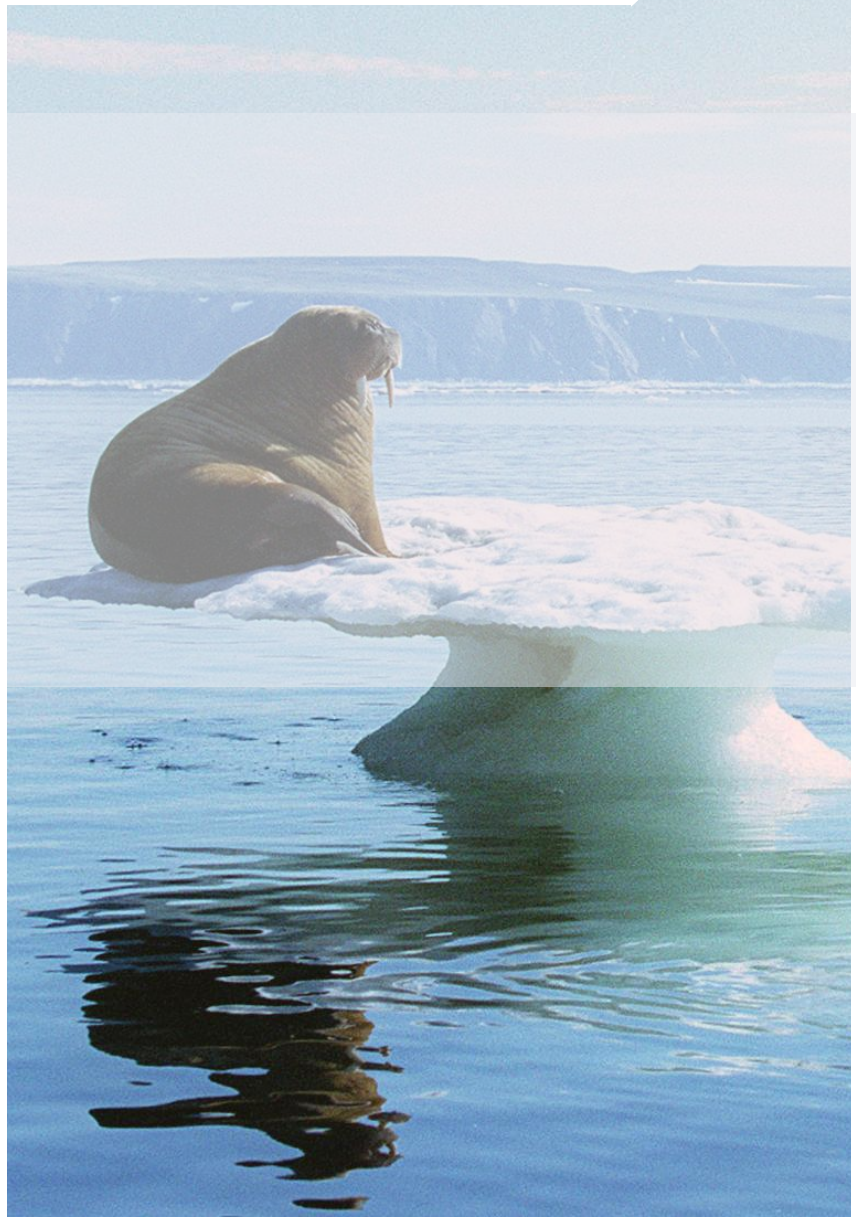
CRYPTOMATHIC



Control Your Cloud: BYOK is Good,

But not Good Enough

May 18th, 2017, ICMC'2017, Arlington, VA, CA

About Cryptomathic

- **In business for 30+ years**
- **A software company, which uses HSMs and Hardware Security Peripherals Extensively.**
- **A technology provider of Cryptographic Key Management Systems**
  - Sweet spot in helping augment hybrid architectures
  - We rely on good and sound Hardware Security Products

BYOK

- **BYOK = Bring Your Own Key**
- It suggests a one-way mechanism:
  - From the perspective of a Cloud Computing Provider: ***Your Key, into my Cloud.***
- The word *"**key**"* tends to be generally understood in a very broad sense
  - Symmetric Keys
    - General Purpose Encryption / Decryption Keys
    - Master Derivation Keys (especially used in financial service)
  - Asymmetric Key (Pairs)
    - -and corresponding certificates.
- However, in the context of Cloud Service Providers, it appears to have been assigned a more limited meaning for general purpose crypto only – at least initially.

Cloud Service Providers (CSPs) Offering

- **Three major cloud service providers all offer some form of Cryptographic Services**
  - Amazon AWS
  - Microsoft Azure
  - Google Cloud Platform
- **The main purposes appear to be**
  - Promoting direct integration with their own services
  - through offering external APIs and capabilities.
- **All three offer some form of Key Management Service and cryptographic APIs.**

CRYPTOMATHIC

Key Management Services offered (re. BYOK)

Microsoft Azure

- **HSM**
  - Thales nShield HSM
- **Crypto**
  - AES 128 or 256 and RSA keys
- **BYOK Protocol / Format**
  - based on Thales commands

Amazon AWS

- **HSM**
  - Gemalto Luna SA HSM
- **Crypto**
  - AES 128 and 256 keys only
- **BYOK Protocol / Format**
  - PKCS#1 to wrap a key

Google Cloud Platform

- **HSM**
  - None currently
- **Crypto**
  - AES 256 keys only
- **BYOK Protocol / Format**
  - RSA-OAEP encrypted key

CRYPTOMATHIC

Data-at-rest Encryption and API functionality

- **Data-rest Encryption**
  - AES 128 or 256
  - + rights management policy
- **Crypto services and APIs**
  - Encrypt/decrypt
  - Sign and Verify
  - Wrap/unwrap

- **Data-at-rest encryption**
  - AES-GCM 128 or 256
- **Crypto services and APIs**
  - encrypt/decrypt only with AES-GCM
  - based on Gemalto HSM

- **Data-at-rest encryption**
  - AES-GCM 256
- **Crypto services and APIs**
  - encrypt/decrypt only with AES-GCM

BYOK – an important tool (but not the only one)

- **BYOK helps you get your own generated key into the Cloud**
  - -rather than having the CSP generate one for you on your behalf.
- **The Cloud Service Provider "will handle it for you" – but there is no common export facility**
  - Thus, if you need a copy, be sure to save one before submitting it!
- **BYOK has (slightly) different meanings in the eyes of the CSP**
  - Be sure you understand the limitations of what is available
  - Also understand your responsibilities, i.e.
    - Do you really want to manage your encryption key in a spreadsheet?
    - Probably, you also have many other types of keys you need to manage

CRYPTOMATHIC

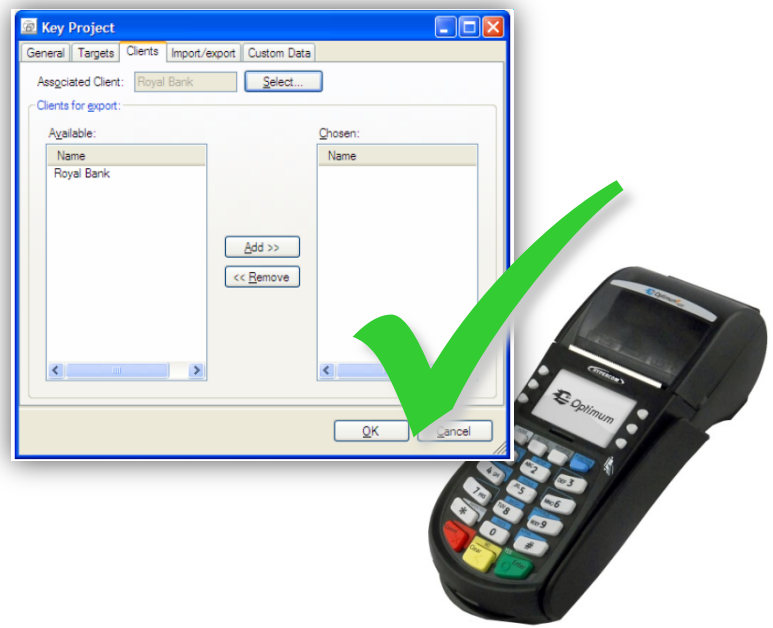
Enter MYOK™ - Manage Your Own Key(s)

- **In managing your own keys, it is implied that**
  - You can work with your keys securely
  - You can provision keys to where they are needed
  - You are able to manage the life-cycle of keys you manage
    - Generation, Import, Export
    - Backup, Restore
    - Update, Roll-back, Recover
    - Certify, Recertify and Revoke
- **Ideally, you need to be able to do this in a way that is meaningful to your business**
  - A central system, available (to you) and under your sole command.

CRYPTOMATHIC

MYOK solutions – an example

Centralized Key Management System replacing and unifying poorly-designed, proprietary and manual key management interfaces of existing products and HSMs

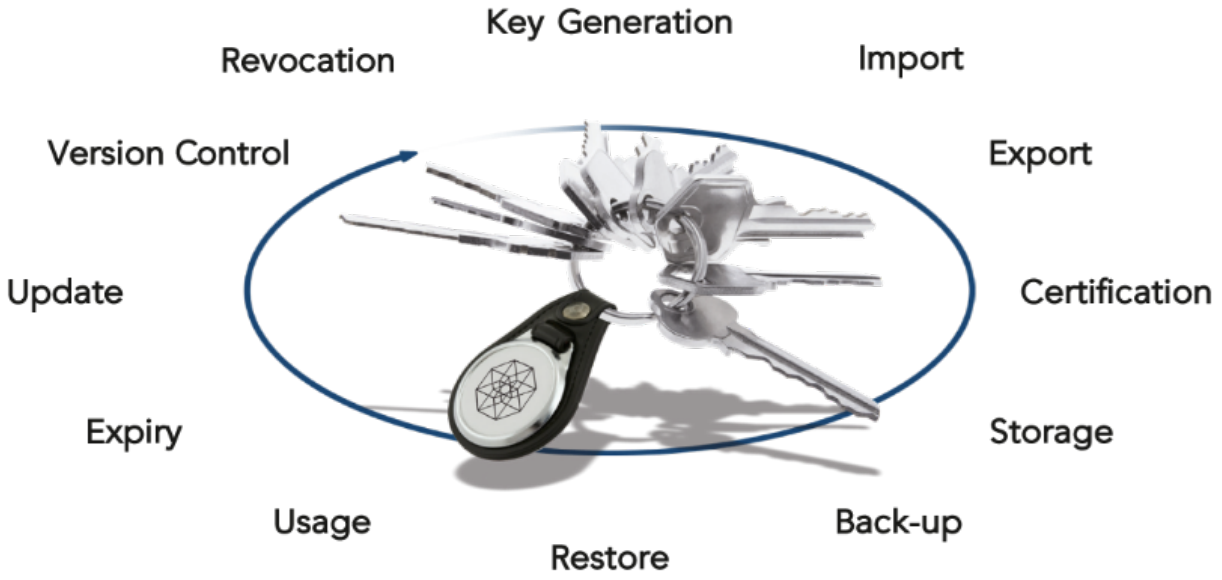


CRYPTOMATHIC

Advanced Key Lifecycle Management

- **More than just keys**
  - Name
  - Algorithm and length
  - Export settings
    - KCV length
    - Intended recipients
    - Formats

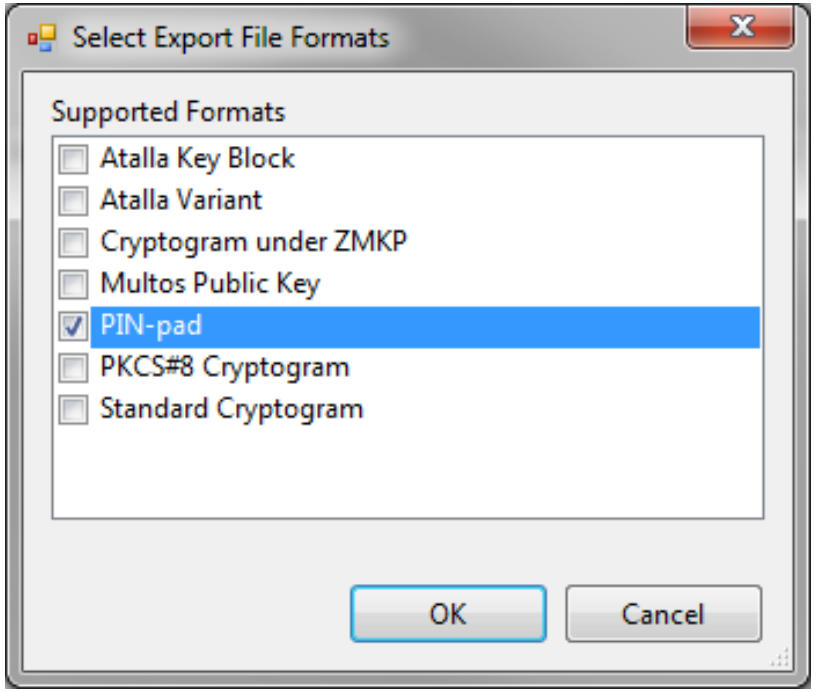
- **The bigger picture**
  - Key Usage Logs
  - Lifecycle status
  - Custom data



CRYPTOMATHIC

Typically Encountered Key Formats (other than BYOK)

- **Atalla Key Block / Variant**
  - File-based format. Application keys only.
- **Cryptogram under ZMKP**
  - Export to a file encrypted by a public key.
- **PIN pad**
  - Export as XOR shares on a PIN pad. Symmetric keys only.
- **PKCS #8 Cryptogram**
  - Export as an encrypted PKCS #8 file. Asymmetric keys only.
- **Standard Cryptogram**
  - Export as an encrypted key file. Symmetric keys only.
- **Subject Public Key Info**
  - Export of public keys.
- **TR-31**
  - Compatible with e.g. Thales Payments HSMs
- **IBM CCA**
  - For IBM HSMs (with control vector)

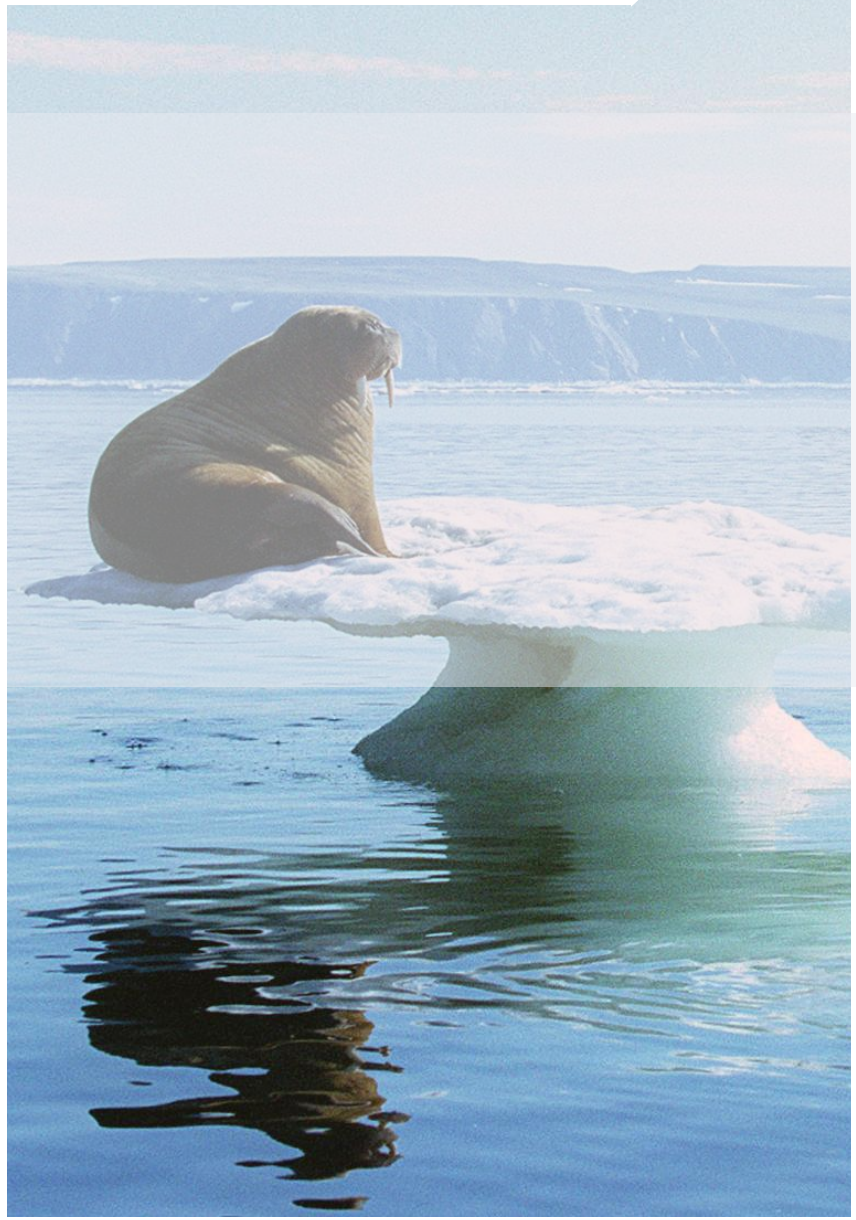


CRYPTOMATHIC

Sound Architecture

- **Client/server design**
  - A service which can run from your labs (whether own data center or dessktop)
  - DBMS, HSM (FIPS 140-2, L3)
- **Administrators connect from Windows client**
  - Smart card based authentication for all operations (FIPS 140-2, L3)
  - PIN pads for reading cards and importing/ exporting/printing key shares

CRYPTOMATHIC



Thank you

matt.Landrock@cryptomathic.com