GÉANT
Networks • Services • People

Cryptech HSM – Preparation Phase

Sprint demo – 5th April 2019

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

Q1 2019

Restricted

www.geant.org

Cryptech HSM – Objectives and Activities

Investigate Cryptech HSM modules capability and applicability to a variety of HSM use cases gathered within GÉANT and the wider community and identify opportunities for HSM as a Service

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 locations for Diamond Key Appliances
- Install the Diamond Key appliances
- Determine Diamond Key Capabilities
- Initial Community engagement for use cases
- Document use cases

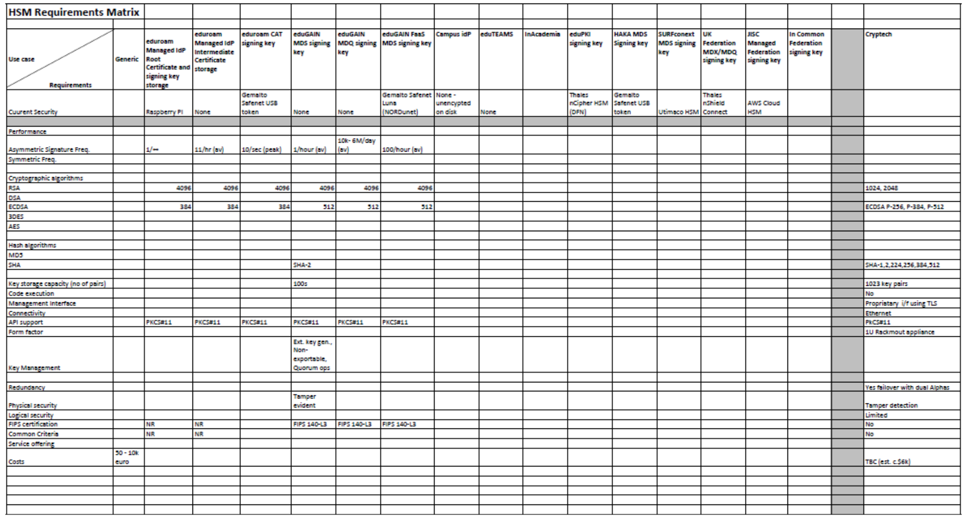
Results and Conclusions (so far)

Achievements

- Discussions held with Cryptech
- Requirements for GEANT services tabulated
- Engagement via eduGAIN with community
- Use cases document underway
- Location for Diamond Key installation identified

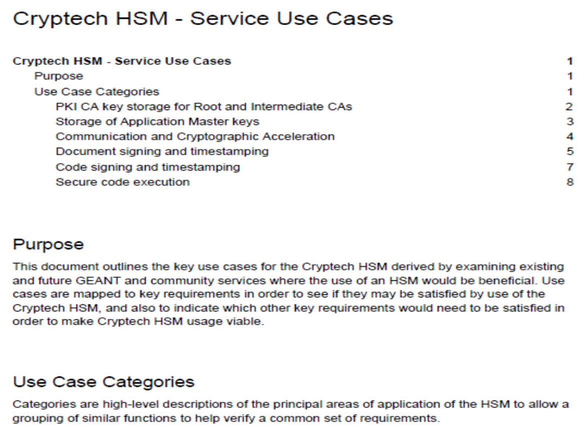
Thoughts so far

- Mainly signing use cases (metadata)
- Limited performance needs (except MDQ)
- Some possible crypto acceleration needs
- Formal certifications (FIPS) not big issue
- Displacing incumbent HSMS/HW harder



HSM Requirements Matrix

Use case Requirements	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	Campus idP	eduTEAMS	InAcademia	eduPKI signing key	HAKA MDS Signing key	SURFconext MDS signing key	UK Federation MDX/MDQ signing key	JISC Managed Federation signing key	In Common Federation signing key		Cryptech
Cuurent Security		Raspberry PI	None	Gemalto Safenet USB token	None	None	Gemalto Safenet Luna (NORDunet)	None - unencypted on disk	None		Thales nCipher HSM (DFN)	Gemalto Safenet USB token	Utimaco HSM	Thales nShield Connect	AWS Cloud HSM			
Performance																		
Asymmetric Signature Freq.		1/--	11/hr (av)	10/sec (peak)	1/hour (av)	10k- 6M/day (av)	100/hour (av)											
Symmetric Freq.																		
Cryptographic algorithms																		
RSA		4096	4096	4096	4096	4096	4096											1024, 2048
DSA																		
ECDSA		384	384	384	512	512	512											ECDSA P-256, P-384, P-512
3DES																		
AES																		
Hash algorithms																		
MD5																		
SHA					SHA-2													SHA-1,2,224,256,384,512
Key storage capacity (no of pairs)					100s													1023 key pairs
Code execution																		No
Management Interface																		Propriatary i/f using TLS
Connectivity																		Ethernet
API support		PKCS#11	PKCS#11	PKCS#11	PKCS#11	PKCS#11	PKCS#11											PkCS#11
Form factor																		1U Rackmout appliance
Key Management					Ext. key gen., Non-exportable, Quorum ops													
Redundancy																		Yes failover with dual Alphas
Physical security					Tamper evident													Tamper detection
Logical security																		Limited
FIPS certification		NR	NR		FIPS 140-L3	FIPS 140-L3	FIPS 140-L3											No
Common Criteria		NR	NR															No
Service offering																		
Costs	50 - 10k euro																	TBC (est. c.$6k)



Cryptech HSM - Service Use Cases

Purpose

This document outlines the key use cases for the Cryptech HSM derived by examining existing and future GEANT and community services where the use of an HSM would be beneficial. Use cases are mapped to key requirements in order to see if they may be satisfied by use of the Cryptech HSM, and also to indicate which other key requirements would need to be satisfied in order to make Cryptech HSM usage viable.

Use Case Categories

Categories are high-level descriptions of the principal areas of application of the HSM to allow a grouping of similar functions to help verify a common set of requirements.

Over to you…………… Questions??

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).