cryptech.is

what why who

alpha board launch - Berlin 2016

https://xkcd.com/525/

What?

cryptech.is is an effort to create an open hardware cryptographic engine and the tools needed to make it trustworthy.

Why?

RFC 7258/BCP 188
Pervasive Monitoring is an Attack

Who?


Internet Society


Google


COMCAST


CISCO


Your
Public Interest
Registry


SURF NET


Afilias

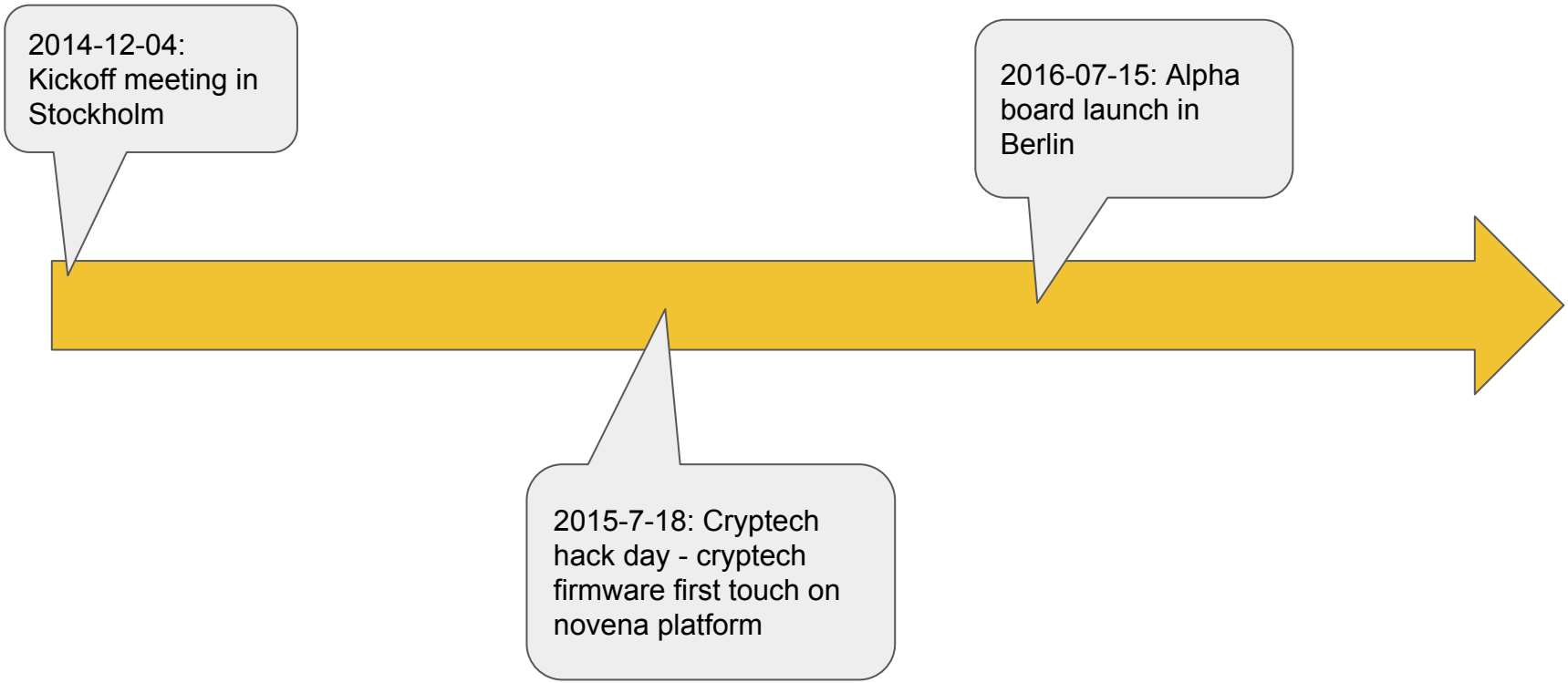

RIPE NCC
RIPE NETWORK COORDINATION CENTRE


afnic

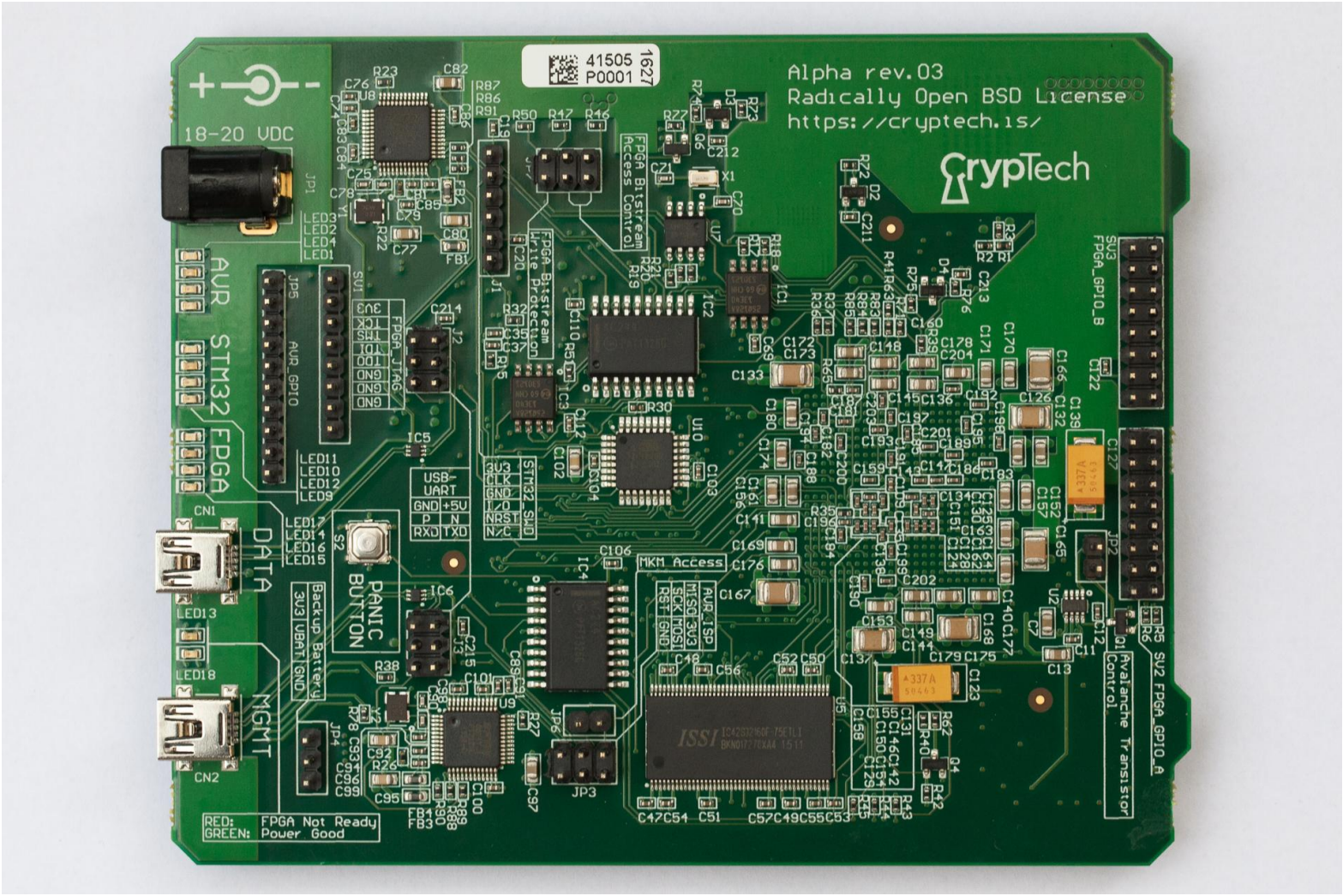

IIS

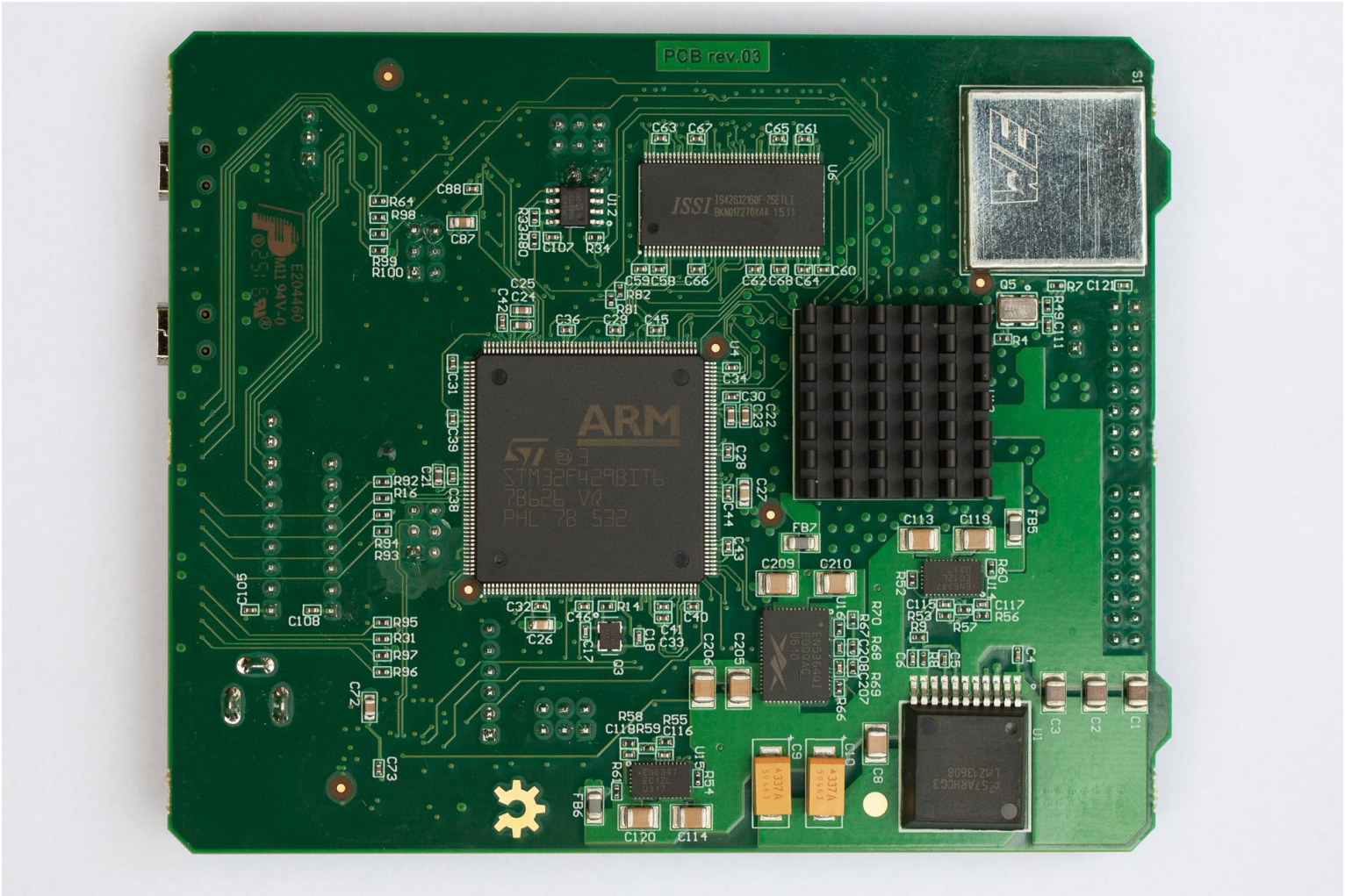

ICANN


DuckDuckGo


2014-12-04: Kickoff meeting in Stockholm
2015-7-18: Cryptech hack day - cryptech firmware first touch on novena platform
2016-07-15: Alpha board launch in Berlin

And now...


41505
P0001
1627
Alpha rev.03
Radically Open BSD License
https://cryptech.is/
CrypTech
18-20 VDC
AVR STM32 FPGA
DATA
MGMT
PANIC BUTTON
MKM Access
Avalanche Transistor Control
FPGA Bitstream Access Control
FPGA Bitstream Write Protection
USB-UART
Backup Battery
RED: FPGA Not Ready
GREEN: Power Good
ISSI


PCB rev.03
ISSI
IS42S32160F-75ETLI
ARM
STM32F429BITb
7B626 V0
PHL 7B 532
E204460
94V-0

https://www.crowdsupply.com/cryptech/open-hardware-security-module

Berlin workshop

Agenda Friday

0830	Coffee
0930	Introductions, setup
1000	Presentation of the cryptech alpha device
	- cryptech overview
	- overall hardware architecture
	- the FPGA
	- HSM software architecture, CLI, and RPC mechanism
	- PKCS11, client-side software, how to configure the board
1100	Break
1130	Hands-on testing
1230	Buffet lunch
1330	Hands-on testing continues
1500	Coffee break
1530	Hands-on testing continues
1700	Finish day one

Agenda Saturday

0900	Hands-on testing continues
1030	Coffee break
1100	Workshop wrap-up
	- outstanding questions
	- feedback from the participants
	- opportunity to articulate what participants will need that isn't readily available
1300	Finish

Some light reading to get you started

- https://trac.cryptech.is/wiki/BerlinWorkshop
  - Agenda for the Berlin workshop
- https://trac.cryptech.is/wiki/BinaryPackages
  - HOWTO setup APT and Homebrew for Cryptech software
- https://trac.cryptech.is/wiki/OpenDNSSEC
  - HOWTO setup an Alpha rev03 to do DNSSEC signing using OpenDNSSEC