

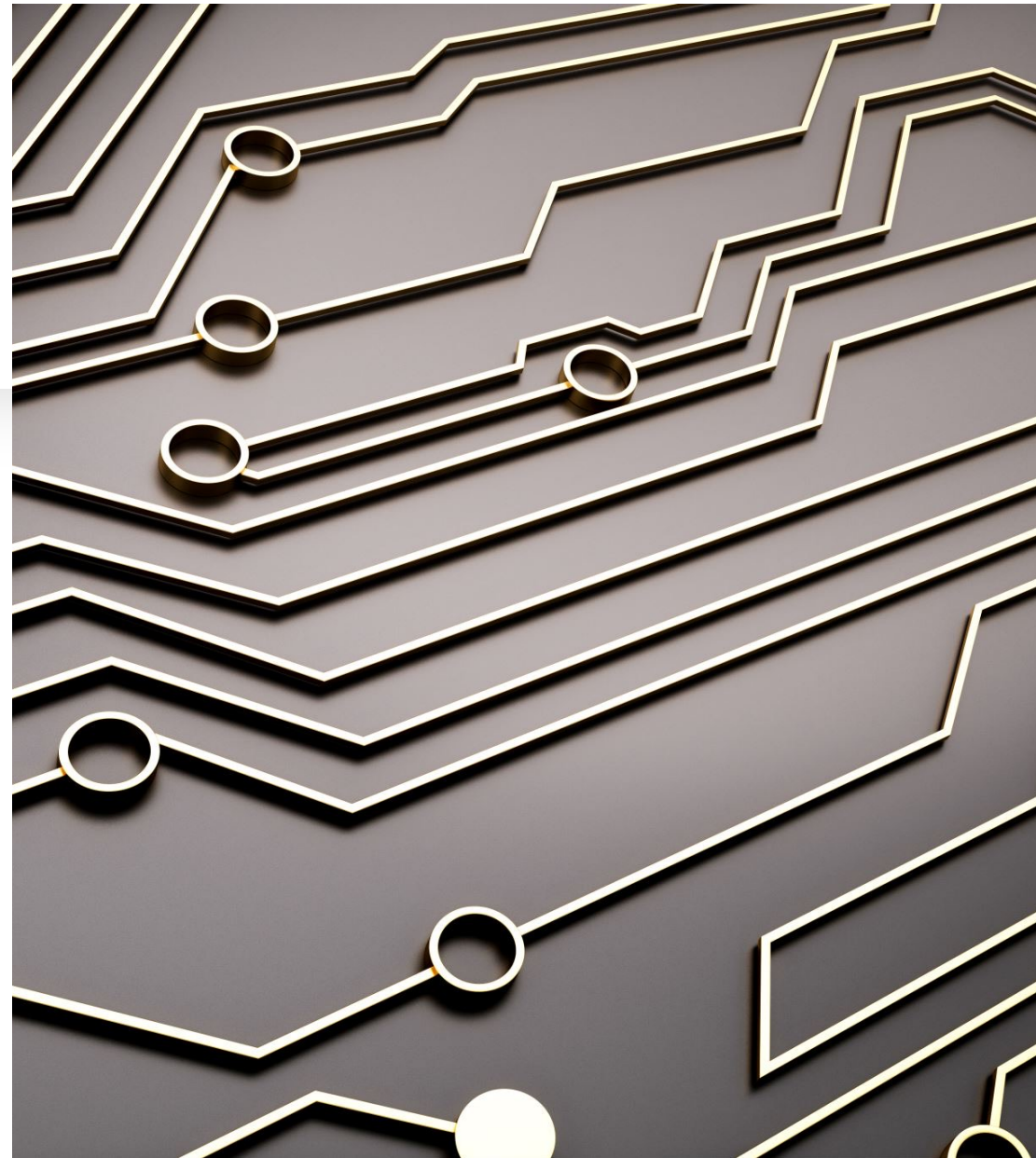


Thales HSM & KSM

Analisi condotta da Luisa Mele

HSM AND CSM

- Key management system is used to provide streamlined management of the entire lifecycle of cryptographic keys according to specific compliance standards, whereas an HSM is the foundation for the secure generation, protection and usage of the keys.
- Hardware Security Mode
- Key management System



KSM

- Generare, proteggere, storing chiavi crittografiche
- Controllare e gestire la rotazione delle chiavi
- Mantenere una copia di backup
- Audit logs
- Cancellare materiale sulle chiavi

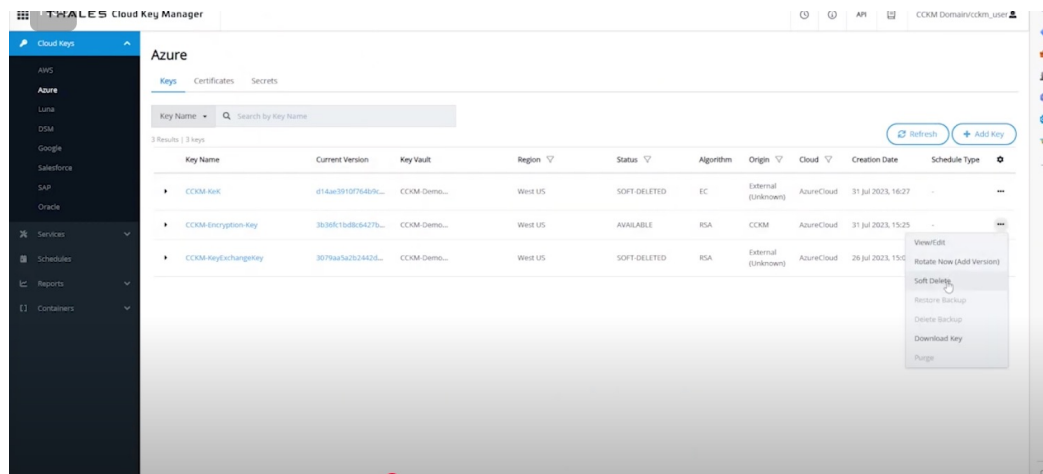


Azure e KSM

- Andare su Azure (nello storage Account) >
- Encryption parameter > Encryption type “Custom managed keys”
- Andare su Thales Interface > Cloud key Manager Tab > Azure Cloud Keys (qua abbiamo visibilità su tutte le chiavi disponibili)
- Tornare su Azure > Fileshare > fare upload di un file (se si ha accesso a encryption-decryption keys) > visualizzare il file

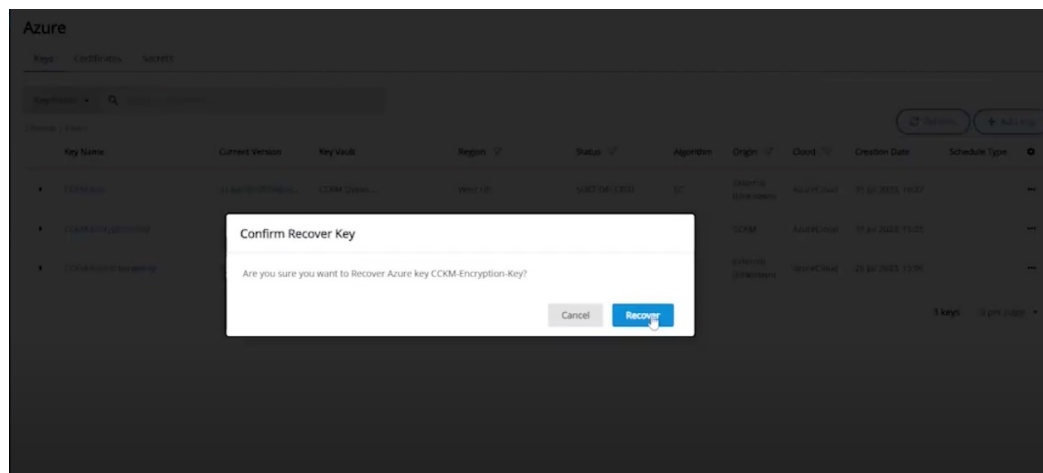


Delete



- Tornare su Thales, andare sul menù a tendina indicato da “-” e cliccare “soft delete”.
- Ora, se torniamo su Azure, non abbiamo più accesso alla share, in quanto abbiamo appena cancellato la chiave di decrittazione.

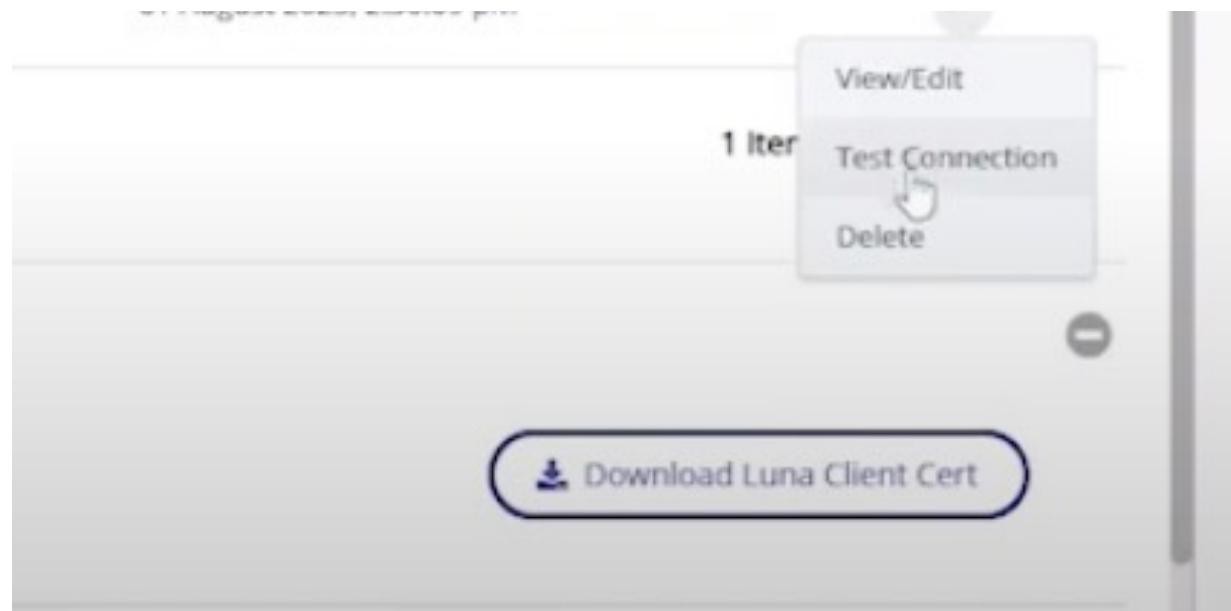
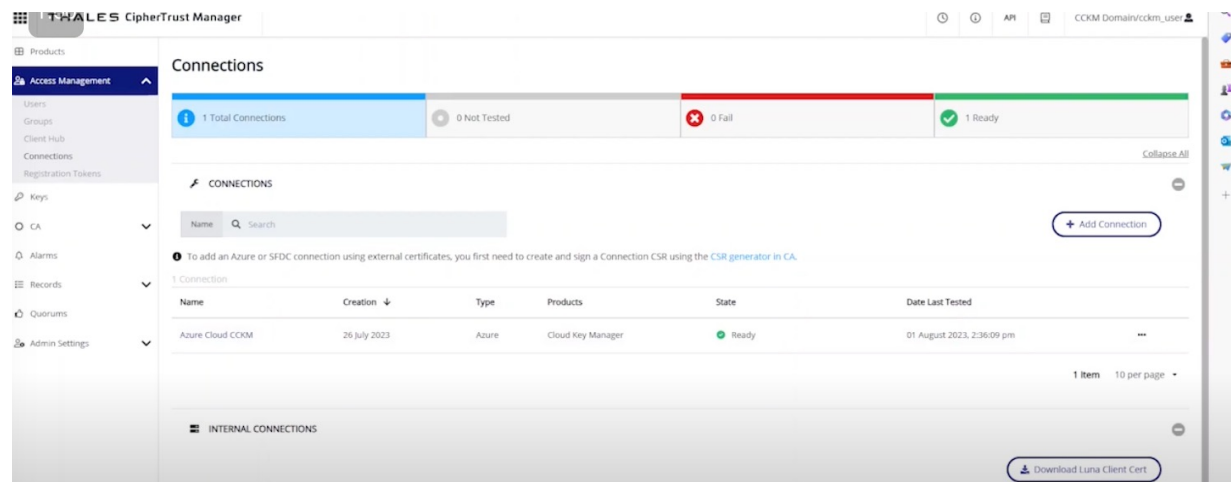
Recovering



- Possiamo ancora recuperare la chiave e avere nuovamente accesso al file

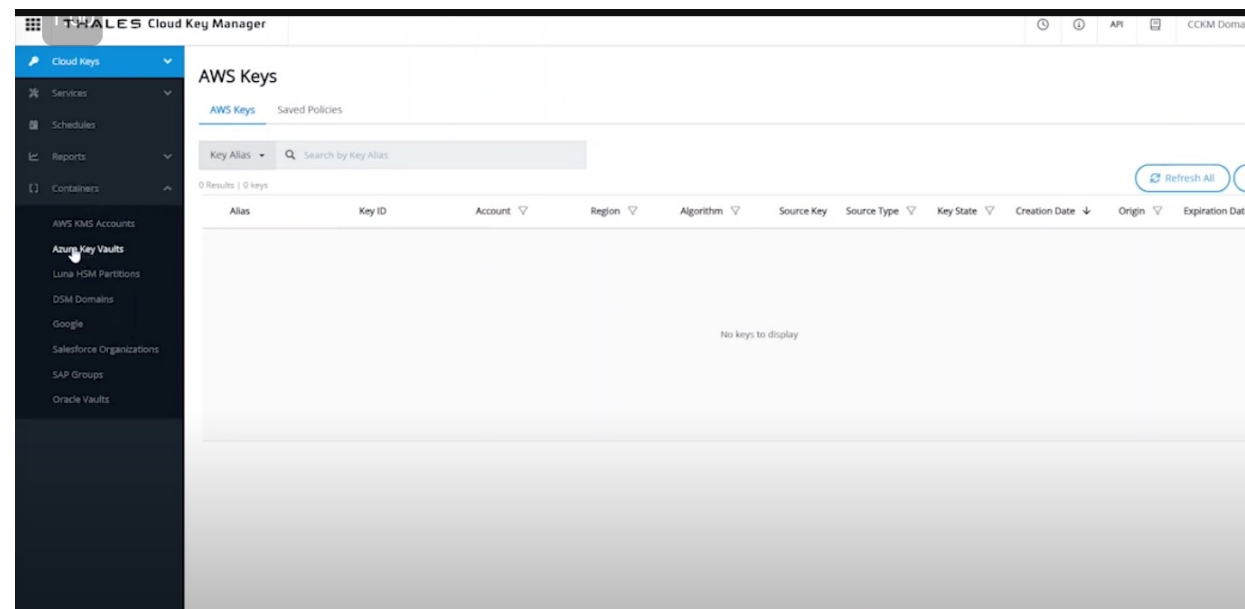
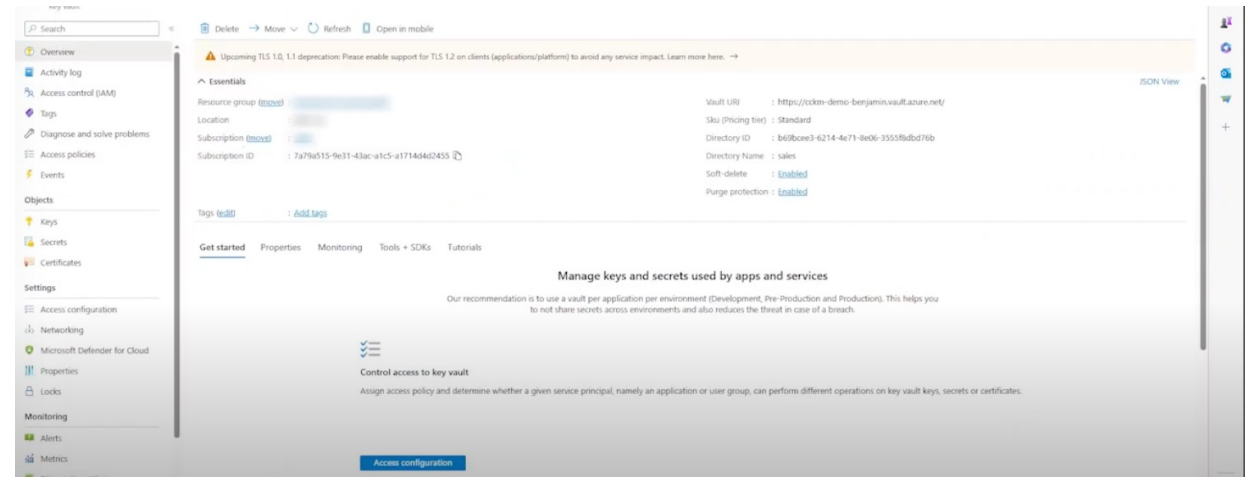
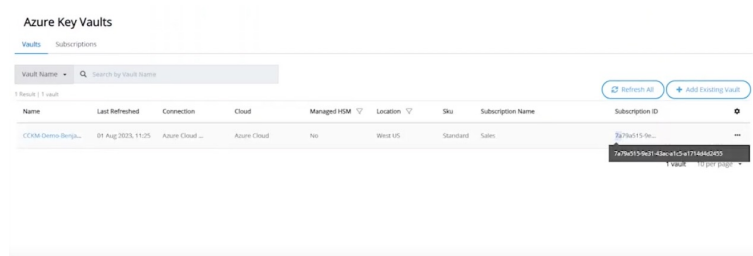
Connessione ad Azure

Da questa interfaccia possiamo gestire la connessione ad Azure, possiamo anche testare la connettività



Key Vault on Azure & Thales

- In questa interfaccia di Azure abbiamo il nostro Key Vault con il subscription ID.
- Il key vault è visibile da Thales come un container con lo stesso ID



Creare nuove chiavi

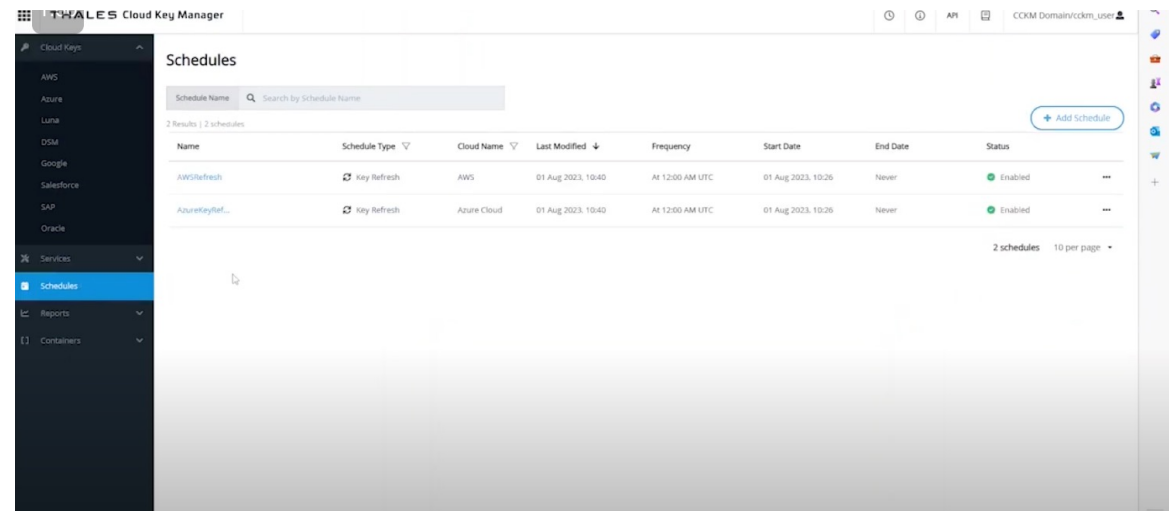
- Da Thales possiamo creare nuove chiavi, scegliere il Vault in cui fare l'upload della chiave, la chiave verrà mostrata su Azure "keys"

The screenshot shows the 'Add Azure Key' dialog box in the Thales Cloud Key Manager interface. The dialog is titled 'Add Azure Key' and has a close button (X) in the top right corner. It features a progress bar with three steps: 1. Select Material Origin (active), 2. Configure Destination (Azure) Key, and 3. Review and Add. Under 'Select Method', there are two options: 'Create/Upload New Key Material' (selected) and 'Clone Existing Key Material'. The 'Create/Upload New Key Material' option has a sub-label: 'Add key material by creating and uploading new source key or creating new native key.' Under 'Select Source', there are four options: 'CipherTrust (Local)', 'Luna HSM', 'Microsoft Azure (Native)', and 'Vormetric DSM'. Each source option has a sub-label describing the upload method. At the bottom right, there are 'Cancel' and 'Next' buttons.

The screenshot shows the 'Add Azure Key' dialog box in the Thales Cloud Key Manager interface, specifically the 'Configure Destination (Azure) Key' step. The dialog has a close button (X) in the top right corner. The progress bar shows three steps: 1. Select Material Origin, 2. Configure Source Key, and 3. Configure Destination (Azure) Key (active). Below the progress bar, there are several fields and checkboxes: 'Azure Key Name' (text input with 'TestKey'), 'Vault' (dropdown menu with 'CCKM-Demo-Benjamin::7a79a515-9e31-43ac-a1c5-a1714d4d2455'), 'Key Type' (radio button selected for 'RSA'), 'Set Activation Date' (checkbox), 'Set Expiration Date' (checkbox), 'Enable Key' (checkbox checked), and 'Key Attributes' (checkboxes for 'Encrypt', 'Decrypt', 'Sign', 'Verify', 'Wrap Key', and 'Unwrap Key', all checked). At the bottom, there are 'Tags (upto 128 characters)' with 'Tag Name' and 'Tag Value' input fields, each with a '0 / 128' character count and a '+' button. At the bottom right, there is a 'Next' button.

Key rotation

- Da “schedules” su Thales, possiamo scegliere la key rotation



Keys in Hardware	keys never leave tamper-proof root of trust in plain text form	keys need to be created, managed and stored securely
Compliance	establish trust with a FIPS 140-2 validated HSM	FIPS 140-2 level 3 HSM secures the PKI encryption key
Key Control	control your keys and ultimately your data	generate keys in on-premises, tamper proof HSM
Disaster Recovery	business continuity	secure copy of key in your possession (DR)
Flexibility	take your keys where you want to go	ability to use the same key in multiple clouds
Secure Backup	hardware to hardware backup	encryption keys need to be securely backed up

Benefits of HSM