P6R PKCS#11 Integration with Atalla HSM

Technology Alliance Partner Solution Brief

P6R and Micro Focus are committed to ensuring interoperability. The P6R PKCS #1 Library implements v2.40 API of the PKCS#11 specification and meets the requirements for conformance of a PKCS#11 extended provider and authentication token. The PKCS# 11 library allows the definition of any number of KMIP tokens all pointing to the same or different KMIP servers. This allows developers familiar with PKCS 11 to store their keys on a KMIP server without having to learn about the KMIP protocol or KMIP SDKs.

Key benefits of the P6R's PKCS#11 and Atalla HSM Integration

- **Provides a full PKCS#11 API for the Atalla HSM**
- **Manages all keys generated by the Atalla HSM in either a local Sqlite or a local/remote Postgres database**
- **Supports the PKCS#1 *CKA_UNIQUE_ID* attribute that provides a token assigned unique identifier for any object residing on a token**

P6R's PKCS#11 Solution:

P6R's library (https://www.p6r.com/software/skc.html#pkcs11) is a PKCS#11 provider that implements version 2.40 of the PKCS#11 specification. The library supports either types of tokens and also allows a customer to provide their own token types via a *plugin* interface. One of the benefits of the PKCS#11 API is that it provides a standard based keystore API.

The Atalla HSM Solution:

Micro Focus' Atalla Hardware Security Module (HSM) is a payments security module for protecting sensitive data and associated keys for non-cash retail payment transactions, cardholder authentication, and cryptographic keys. Atalla HSM enables data and ecommerce protection and key management operations for PIN translations, payment card verification, production and personalization, electronic funds interchange (EFTPOS, ATM), cash-card reloading, EMV transaction processing, and key generation and injection. Atalla HSM, a PCI-DSS compliant, provides unrivaled protection for AES and other cryptographic keys when safeguarding payment transactions. The HSM protects and manages encryption keys needed for key derivation within the tamper-resistant hardware device.

Micro Focus and P6R Leadership:

- Micro Focus and P6R are long-time active contributors to the OASIS KMIP Technical Committee, KMIP Interop Subgroup, and annual interop demos.
- SKC Secure KMIP Client SDK is compliant with US export controls and obtained the Commodity Classification from the Commerce Department's Bureau of Industry and Security. This classification should help customers with their own export compliance obligations.
- The Atalla HSM is FIPS 140-2 level 3 certificated

About P6R

P6R is a privately held, self- funded and self-sustaining software company founded in 2004. Providing multi-platform solutions to a broad range of businesses, P6R's security products and professional services enable businesses to easily solve their key management and encryption integration challenges with OASIS KMIP and PKCS#11 toolkits and custom clients. P6R partners with customers in an ongoing relationship to develop successful solutions that deliver the highest levels of quality and customer value. P6R has a wide range of expertise in areas including email, ad serving, networking, scalability, and high-availability and computer security.

About Micro Focus

Micro Focus drives leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise we protect the world's largest brands and neutralize breach impact by securing sensitive data-at-rest, in-motion and in-use. Our solutions provide advanced encryption, tokenization and key management that protect sensitive data across enterprise applications, data processing IT, cloud, payments ecosystems, mission critical transactions, storage and big data ecosystems. Voltage and Atalla security solutions solve one of the industry's biggest challenges: how to simplify the protection of sensitive data in even the most complex use cases."

For additional information

Please visit our websites at **software.microfocus.com and P6R.com/software/skc**