Krestfield PKCloud

Key Stores

version 2.1

Overview

Key Stores securely store the PKI and Symmetric keys and certificates. A Key Store can be any one of the following types:

- **Software**
  - The keys and certificates will be stored, encrypted in files. Cryptographic operations will be performed in software

- **PKCS#11 HSM**
  - Keys will be stored in an HSM supporting the PKCS#11 interface
  - Cryptographic operations will also be performed within the hardware device
  - Supported HSMs include:
    - nCipher
    - Thales Luna (including the Data Protection on Demand Cloud HSM)
    - Utimaco
    - AWS CloudHSM

- **PayShield HSM**
  - Keys will be protected by the Thales HSM PayShield device. Cryptographic operations will also be performed within the device
  - Note. Only PKI channels are supported by PayShield HSMs

- **Google KMS**
  - Hosted in the Google Cloud, this key store will use keys hosted in a Google KMS (Key Management Service) Key Ring

- **Azure Key Vault**
  - Hosted in Azure, this key store will use keys hosted in an Azure Key Vault

A Key Store must be configured before any Channels are configured, as a Key Store is required to store channel objects (keys and certificates) and perform any channel cryptographic operations

Configuration

Select the Key Stores menu item and follow the steps below for the Key Store type required

Software Key Store

Click **New Software Key Store** and in the form enter:

- **Key Store Name**
  - Enter a name to reference this Key Store by

- **Key Store Password**
  - Enter the password used to protect the Key Store. This password will be used to generate an AES-256 key which will protect the key files

PKCS#11 HSM

Click **New PKCS#11 HSM** and in the form enter:

- **Key Store Name**
  - Enter a name to reference this Key Store by

- **HSM Model**
  - Select the model of HSM being used from the list. Note, if the particular HSM model is not listed, Generic may be used for an HSM that adheres to the PKCS#11 standard

- **PKCS#11 Library**
  - Enter the full path to the PKCS#11 library file. Note: This is the path local to the PKCloud server and not necessarily the local machine accessing the browser (unless they are the same)

    The HSM must already have been setup on the PKCloud Server including any configuration required for the device (e.g. setting of the Security World for nCipher HSMs)

    For example, the nCipher library on windows could be located at:

    C:\Program Files (x86)\nCipher\nfast\toolkits\pkcs11\cknfast-64.dll

    On a Linux/Unix platform this could be something like:

    /opt/nfast/toolkits/pkcs11/libcknfast.so

- **PKCS#11 Slot**
  - Enter the slot number to be used for the HSM

    This may depend on how the HSM has been configured or vendor specific requirements

    For nCipher HSMs, if an Operator card set has been configured, the slot number will be 1 for the first card set, and increment for any further card sets configured. If using module protection the slot number is usually 0

- **Use module protection**
  - If no password is required to access the HSM (referred to as Module Protection), check this option

    If this is enabled the HSM will not be logged onto when performing operations. Ensure the HSM is configured to allow this. The Key Store Password must still be set as this is still used to encrypt local files associated with the Key Store

- **HSM/Key Store Password**
  - Enter the password required to logon to the HSM

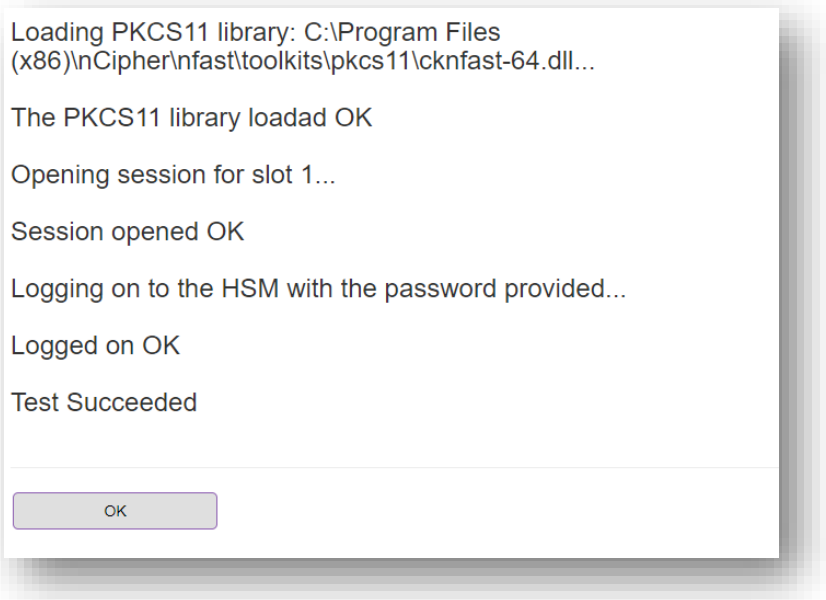
    If using module protection this password can be any strong password and does not need to be configured on the HSM

    For nCipher HSMs, if using an operator card set, the password entered here must match the card set password

    For other HSMs this may be the password of the account configured to access the HSM

Test the Configuration

You may click the **Test** button to confirm these settings. The test will attempt to load the provided library and open a session to the HSM using the details provided



Click **OK** and the click **Add** to save the settings

PayShield HSM

Click the **New PayShield HSM** button and in the form enter

- **Key Store Name**
  - Enter a name to reference this Key Store by
- **IP Address**
  - Enter the IP address of the HSM

    If load-balancing between multiple HSMs, then this IP address will be that of the load-balancer
- **Port**
  - Enter the port number the HSM has been configured to listen on
- **Header Length**
  - Enter the message header length. By default this is 4 unless configured differently on the HSM
- **Connection Timeout (ms)**
  - If the HSM does not respond to a message, the call will timeout (and an error be raised) after this period. Enter the timeout value in milliseconds
- **LMK Type**
  - Select the type of LMK that is loaded on the HSM. It is recommended to configure the PayShield with a Key Block LMK
- **Specify LMK ID**
  - If this option is checked the option to enter the LMK ID will be displayed. If your HSM has multiple LMKs loaded you can specify the one the system will use here. If this is not checked, the default LMK will be used (as specified in the PayShield's security settings)
- **HSM/Key Store Password**
  - Enter the password. This password can be any strong password and does not need to be configured on the HSM. The PayShield does not require a password for authentication

Once all details have been entered click the **Add** button

Google KMS

To access the Google KMS you must have created a Key Ring (from the Security section in the Google Cloud) and a Service Account (from the IAM section). A key pair must also be generated (with Key type = JSON) for the service account and this file downloaded. This file is referred to as the credential file below

Click **New Google KMS** and in the form enter:

- **Key Store Name**
  - Enter a name to reference this Key Store by

- **Project**
  - Enter the project ID of your project as configured in Google Cloud. This can be found when viewing the Project info and will be listed under Project ID. It is often just the lowercase version of the Project name

- **Location**
  - Enter the location of the Key Ring. Key Rings can be created in specific regions or set to be global. When you list your Key Rings in Google Cloud the location will be displayed

- **Key Ring**
  - Enter the name of the Key Ring that has been created e.g. ezsign

- **Credential Filename**
  - Enter the full path to the JSON formatted credential file that would have been downloaded from the Google Cloud console when a key-pair was created for the service account

- **Key Store Password**
  - Enter the password. This password can be any strong password and does not need to be configured in the Google KMS. Google KMS credentials are contained within the credential file. This password will be used to protect information about the Google KMS

Once all details have been entered click the **Add** button

Azure Key Vault

To use Azure Key Vault you must have created a Key Vault from the Azure Portal. The Key Vault must be on the Premium pricing tier as this allows for HSM backed key protection

An application must have been registered in Azure Active Directory and the following information obtained:

- Client ID (also referred to as the App ID)
- Tenant ID
- Key Vault URL
- Client Secret (also just referred to as the password)

The application must have the correct permissions to access the Key Vault and manage its contents. Refer to the Azure Key Vault Configuration note for details

Click **New Azure Key Vault** and in the form enter:

- **Key Store Name**
  - Enter a name to reference this Key Store by
- **Client ID**
  - Enter the Client ID for the registered application
- **Tenant ID**
  - Enter the Tenant ID
- **Key Vault Name**
  - Enter the full URI of the Key Vault. When viewing the Overview of the Key Vault in the Azure portal, this is shown as the DNS Name e.g. https://ezsign.vault.azure.net
- **Client Credential**
  - Enter the Client Credential (or password) that has been assigned to the registered application

Once all details have been entered click the **Add** button