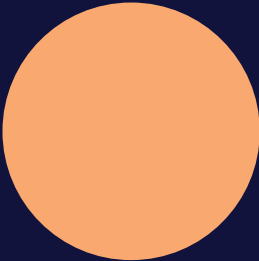


HARDWARE MANAGED KEYS IN AZURE

Or why encrypt data in the cloud if the cloud operator handles the keys?

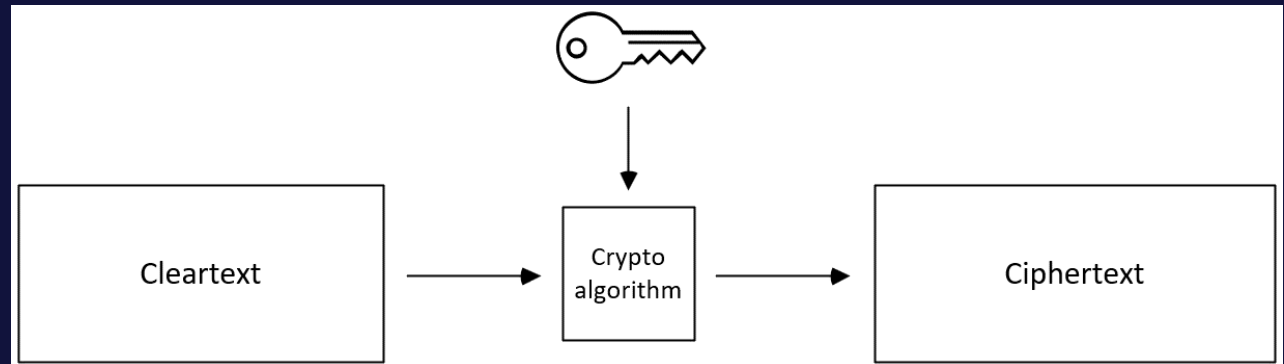
Lars Olaussen
Norsk kryptoseminar 2023
2023-10-27



bouvet

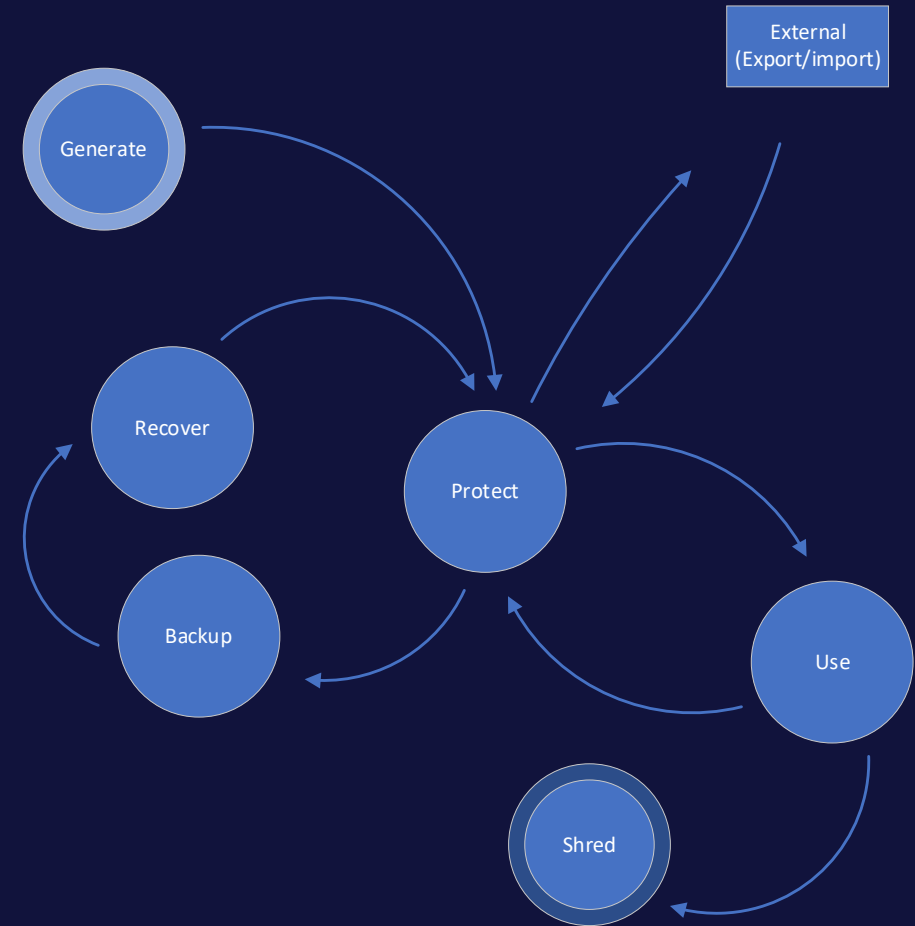
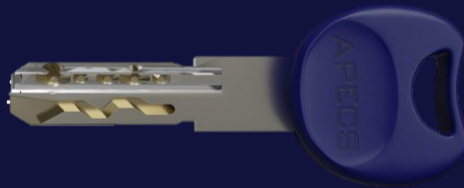
What is crypto?

- Encyclopædia Britannica:
 - «Practice of the enciphering and deciphering of messages in secret code in order to render them unintelligible to all but the intended receiver.»
- Mathematical functions and algorithms that provides...
 - Authentication/authenticity
 - Integrity
 - Confidentiality
 - ...
- According to Kerckhoffs: Dependent on secrecy of keys



What is key management?

- Handling of keys in their entire lifecycle
 - From seconds (reading online news)
 - To years (protecting archived data)
- ¡Difficult!



What is an HSM?

Hardware Security Module

- «Device» designed and implemented to securely...
 - Generate
 - Protect
 - Import and export
 - Use
 - Update
 - Replicate, backup and restore
- ...strong keys (i.e. (mainly) inside the HSM)
- Usually evaluated according to FIPS 140-2/3 (ISO/IEC 19790) that specifies four security levels:
 - 1 and 2 can be software based
 - 3 and 4 must be hardware based



What is Azure?

- Microsoft's Cloud Platform
 - Identity
 - Computer services
 - Storage
 - Data management
 - Communication
 - ...
- Where everyone is going*



*Except AWS, Google, OCI

Protecting Information in Azure

- Data is encrypted *at rest* (disk drives) and *in transit* (network)
- Keys are handled by Microsoft
- Protects against physical attacks in datacentres
- Does not protect information between tenants or from Microsoft
- (Client-side encryption is outside of scope)



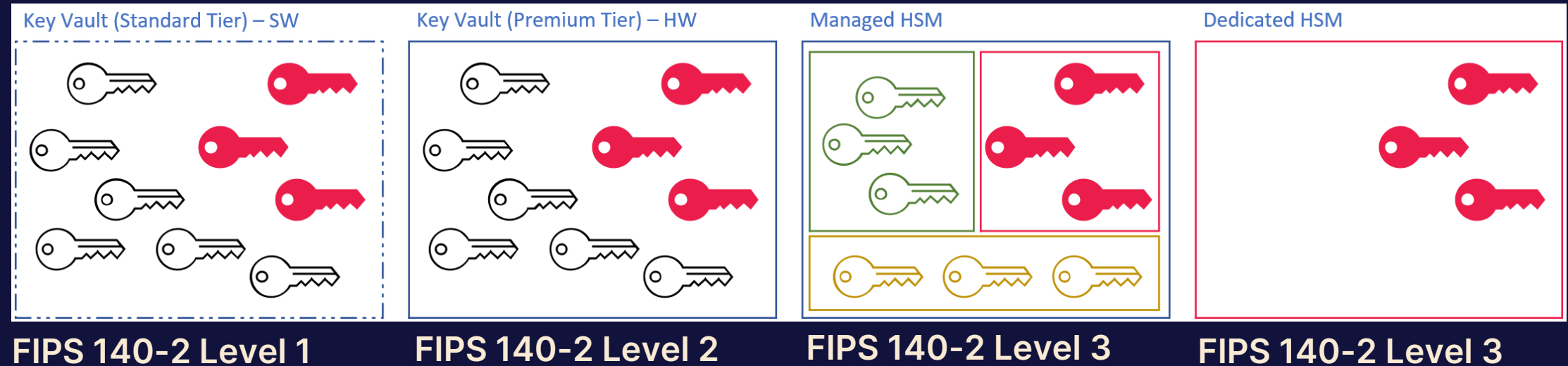
The missing pieces

- Management of own keys
(Customer Managed Keys (CMK))
- Use own keys to encrypt data *at rest* and *in transit*



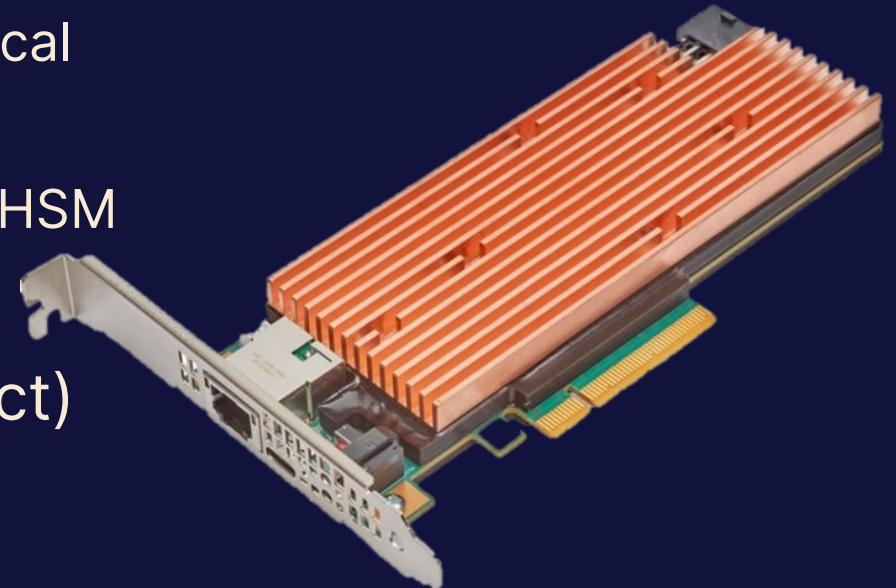
How to manage own keys in Azure

«Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data»



Azure Managed HSM

- Centralized, managed, redundant, and dedicated HSM instance in Azure for managing own keys
 - Microsoft's upgrades, updates, and maintains the modules
 - (At least) One virtual instance spread across 3 physical modules in at least two different availability zones
 - The customer 'formats' and holds the keys to its own HSM partition
- Microsoft does not have visibility into or (direct) access to the keys



Azure Managed HSM II

- Supports key management for built-in cloud services
- Enforce specific algorithms, key lengths and key lifetimes
- Manages keys only, not certificates or secrets
- Provides access control on keys
- Logs/monitors key usage
- Separates use of keys from management of keys and HSM

Azure Managed HSM III

- Secure
- Easy to use
 - Keys are 'accessed' by URI
 - URI is 'only' difference between different key vaults

Supported key types and algorithms

Key Type	Encrypt/Decrypt (Wrap/UnWrap)	Sign/Verify	HMAC
RSA 2048 RSA 3072 RSA 4096	RSA-OAEP RSA-OAEP-256 RSA1_5	PS256 PS384 PS512 RS256 RS384	-
AES-128, AES-256	AES-KW AES-GCM AES-CBC	-	SHA-256 SHA-384
EC-P256, EC-P256K EC-P384 EC-P521	-	ES256, ES256K ES384 ES512	-

Use of own keys

- Built-in services
 - Encryption of data at rest
- Third-party services
 - SSL/TLS offload
 - PKI
- Own services and apps
- Confidential Computing



Is Azure special?

- No
- 'All' major Cloud operators provide ways of manage keys in hardware

QUESTIONS?

Lars.Olaussen@bouvet.no

