

Cryptech HSM – Preparation Phase

Sprint demo #6 – 8th October 2019

Alan Lewis

(on behalf of the Alphas Cryptech HSM team)

Q4 2019

Public

www.geant.org



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











Current Status

Use cases for GEANT services documented



Applicability to services determined



Interest from GEANT, JISC and SURFnet in trials



Devices deployed at SURFnet offices



Hardware and software upgrade pending



Diamond Key cease operations





02-05-2019

Deliverable Cryptech HSM Use Cases and Requirements

WP5 Task2 Incubator





Notes on next steps

DK Operations		
Operations have ceased but	Create HSM testbed	
DK to OS all assets under BSD licence	Project owns two DK appliances	Next Incubator cycle
Cryptech continues to be funded	Utilise these for community benefit	Define scope of testbed
	Engagrada OS project acquirity decign	Create access and registration process
	Encourage OS project security design	
	Test with an HSM – PKCS#11	Reconnect with interested parties





Thank you

www.geant.org



© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2). 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).

