Cryptech HSM – Preparation Phase

Sprint demo #7– 12th November 2019

Alan Lewis
(on behalf of the Alphas Cryptech HSM team)

Q4 2019

Public

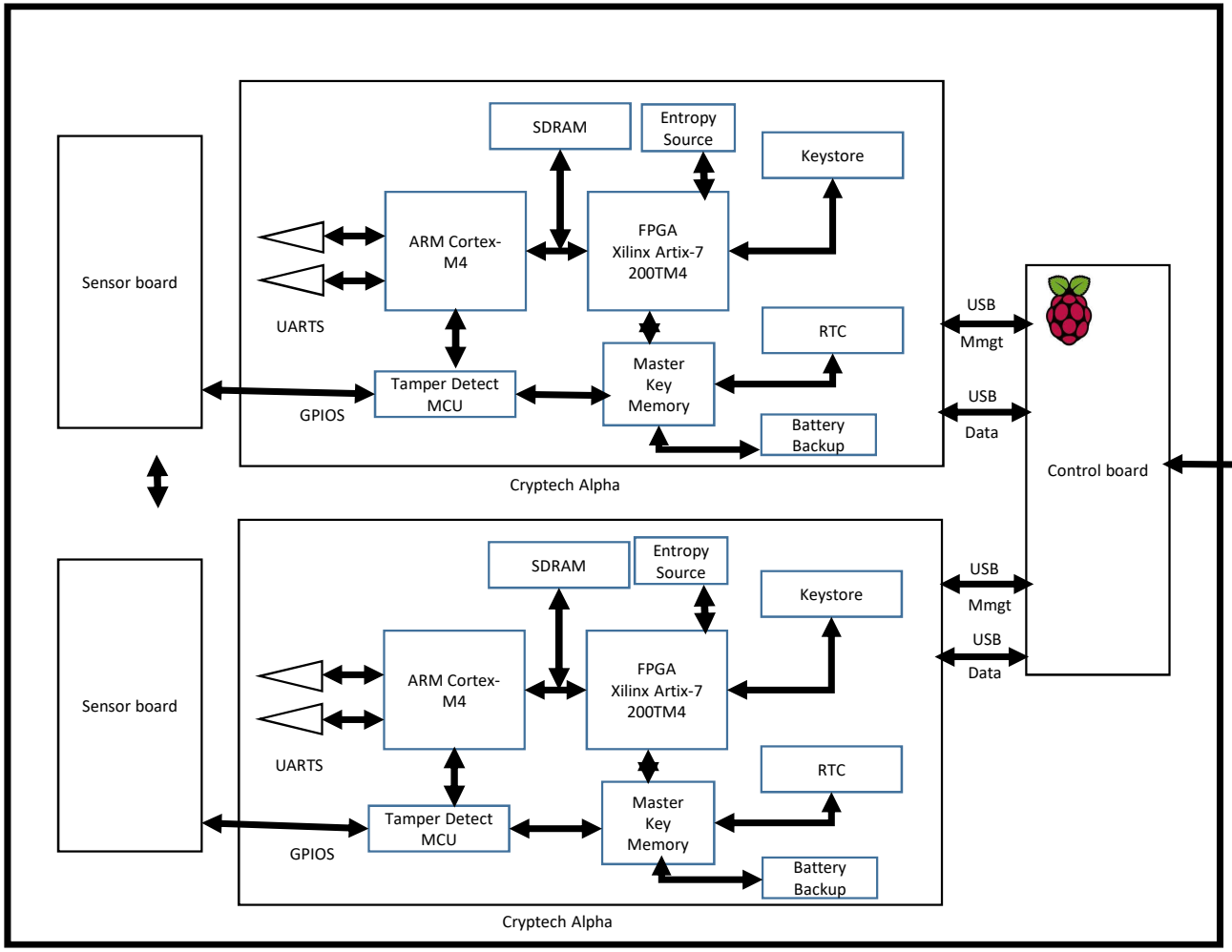
www.geant.org

Background

- Cryptech Project launched in December 2013
  - Aim: Create a reference design for a low-cost, secure, auditable cryptographic engine to:
    - Enable broader use of cryptographic technologies
    - Ensure the technology implementation is trustworthy

- Diamond Key Security launched in 2017
  - Aim: Productise and deliver Cryptech technology to the market to:
    - Deliver a commercial HSM product offering to the market
    - Generate sufficient revenues to sustain the Cryptech project

Diamond Key HSM



- 19 inch Rack mount appliance
- Single board Raspberry Pi Controller
  - Host command interface
  - External ethernet port
  - USB
- 2x Cryptech Alpha crypto modules
  - ARM Cortex-based
  - Entropy-based TRNG
  - FPGA crypto core
  - Battery-backed Master key storage
  - Tamper detect processor (clears MKM)
- 2x Sensor modules
  - Temperature
  - Motion
  - Light
  - Case open

Overview

Investigate the applicability of the Diamond Key (Cryptech) HSM as a low-cost means to maintain and enhance the security of GÉANT and community, services

- Document GÉANT services HSM use cases
- Determine Diamond Key Capabilities
- Identify hosting for Diamond Key Appliances
- Install the Diamond Key appliances
- Identify service teams interested in HSM testing
- Conduct HSM trials in next Incubator cycle

Key Use Case Needs

PKI Key Storage/Signing		Code signing		Document Signing		
eduroam Managed IdP Root Certificate	eduroam Managed IdP Intermediate Certificate	eduroam CAT installer signing	eduroam Managed IdP Installer signing	eduGAIN MDS signing	eduGAIN MDQ signing	eduGAIN FaaS MDS signing

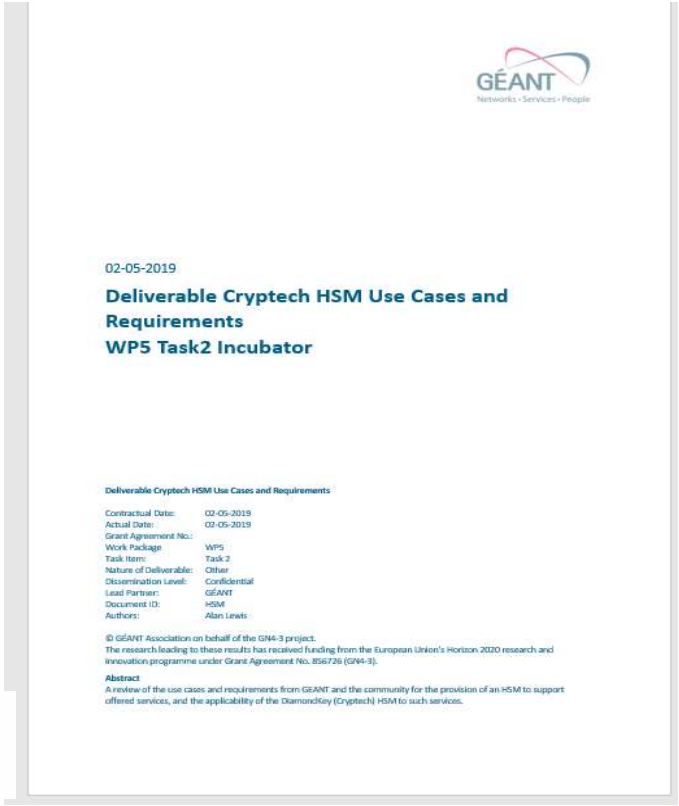
- Most requirements are for signing
- Performance requirement general low/moderate
- Must support RSA (4096), ECDSA P-384 and SHA-512/SHA-2
- Must support standard PKCK#11 interface
- Cost must be low to overcome inertia

HSM Suitability

- So how well suited is the HSM to our needs?
  - Supports RSA(4096) but performance < 1 sig./sec
  - ECDSA supported up to. c. 100 sig./sec
  - Supports necessary hash algorithms (SHA-512/256)
  - PKCS#11 client APIs available for Linux and Windows
  - Tamper resistant design… but not FIPS 140-2 certified
  - Will sell @ cost $6,000 (c.w. nShield Connect c. $40,000)

Achievements Summary

- Use cases for GEANT services documented ✓
- Applicability to services determined ✓
- GEANT, JISC and SURFnet interest in trials ✓
- Devices deployed at SURFnet offices ✓
- Diamond Key cease operations ☹
- Hardware and software upgrade pending ✗



GÉANT

02-05-2019

Deliverable Cryptech HSM Use Cases and Requirements
WP5 Task2 Incubator

Deliverable Cryptech HSM Use Cases and Requirements

Contractual Date:	02-05-2019
Actual Date:	02-05-2019
Grant Agreement No.:	
Work Package	WP5
Task Item:	Task 2
Nature of Deliverable:	Other
Dissemination Level:	Confidential
Lead Partner:	GÉANT
Document ID:	HSM
Authors:	Alan Lewis

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

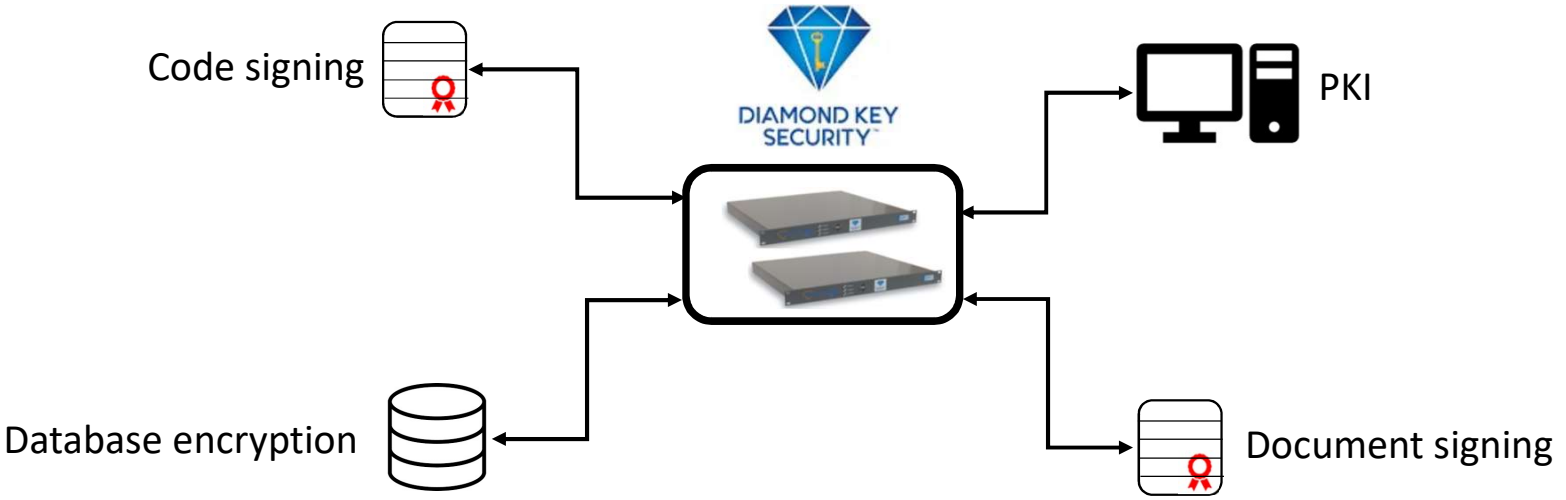
Abstract
A review of the use cases and requirements from GEANT and the community for the provision of an HSM to support offered services, and the applicability of the DiamondKey (Cryptech) HSM to such services.

Looking ahead

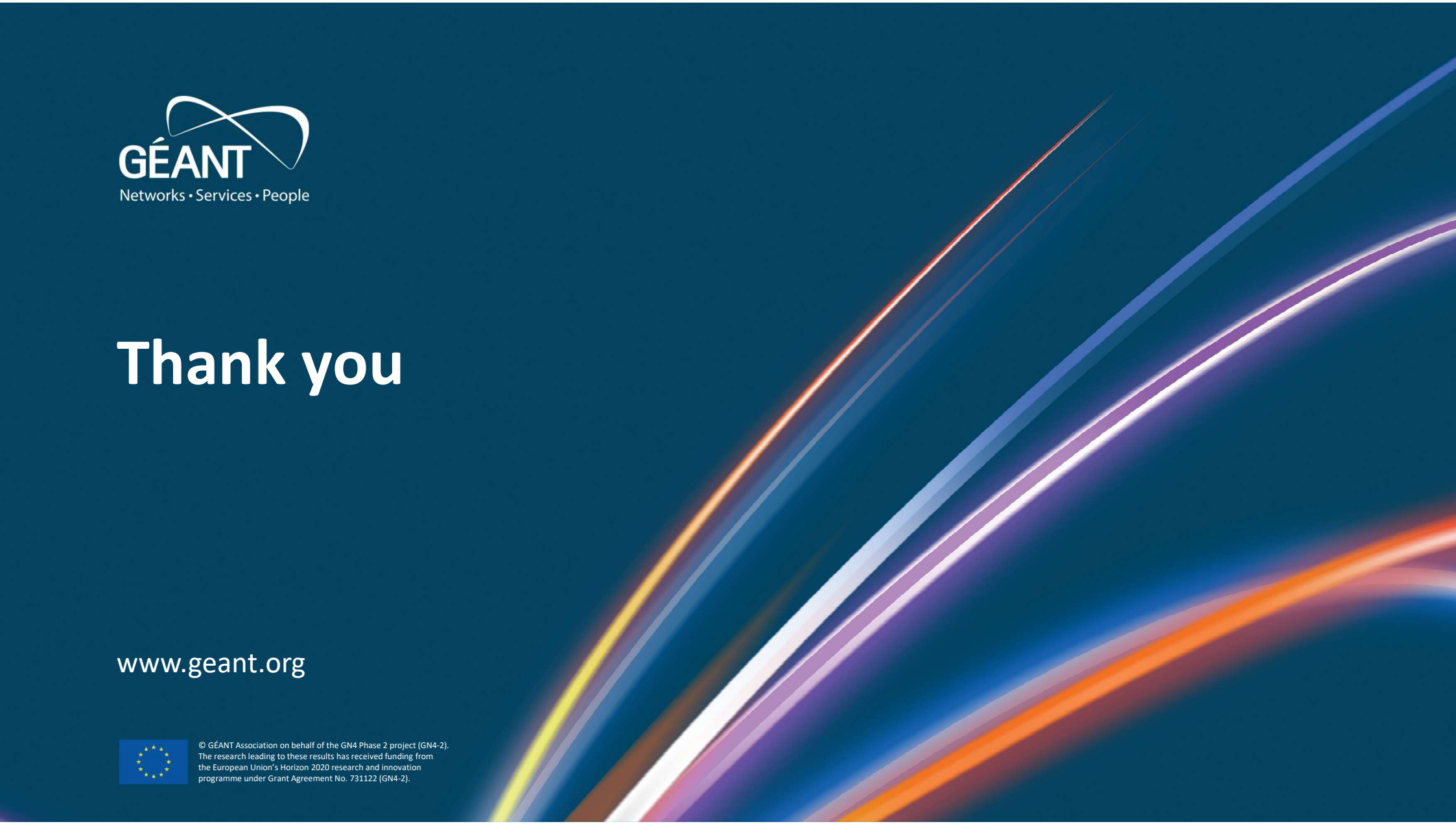
The trust in many T&I services rests on the security of their secret key material
Best practice recommends the use of an HSM to securely store such material

BUT …

HSMs are expensive and there is suspicion of commercial closed solutions
Developers lack access to HSMs during development reducing their adoption



Goal: Enable developer access to an HSM to improve security of their offerings



Thank you

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).