GÉANT
Networks • Services • People

Cryptech HSM – Preparation Phase

Sprint demo – 25th June 2019

Alan Lewis

(on behalf of the Alphas Cryptech HSM team)

Q2 2019

Restricted

Cryptech HSM – Objectives and Activities

Investigate Diamond Key (Cryptech) HSM capability and applicability to a variety of HSM use cases gathered within GÉANT and the wider community, setup the devices and identify the service teams who will participate in testing.

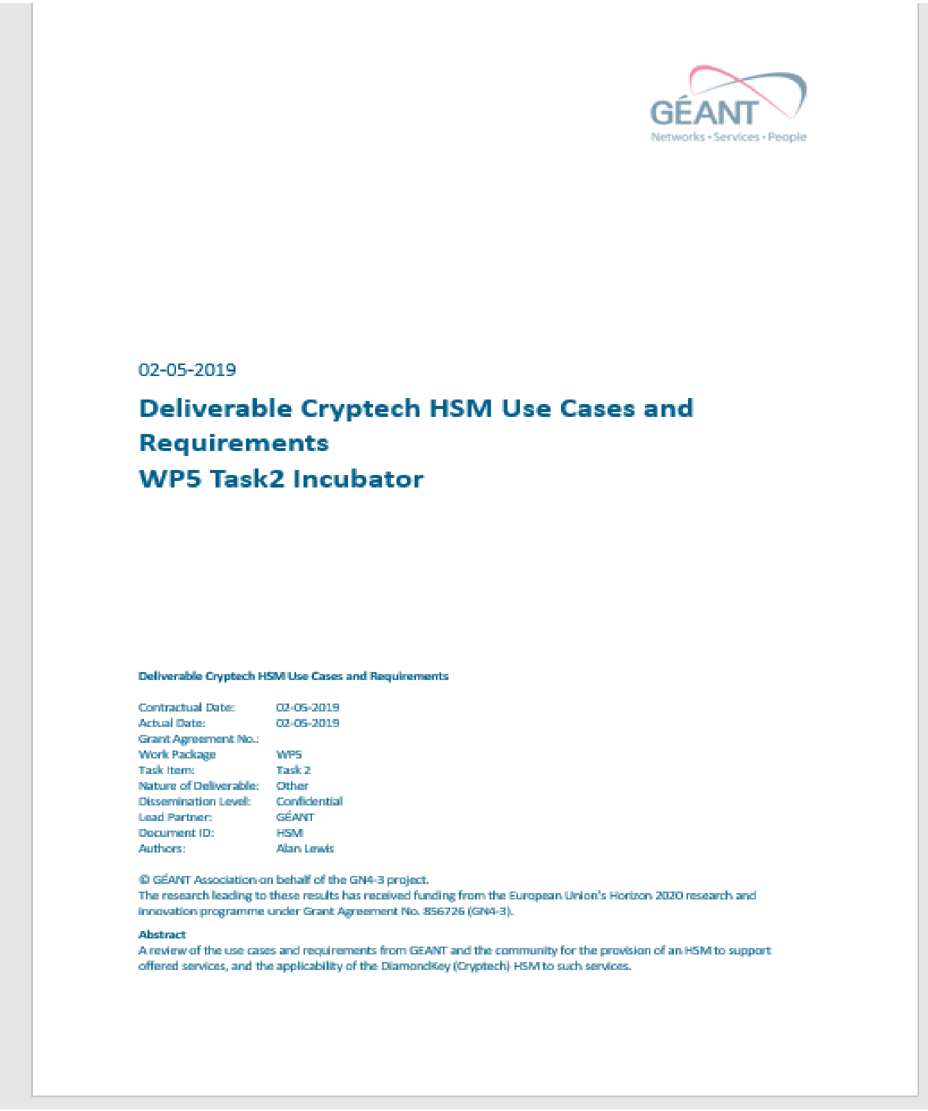
Name	Role
Brook Schofield	Magnum
Leif Johansson	P.I.
Niels van Dijk	Mentor
Michael Schmidt	Scrum Master
Branko Marovic	Team Member
Alan Lewis	Team Member

- Identify hosting for Diamond Key Appliances
- Install the Diamond Key appliances
- Document GÉANT services HSM use cases
- Determine Diamond Key Capabilities
- Document broader community HSM for use cases
- Identify service teams interested in HSM testing

Activities status

Status

- Technical capabilities discussed with DK ✓
- Use cases for GEANT services documented ✓
- Collating community T&I use cases underway ✓
- Diamond Key installation locations identified ✓
- Update and setup Diamond Key appliances ✓
- Identify interested teams for testing ✓
- Discuss findings with Cryptech and Community



GÉANT
Networks • Services • People

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

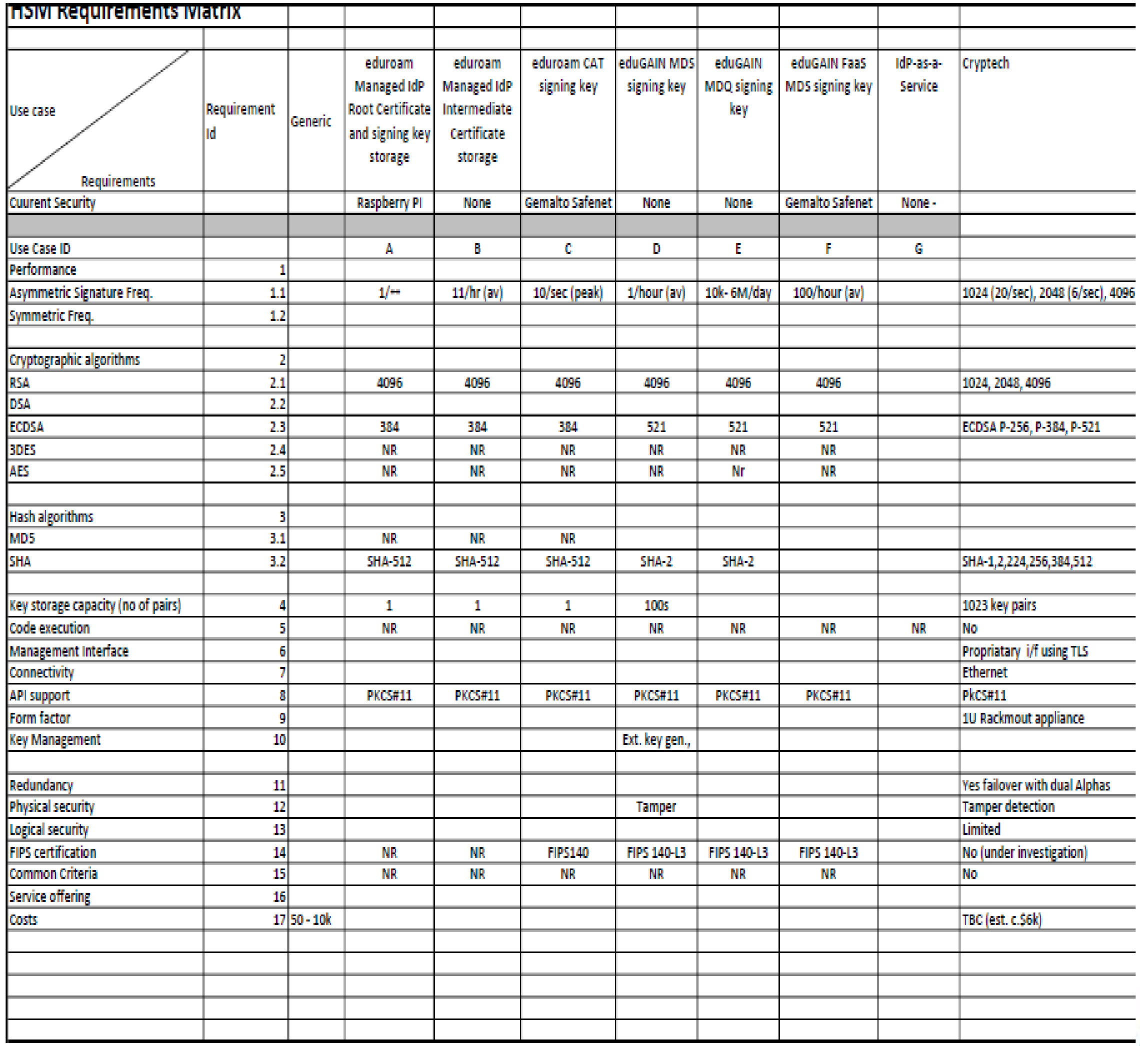
© GÉANT Association on behalf of the GN4-3 project.
The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

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.

Results and Conclusions (so far)

DiamondKey HSM suitability

- Most requirements are for signing
- Many requirements supported but two key omissions
  - Asymmetric performance for longer key lengths
  - FIPS certification
- Inertia for services already using an HSM
- Costs vs. benefits for service with no HSM
- Track record and sustainability



HSM Requirements Matrix

Use case Requirements	Requirement Id	Generic	eduroam Managed IdP Root Certificate and signing key storage	eduroam Managed IdP Intermediate Certificate storage	eduroam CAT signing key	eduGAIN MDS signing key	eduGAIN MDQ signing key	eduGAIN FaaS MDS signing key	IdP-as-a-Service	Cryptech
Cuurent Security			Raspberry PI	None	Gemalto Safenet	None	None	Gemalto Safenet	None -	
Use Case ID			A	B	C	D	E	F	G	
Performance	1									
Asymmetric Signature Freq.	1.1		1/↔	11/hr (av)	10/sec (peak)	1/hour (av)	10k- 6M/day	100/hour (av)		1024 (20/sec), 2048 (6/sec), 4096
Symmetric Freq.	1.2									
Cryptographic algorithms	2									
RSA	2.1		4096	4096	4096	4096	4096	4096		1024, 2048, 4096
DSA	2.2									
ECDSA	2.3		384	384	384	521	521	521		ECDSA P-256, P-384, P-521
3DES	2.4		NR	NR	NR	NR	NR	NR		
AES	2.5		NR	NR	NR	NR	Nr	NR		
Hash algorithms	3									
MD5	3.1		NR	NR	NR					
SHA	3.2		SHA-512	SHA-512	SHA-512	SHA-2	SHA-2			SHA-1,2,224,256,384,512
Key storage capacity (no of pairs)	4		1	1	1	100s				1023 key pairs
Code execution	5		NR	NR	NR	NR	NR	NR	NR	No
Management Interface	6									Propriatary i/f using TLS
Connectivity	7									Ethernet
API support	8		PKCS#11	PKCS#11	PKCS#11	PKCS#11	PKCS#11	PKCS#11		PkCS#11
Form factor	9									1U Rackmout appliance
Key Management	10					Ext. key gen.,				
Redundancy	11									Yes failover with dual Alphas
Physical security	12					Tamper				Tamper detection
Logical security	13									Limited
FIPS certification	14		NR	NR	FIPS140	FIPS 140-L3	FIPS 140-L3	FIPS 140-L3		No (under investigation)
Common Criteria	15		NR	NR	NR	NR	NR	NR		No
Service offering	16									
Costs	17	50 - 10k								TBC (est. c.$6k)

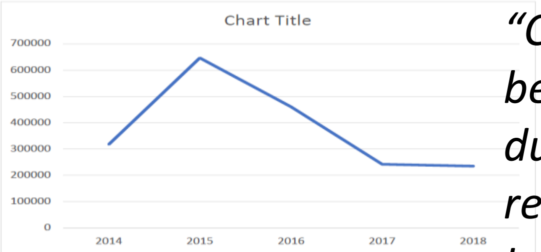


Figure 4. Donations by year (2014-2018)

"CrypTech has only once been forced to stop work due to lack of funds, it remains a systemic risk to the project."

GÉANT
Networks • Services • People

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).