PKCS #11 Proxy

PKCS #11 Proxy

PKCS (Public Key Cryptography Standards) are public-key cryptography standards devised and published by RSA Security LLC, in the early 1990s. PKCS #11 is a standard that provides a way for applications to interact with cryptographic devices in a standardized manner. This allows developers to write software that can communicate with different types of cryptographic hardware without needing to know the specific details of each device.

PKCS #11 is a crucial standard for integrating and using cryptographic hardware, enabling secure and standardized interactions between software applications and hardware security devices.

Cogito provides a PKCS #11 Proxy solution that enables applications to interact with Cogito Hardware Security Modules (HSMs) through the PKCS #11 protocol, appearing as though the HSMs are local to the application.

This approach allows customers to leverage the PKCS #11 API with Cogito HSMs, avoiding the expense and administrative burden of managing their own HSMs.

Since the proxy adheres to the PKCS #11 standard, both new and existing applications can seamlessly integrate with it without requiring any modifications or experiencing differences in behavior.

Benefits

The benefits of PKCS #11 Proxy include:

- Seamless integration with Cogito HSMs using the PKCS #11 protocol.
- Eliminates the need for managing and maintaining physical HSMs, **reducing costs** and administrative overhead.
- Plug and play, **no firmware or drivers** required, simply load the DLL or Link Library into your application.
- **No firewall rules** or network management. Proxy works out of the box.
- Can support **multiple partitions on different hardware** (e.g. a Luna 7 partition used in parallel with an nCipher XC Softcard slot).

Design

The PKCS #11 Proxy is deployed as a Dynamic Link Library (.dll) in Windows and as a Shared Object (.so) in Linux.

The general overview of behavior is as follows:

- The Cogito PKCS #11 Proxy is loaded by your application as a .dll or .so file (as normal for PKCS #11 Applications).
- The Proxy securely authenticates to Jellyfish and retrieves all available HSMs and Partitions for your tenancy.
- The client Application then interfaces with Cogito HSMs as if they were local to it.

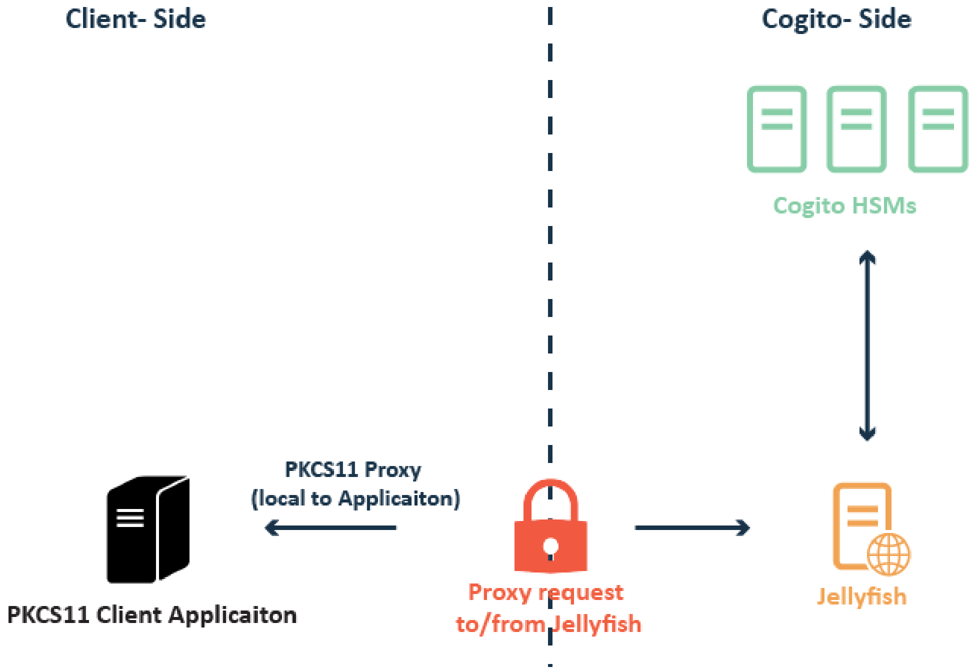

Figure 1- Diagram of traffic through PKCS #11 Proxy

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.