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.

PKI CA key storage for Root and Intermediate CAs

Use case name	eduroam Managed IdP Root Key Storage
Actors	Security Manager, Key Ceremony participants
Description	The root server private keys and certificates are stored inside an HSM The root CA key is used once and stored offline,
Trigger	A new intermediate (issuing) certificate is required to be signed by the root CA.
Connected Requirements	A.1.1 , A.2.1, A.2.3, A.8
Requirements Traceability	
Contact	Organisation
Miroslav Milinovic Stefan Winter	University of Zagreb (Carnet) RESTENA

Use case name	eduroam Managed IdP Intermediate Key Storage
Actors	Root CA signer, Security manager
Description	The intermediate server private keys and certificates are stored inside an HSM The intermediate CA key is used to sign certificates at a rate of up to 4000 TPS.
Trigger	A new user certificate request is received at the intermediate (issuing) CA
Connected Requirements	B.1.1 , B.2.1, B.2.3, B.8
Requirements Traceability	
Contact	Organisation
Miroslav Milinovic Stefan Winter	University of Zagreb (Carnet) RESTENA

Use case name	eduPKI Root CA key
Actors	Security Manager, Key Ceremony participants
Description	The root private key and certificates are stored inside an HSM to enable service specific certificates to be issued where this would otherwise not be possible
Trigger	A new user certificate request is received to be signed by the root CA private key.
Connected Requirements	
Requirements Traceability	
Contact	Organisation
Miroslav Milinovic Reimer Karlsen-Masur	University of Zagreb (Carnet) DFN

Storage of Application Master keys

Communication and Cryptographic Acceleration

Use case name	Securing TLS connections
Actors	TLS/SSL server
Description	During client server authentication in a TLS transaction the servers private key that is used to encrypt the data is stored inside an HSM
Trigger	A private is required to be securely stored
Connected Requirements	
Requirements Traceability	

Contact	Organisation
peter.schober@univie.ac.at	ACOnet

Document signing and timestamping

Use case name	eduGAIN MDS signing
Actors	eduGAIN metadata signing authority
Description	The eduGAIN MetaData aggregate is signed with a key that is stored inside an HSM, to be consumed by participating federations
Trigger	A new eduGAIN metadata aggregate is available for signing hourly.
Connected Requirements	D1.1, D2.1, D2.3, D3.2, D4, D8, D10, D12, D14
Requirements Traceability	
Contact	Organisation
peter.schober@univie.ac.at	ACOnet
farhan@sifulan.my	SIFULAN

Use case name	eduGAIN MDQ signing
Actors	eduGAIN metadata signing authority
Description	The eduGAIN MetaData Query service allows entities to request only the metadata they require when they need it without requiring the complete aggregate. Metadata from the MDQ server is signed with a key that is stored inside an HSM.
Trigger	A federation requests the metadata they need and it is signed as

	required.
Connected Requirements	E1.1, E2.1, E2.3, E8,E14
Requirements Traceability	
Contact	Organisation
peter.schober@univie.ac.at	ACOnet
Davide.Vaghetti@garr.it	GARR

Use case name	eduGAIN FaaS MDS signing
Actors	FaaS metadata signing authority
Description	The federation MetaData aggregate created by FaaS is signed with a key that is stored inside an HSM, to be consumed by eduGAIN to produce a metadata aggregate
Trigger	New federation metadata is available to be signed
Connected Requirements	F1.1, F2.1, F2.3, F8, F14
Requirements Traceability	
Contact	Organisation
Davide.Vaghetti@garr.it	GARR

Use case name	IdP-as-a-Service SAML metadata signing
Actors	IdP-as-a-service signing authority
Description	The IdP-as-service platform creates SAML metadata which is then signed by key that is stored inside an HSM

Trigger	A SAML entity wishes to exchange a message with another SAML entity
Connected Requirements	
Requirements Traceability	
Contact	Organisation

Code signing and timestamping

Use case name	eduroam Managed IdP Installer signing
Actors	Eduroam IdP administrator
Description	The eduroam Managed Idp installer is signed with a key that is stored inside an HSM to allow the use of EV code signing certificates.. Signing takes place for both Windows .exe installers, and iOS, MacOS XML installer. In the case of windows the the file is both signed and timestamped. In the case of iOS/MacOS it is only an S/MIME signature.
Trigger	A new admin wishes to download a new Managed IdP installer.
Connected Requirements	
Requirements Traceability	
Contact	Organisation
Miroslav Milinovic Stefan Winter alan.buxey@myunidays.com	University of Zagreb (Carnet) RESTENA MyUniDays

Use case name	eduroam CAT Installer signing

Actors	Eduroam IdP administrator
Description	The eduroam Configuration Assistant Tool (CAT) installer private key is stored in an HSM to allow the use of EV code signing certificates for enhanced security.
Trigger	A new admin wishes to create an eduroam installer for distribution to an institutions users
Connected Requirements	C1.1, C2.1, C2.3, C8
Requirements Traceability	
Contact	Organisation
Miroslav Milinovic Stefan Winter alan.buxey@myunidays.com	University of Zagreb (Carnet) RESTENA MyUniDays

Secure code execution

Use case name	
Actors	
Description	
Trigger	
Connected Requirements	
Requirements Traceability	
Contact	Organisation