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 – 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 – 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

• Project started to meet the assurance needs of supporting IETF protocols in an open and transparent manner
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
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
How Else Can You Help?

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