#GlobalAzure

The Lord of the Keys

Tus secretos a salvo con Azure Key Vault

Iria Quiroga, Service Delivery Manager

José Ángel Fernández, Cloud Solution Architect

Microsoft


ackstorm
Managed Cloud Solutions


ALTRAN


avanade
Results Realized


capside
architects of the digital society


encamina
PIENSA EN COLORES


Insight


intelequia
SOFTWARE SOLUTIONS


KABEL


NECSIA


plain
concepts


SOGETI


SUSE
We adapt. You succeed.


東京'TOKIOTA

Colabora


Microsoft


2016
Global Azure
BOOTCAMP

Galadriel

a.k.a Iria Quiroga

Service Delivery Manager@Microsoft

@iriaq

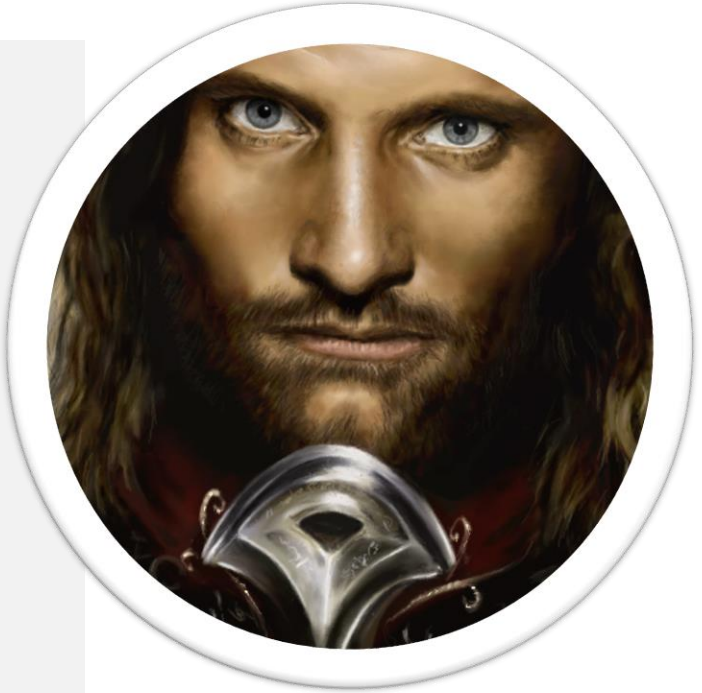
2016 Global Azure BOOTCAMP

Aragorn

a.k.a José Ángel Fernández

Cloud Solution Architect@Microsoft

@jangelfdez



2016 Global Azure BOOTCAMP

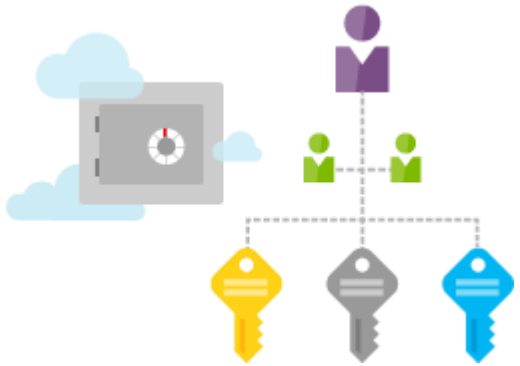
Agenda

- What is Azure Key Vault?
- Terminology
- Key Vault within Azure object model
- What is HSM?
- Types of keys
- Anchored in AD – your org is in control
- Demo time

What is Azure Key Vault?

An Azure resource provider that lets you

1. Store & manage SECRETS (app config), and release them at runtime to authorized apps & users.
2. Store & manage KEYS, and perform cryptographic operations on behalf of authorized apps & users.



Terminology

Secret

What: Any sequence of bytes under 25KB. E.g. SQL connection string, Storage account key.

How used: Authorized users/apps write and *read back* the secret value.

Key

What: A cryptographic key. RSA 2048

How used: *A key cannot be read back*. Caller must ask the service to decryp/sign with the key

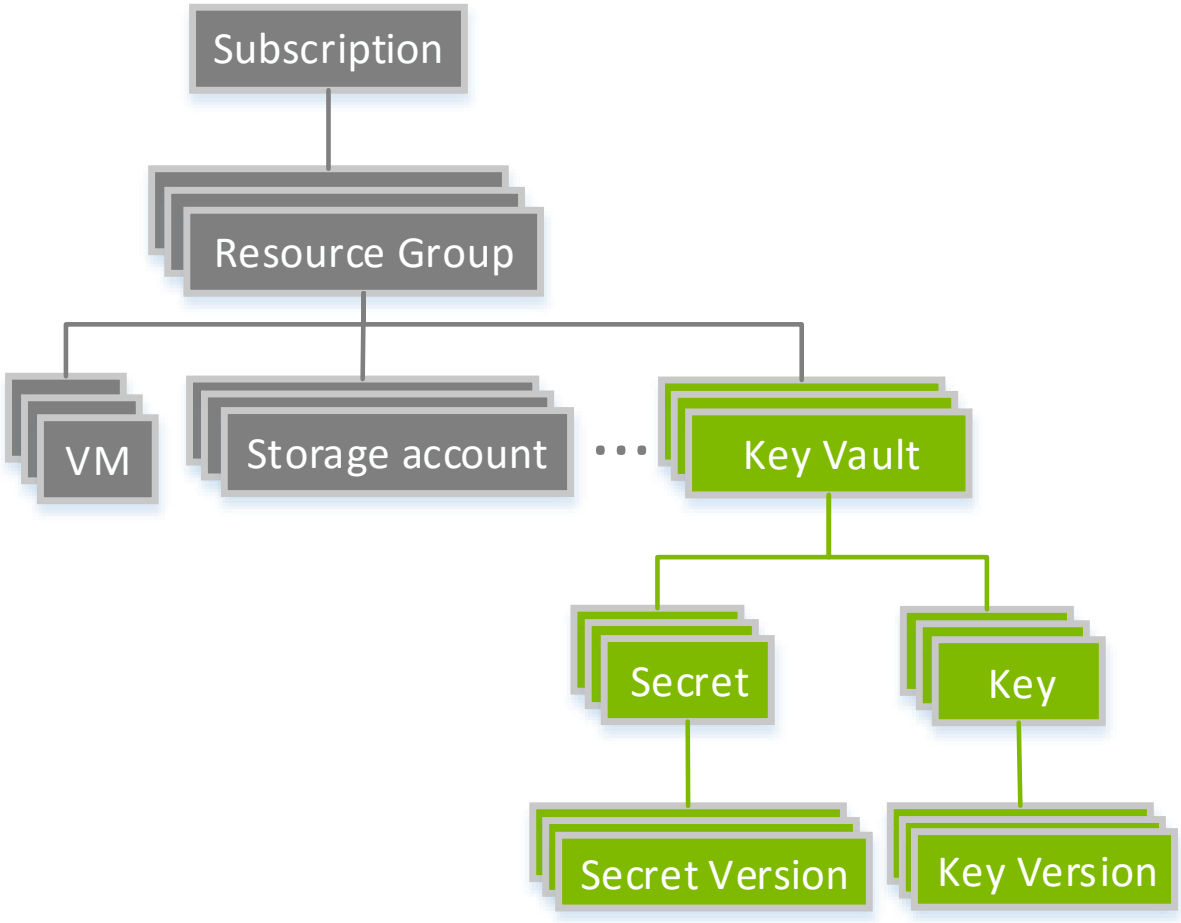
Key Vault

Container for related keys and secrets that are managed together.

Unit of access control, unit of billing.

An Azure resource, like a storage account

Key Vault within Azure object model



What is HSM?

Hardware Security Module (HSM)

- Physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing
- Plug-in card or an external device that attaches directly to a computer or network server

Types of keys

HSM-protected key

- Operations on this key are performed inside HSMs (Thales nShield, FIPS 140-2 Level 2).

Software-protected key

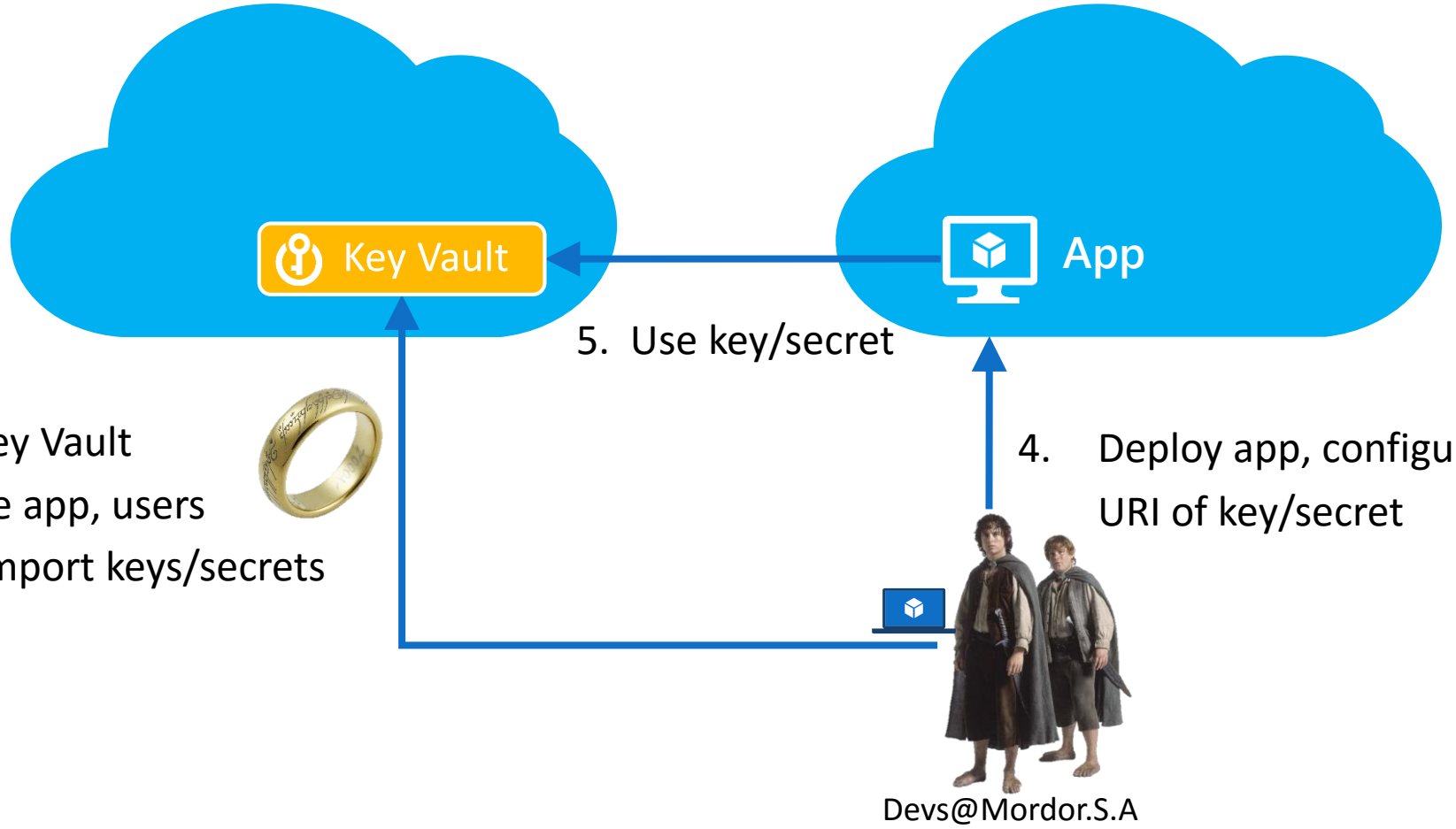
- Operations on this key are performed in VMs on Azure (FIPS 140-2 Level 1 pending).
- When stored, they are encrypted with a key chain that terminates in HSMs.

Anchored in AD – your org is in control

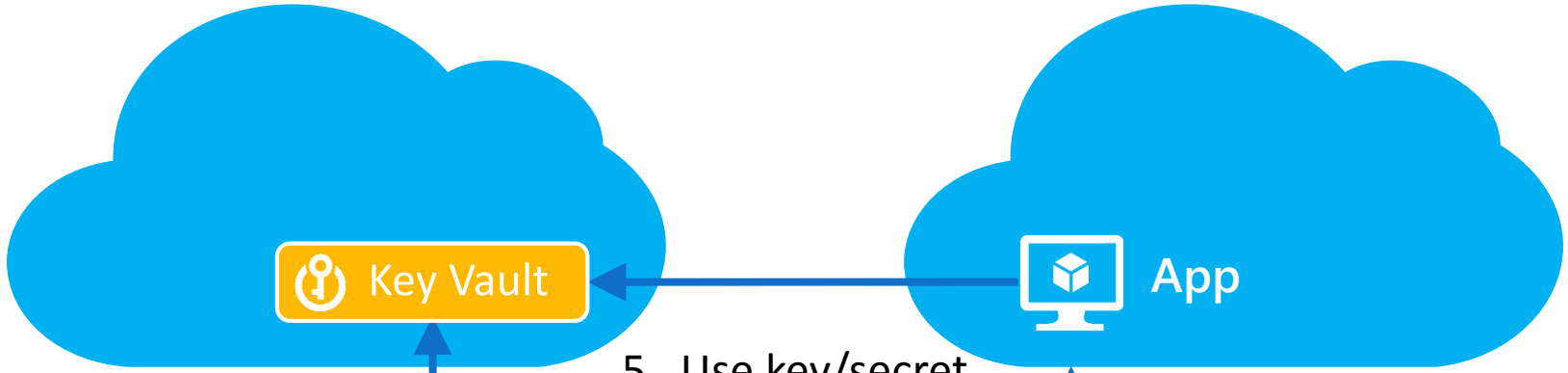
Authentication is via Azure AD tokens

Authorization is via ACL on key vault

Phase 1: Developer builds/tests application



Phase 2: App moves into pilot / pre-prod



5. Use key/secret

1. Create Key Vault
2. Authorize app, users
3. Create/import keys/secrets

Admin@Mordor.S.A.

4. Deploy app, configured with URI of key/secret

Devs@Mordor.S.A.

Phase 3: App moves into production

1. Create Key Vault
2. Authorize app, users
3. Create/import keys/secrets

6. Manage keys/secrets

Admin@Mordor.S.A.

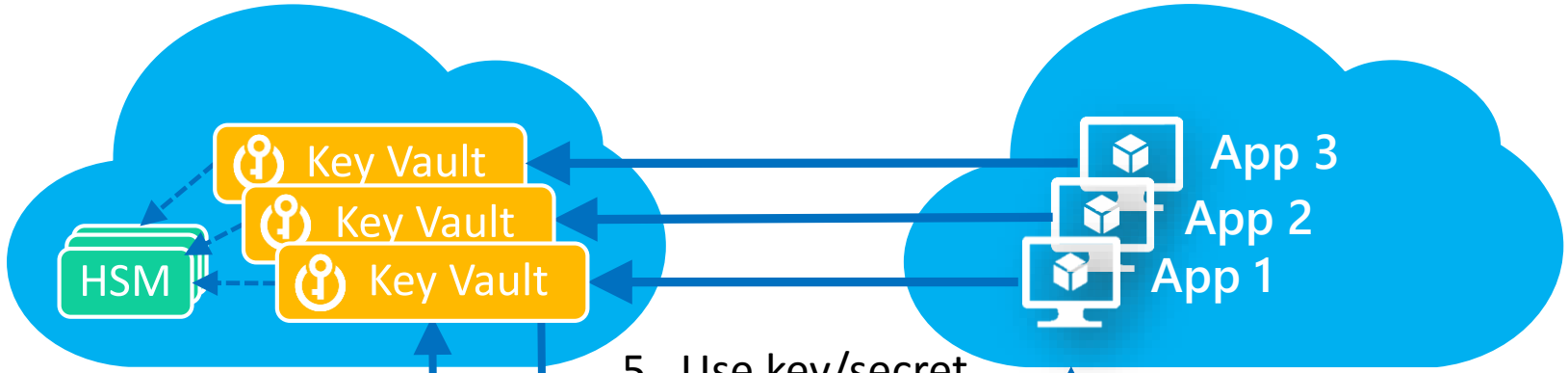
7. Monitor logs

4. Deploy app, configured with URI of key/secret

Devs@Mordor.S.A.

2016 Global Azure BOOTCAMP

Phase 4: Scale, deploy more apps in minutes



1. Create Key Vault
2. Authorize app, users
3. Create/import keys/secrets

6. Manage keys/secrets

5. Use key/secret

7. Monitor logs

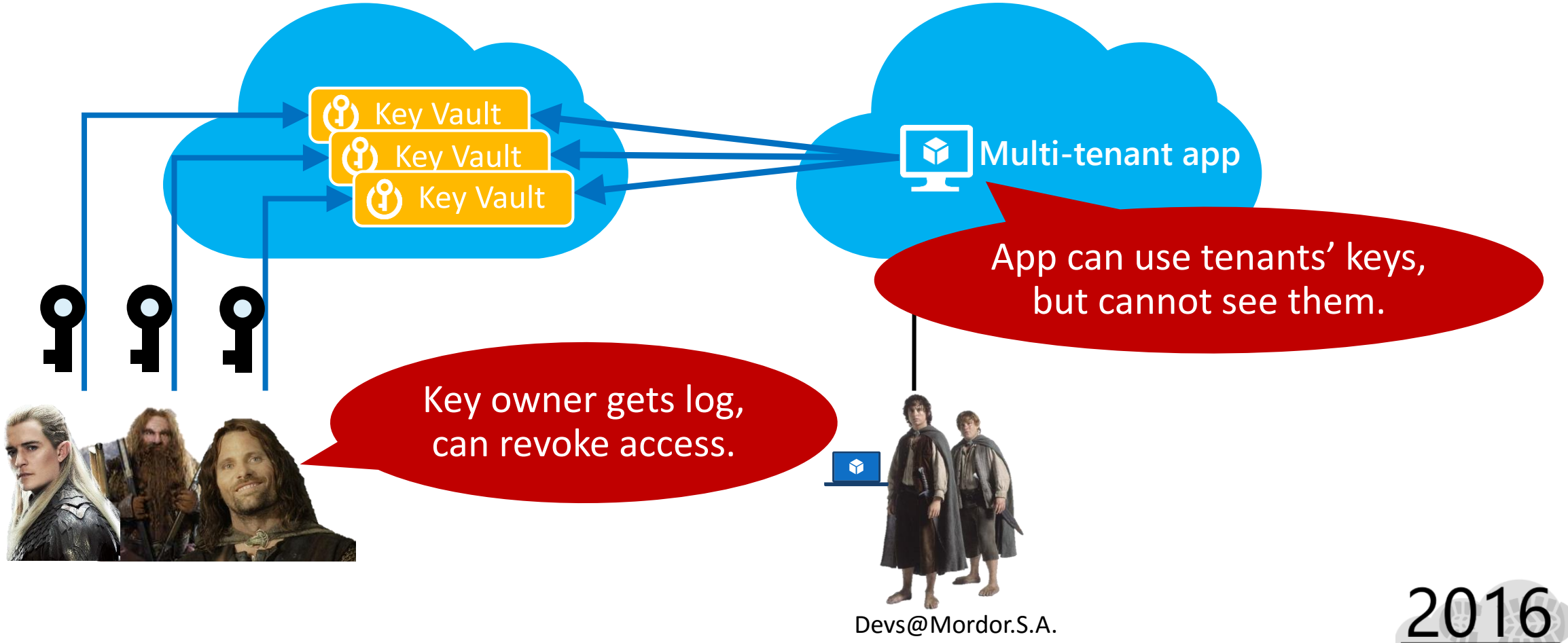
4. Deploy app, configured with URI of key/secret

Admin@Mordor.S.A.

Devs@Mordor.S.A.

2016 Global Azure BOOTCAMP

Multi-tenant app offers customer-managed keys

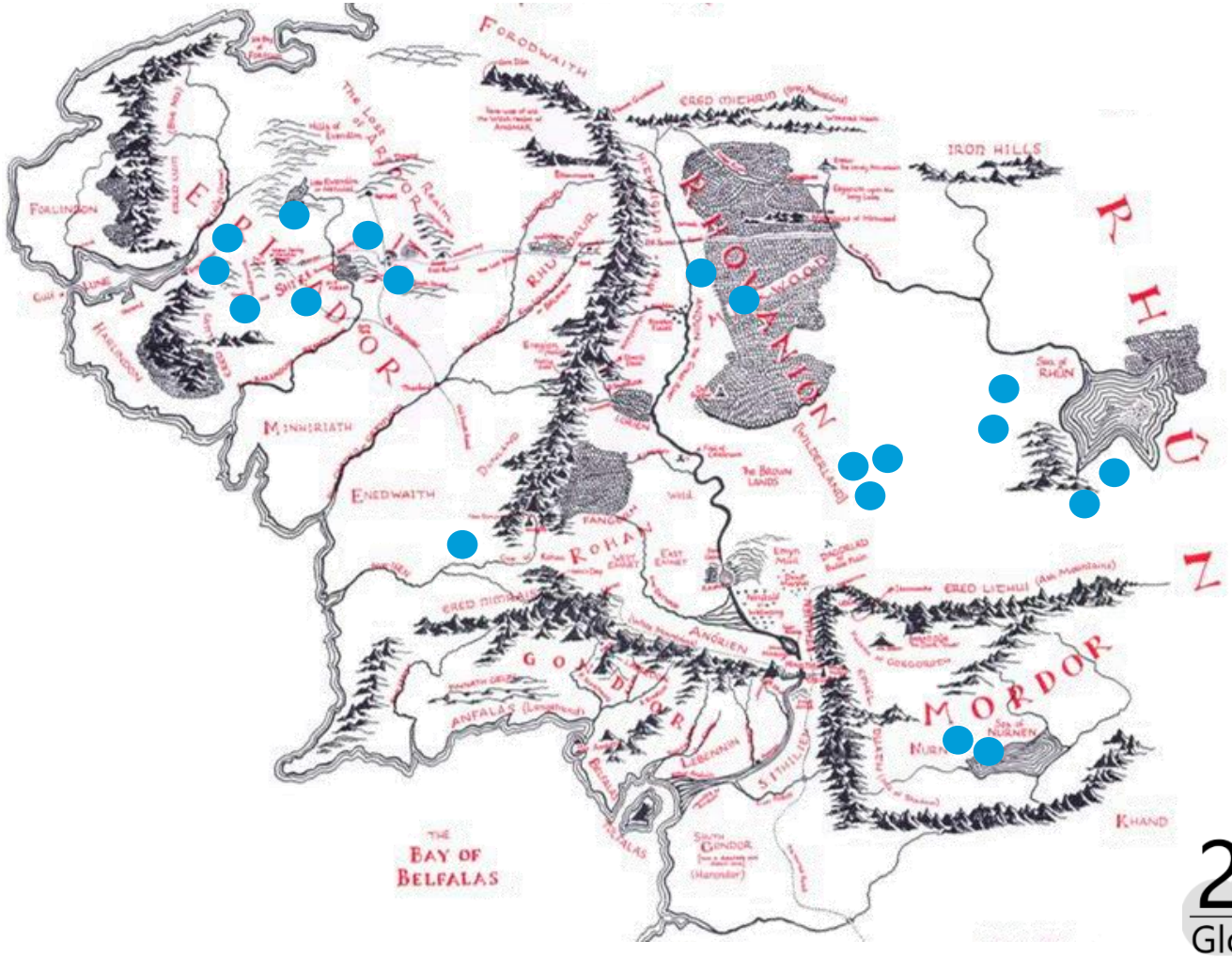


Key Vault Status

Generally Available

Apps offering BYOK via Key Vault:

- Azure RMS*
- SQL Server Transparent Data Encryption
- Azure Storage client SDK
- Azure VM certificate management
- Azure disk encryption – announced
- Office 365 Advanced Encryption – announced
- CloudLink SecureVM
- Brocade Virtual Traffic Manager – Enterprise edition
- Ascertia



2016 Global Azure BOOTCAMP

¿Preguntas?

También en

@iriaq

@jangelfdez

2016 Global Azure BOOTCAMP


ackstorm
Managed Cloud Solutions


ALTRAN


avanade
Results Realized


capside
architects of the digital society


encamina
PIENSA EN COLORES


Insight


intelequia
SOFTWARE SOLUTIONS


KABEL


NECSIA


plain
concepts


SOGETI


SUSE
We adapt. You succeed.


東京'TOKIOTA

Colabora


Microsoft


2016
Global Azure
BOOTCAMP

Thanks!

2016
Global Azure
BOOTCAMP