gradiant

Future present of technology

Connectivity · Intelligence · Security

BlackICE Connect

Empowering Azure Key Vault

BlackICE Connect by Gradiant is a software provider that allows applications to transparently use cryptographic keys provided by Azure Key Vault.

Azure Key Vault provides Cloud-hosted Hardware Security Module (HSM) services that allow you store the keys and perform cryptographic operations in a cluster of FIPS 140-2 certified HSMs. This way there is no need to provision, configure, patch, and maintain HSMs and key management software which leads to a significant reduction in costs. However, many applications need to be modified to use Azure Key Vault because it does not support the most common standard cryptographic providers. Using BlackICE Connect is possible to benefit from the advantages offered by a Cloud based key management service:

- ✓ **Transparently use the key stored in cloud-hosted HSMs**. Effortlessly transform your application to make the most of Cloud key management services.
- ✓ **Reduction in costs.** Improve key security without the hardness and costs of HSM's provision, configurations and management.
- ✓ **Scalability and availability.** The Azure Cloud will also provide scalability and availability to meet applications requirements and match peak demand.

Functionalities

A. Seamless integration with Azure Key Vault

- ✓ By mean of BlackICE Connect, those applications supporting crypto providers natively will interact with Azure Key Vault without modifying any line of code

B. Support for the most common standard crypto providers

- ✓ CNG Key Storage Provider
- ✓ PKCS#11
- ✓ JCE
- ✓ KMIP (ongoing)

C. Secure Key Management

- ✓ Cloud-hosted HSMs certified FIPS 140-2 for key management.
- ✓ Cryptographic keys never leave the Azure Key Vault secure environment
- ✓ No need to worry about configurations, clustering, scaling, patching or installing on-premises HSMs

D. Cryptographic Algorithms

- ✓ RSA for asymmetric encryption and signature purposes
- ✓ ECDSA for signature purpose

Proven applications

A. PKI services:

- ✓ MS Active Directory Certificate Services (ADCS)
- ✓ EJBCA

B. Email signature and encryption (SMIME certificates):

- ✓ MS Outlook
- ✓ Thunderbird

C. Document signature:

- ✓ MS Office suite
- ✓ Adobe
- ✓ SealSign
- ✓ AutoFirma

D. Browsers:

- ✓ Internet Explorer
- ✓ MS Edge
- ✓ Mozilla Firefox
- ✓ Google Chrome

E. Others applications:

- ✓ Windows Certificate Store
- ✓ SecureBlackBox
- ✓ Apache Tomcat SSL
- ✓ OpenStack Barbican
- ✓ OpenVPN
- ✓ Etc.

Supported operating systems

- ✓ Windows Server 2008, 2012, 2016 for 64 bits
- ✓ Windows Desktop Vista, 8, 8.1, 10 for 32 and 64 bits
- ✓ Linux Server for 32 and 64 bits
- ✓ Linux Desktop for 32 and 64 bits

Configuration and installation

- ✓ Installation and configuration through the **BlackICE Connect installer**
- ✓ Configuration file is protected by an user passphrase or PIN

Requirements

- ✓ The customer will need an active Azure account.