CrypTech

Cryptech Update (https://cryptech.is)

Phil Roberts

Outline

- Cryptech – what is it?
- Cryptech – why should the community care?
- Status Update – we have alpha boards now!
- Seeking alpha testers
- How can you help?

CrypTech

Cryptech – what is it?

- Open source HSM (hardware security module) reference designs
- Hardware security modules store and manage digital keys and provide some cryptographic processing
- Standalone devices or cards that ride on servers
- Used in, for example, DNSsec, RPKI, PGP, Tor, Enterprise PKI systems, etc.

CrypTech

Cryptech – Why Should the Community Care?

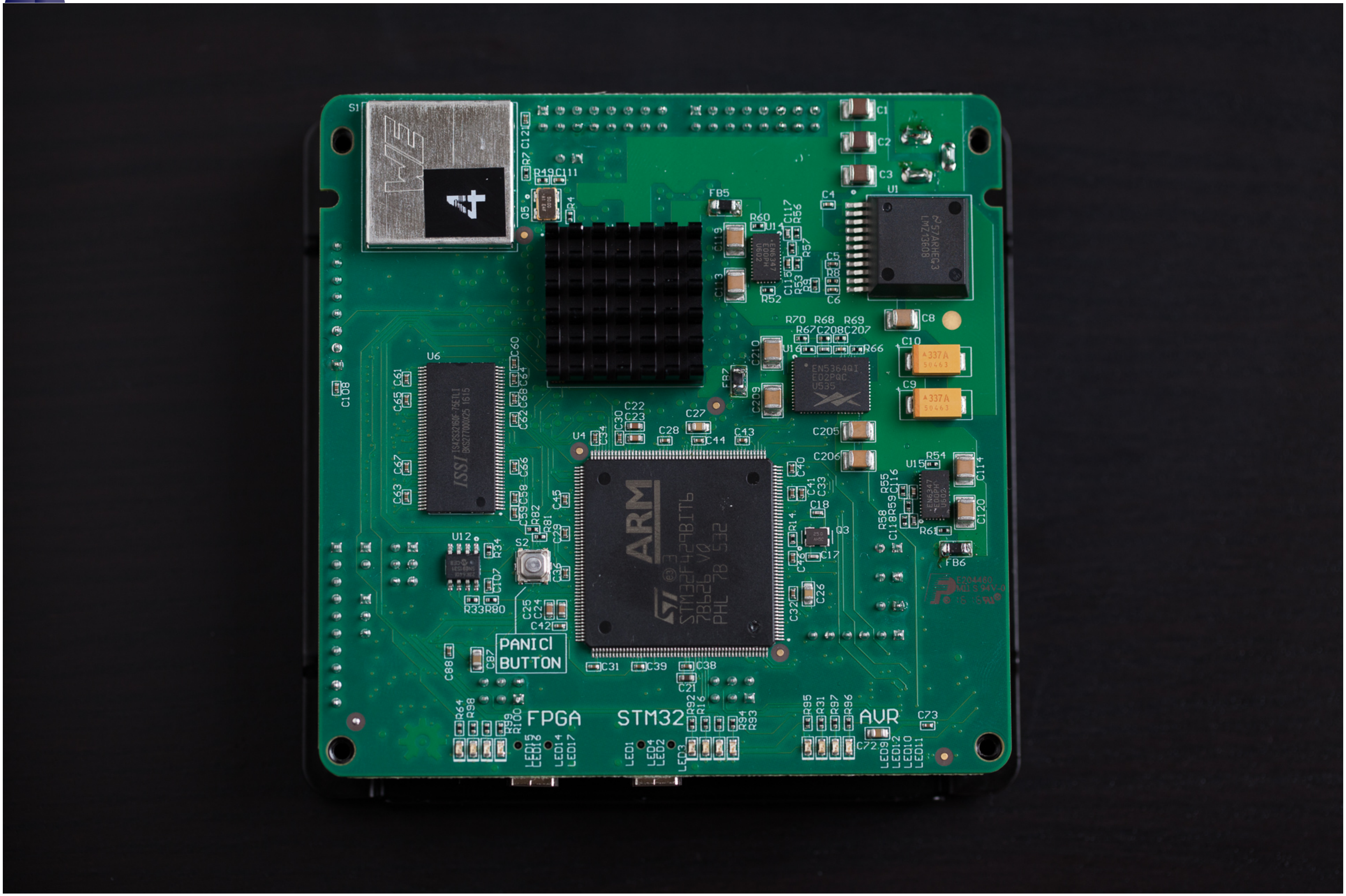
- Concerns about compromised devices in crucial Internet infrastructure – routers, servers, firewalls, etc.
- HSMs protect the most trusted elements in securing communications over the Internet
- Uncertainty about the presence of backdoors in the commercial HSMs available
- Project started to meet the assurance needs of supporting IETF protocols in an open and transparent manner

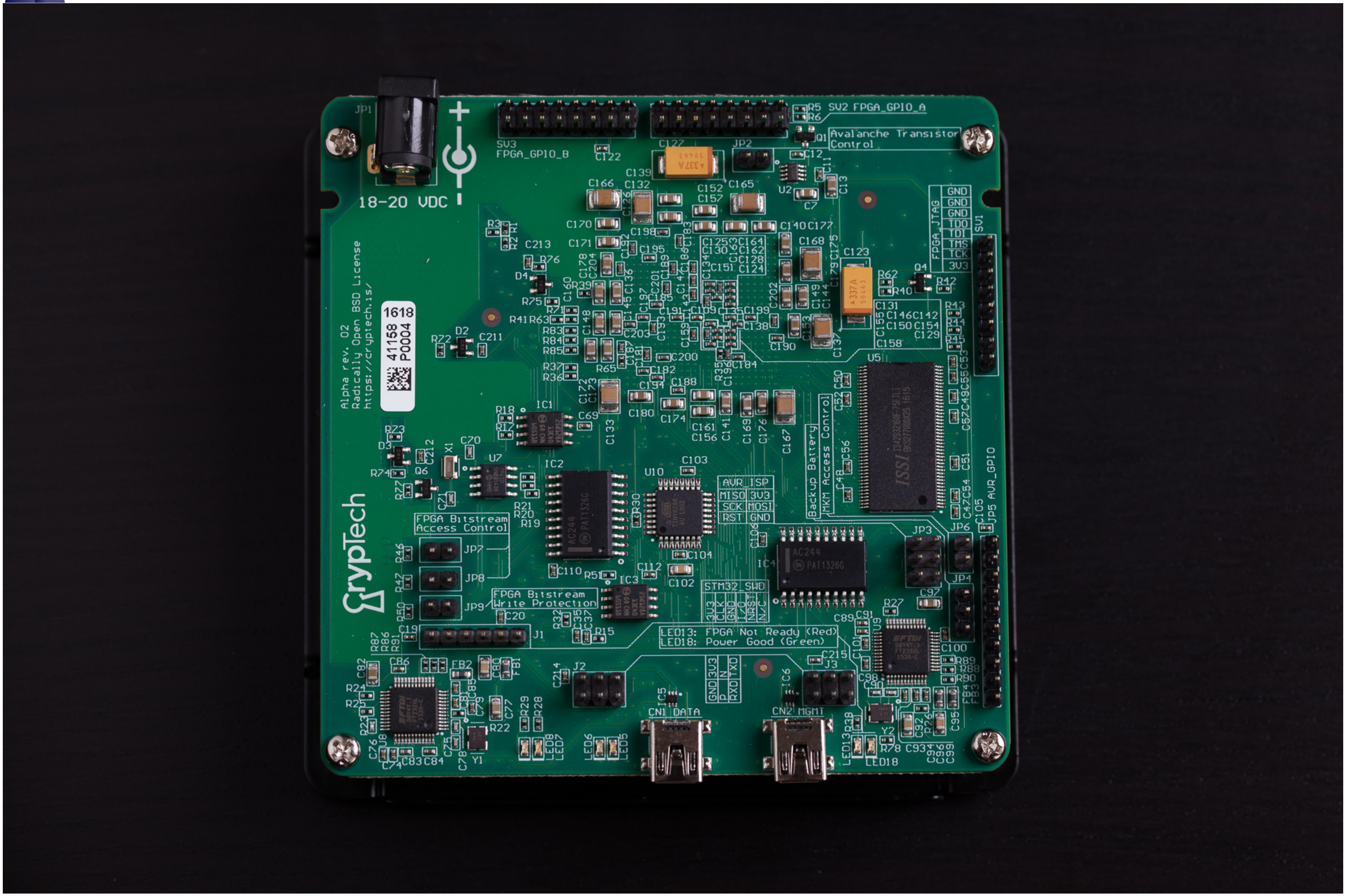
CrypTech

Current Status

- Live alpha boards working!
- Engineering first runs with all major functions verified
- Engineers continuing to test with initial boards
- Ready to create alpha boards for external alpha testing

CrypTech




18-20 VDC
SV3 FPGA_GPIO_B
SV2 FPGA_GPIO_A
Avalanche Transistor Control
FPGA JTAG
GND
GND
GND
TDO
TDI
TMS
TCK
3V3
Alpha rev. 02
Radically Open BSD License
https://cryptech.is/
1618
41158
P0004
CrypTech
Backup Battery
MKM Access Control
AVR_ISP
MISO 3V3
SCK MOSI
RST GND
JP5 AVR_GPIO
FPGA Bitstream Access Control
FPGA Bitstream Write Protection
STM32_SWD
LED13: FPGA Not Ready (Red)
LED18: Power Good (Green)
CN1 DATA
CN2 MGMT

CrypTech

Seeking Alpha Board Testers

- Alpha boards available for external testers this summer
- DNSSEC first
- RPKI soonish
- Looking for folks with implementation and operational experience in these environments to provide additional functional testing

CrypTech

How Else Can You Help?

- Community review (https://trac.cryptech.is/)
- Testing
- Help with documentation
- Business partnership – building eventual product
- $$$

CrypTech

Supporters

Internet Society™

Google

COMCAST

CISCO™

Your Public Interest Registry™

SUNET

SURF NET

Afilias℠

RIPE NCC

afnic

iiS

ICANN

DuckDuckGo