What's New 'Cliff Notes'

SmartKey 2020.3

SmartKey 2020.3 delivers a set of new features enhancing SmartKey capabilities.

SmartKey Direct Access

Direct Access enables customers to connect their Colocation and Network Edge assets to SmartKey via a direct private route, enabling you to bypass lengthy routes over the public internet.

Tokenization Security Object Type

Tokenization eliminates the link to sensitive data and is used in credit card processing to reduce or eliminate breaches. This is a highly secure method of protecting payment credentials which include substituting sensitive data such as credit card/account numbers with a one-time number known as a token that has no relationship to a person or their account. The 16-digit account number is replaced with a randomly generated alphanumeric ID.

HSM (Hardware Security Module) Gateway

For customers who would like to consolidate their entire Key Management needs to SmartKey and gradually migrate to SmartKey without impact on their existing security posture, we have introduced HSM Gateway. HSM Gateway is a way to link existing HSMs or external Key Management Systems (KMS) to SmartKey.

Added LDAP as an App Authentication method

This release has added LDAP to the Authentication methods that allows an application to authenticate to SmartKey. With LDAP, the app can use Active Directory (AD) credentials to authenticate. When this option is selected, you will be presented with a list of enrolled external directories and can select a directory to use. SmartKey will

look up the app by `app_id`, find the corresponding external directory, and present the credential to it to authenticate.

Apps with LDAP authentication methods can have either normal authorization or use LDAP authorization. Authorization for an application extends the App's authorization model to tie it to group membership in an LDAP compliant directory.

Added support for RSA key as wrapping/unwrapping key for symmetric key import/export operation

Symmetric keys can now be wrapped/unwrapped using an RSA key during an import/-export operation.

Added support for importing/exporting HMAC keys as components

Previously, only AES, DES, or DES3 type security objects can be imported/exported as components. We have now added HMAC to the list of security object types that can be imported/exported as components.

Other Enhancements

- Fixed audit log auto-refresh.
- Upgraded Cassandra DB to 3.11.8
- Ubuntu packages updated for security fixes.
- Enhanced KMIP Server: Added support for Locate with cryptographic parameters.
- Fixed ED25519 Signature to **NOT** pre-hash by default in JCE client.