)
Tamper Detection MSP430
RAM-based Master Key Memory contains the symmetric key used to encrypt the Keystore (~ 1024 bit) power supply controlled by tamper circuit
Master Key Memory
RTC
External RAM
External Flash (SD)
Battery
Optional tamper inputs/outputs
Security Boundary
Tamper detection circuit responsible for erasing Master Key Memory upon tamper