Cryptech Project Status: Alpha Board

https://cryptech.is/

CFRG
Berlin
July 2016

Overview

- First development board complete, available for testing
- All open source: board design, firmware, software, soup to nuts
- Composable firmware: mix and match, build what you need
- International design team, not just the usual suspects
- Workshop just prior to IETF 96, testing DNS zone signing
- Pre-built boards and pre-built binaries are available...
- But it's *all* open source, build your own if you like

What This Is And Is Not

- This is not an HSM (no tamper envelope, sensors, . . .)
- This is a development environment for building an HSM
- Think of this as an open source “demo board” for HSMs

Principal Hardware Features

- Custom noise circuitry (noisy diode, “ARRGH” circuit)
- Honking big (XiLinx Artix-7) FPGA
- Cortex M4 ARM CPU
- AVR ATtiny828 MCU (tamper circuit controller)
- High speed USB UARTs (small attack surface, USB outside conceptual security perimeter)
- Flash for firmware (FPGA and CPU) and for keystore
- RAM for working memory and battery-backed Master Key Memory
- “Eurocard” form factor

Algorithms Currently Supported

- RSA (1024–8192 bit), ECDSA (P-256, P-384, P-521)
- SHA-1, SHA-2, HMAC, PBKDF2
- AES-Keywrap
- TRNG uses SHA-2 and ChaCha internally
- More on the way

Interfaces Currently Available

- Simple RPC over USB UART
- PKCS #11 library implemented as RPC protocol client
- Management console on second USB UART

Next Steps

Features	Key backup, M-of-N
Algorithms	SHA-3, other curves, AES driver?
Hardware	Better USB, other form factors
Speed	Parallel signing cores, higher clocking

Join Us!

Web site	`https://cryptech.is/`
Mailing list	`tech@cryptech.is`