What's New 'Cliff Notes'

SmartKey 2021.2

SmartKey 2021.2 introduces enhancements to authentication, tokenization and key rotation.

Subject Alternative Name (SAN) checking for Trusted CA app authentication

This release adds support for checking SAN such as DNS Name, IP Address, and Directory Name for app authentication of type Trusted CA.

More details can be found at: Authentication.

Added more Tokenization data types

We have added the following additional tokenization data types.

- General
  - IP address (v4)
  - Email address
- Identification numbers (USA)
  - Driver's license
  - Individual taxpayer ID
  - Employer ID (EIN)
- Military service number (USA)
  - Army and Airforce service number
  - Navy service number
  - Coast guard service number

- Marine corps service number
- Military offices service number

More details can be found at: Tokenization.

Quorum policy for key rotation

Key rotation is now a sensitive operation and will require quorum approval if quorum policy is enabled for the SmartKey group.

Secret rotation

Secrets can now be rotated. A history of all previous versions of the secret will be logged. Rotation allows adding new object values for the secrets.

KMIP support for Tape Library Profile

This profile specifies the use of the KMIP Application Specific Information (ASI) attribute in the KMIP server.

API Changes

- Batch API support for HMAC - This release adds a new batch API in the 'Digest' section of REST API for Mac and MacVerify.
- Added support for encrypted PKCS#8 format.

Other Enhancements

- Audit logs have been migrated to Cassandra from Elastisearch database.
- Upgraded Cassandra DB to 3.11.10.
- The Amazon SES signature that is used for sending an email using Amazon SES is migrated to the latest version (version 4) which offers enhanced security for authentication and authorization of Amazon SES users.
- UI/Proxy containers updated to NGINX 1.19.8.

- Disabled weak cipher suites on nginx-proxy.
- The backend priority number of a HSM will now be displayed when there are multiple HSM nodes.
- When configuring an AWS group, you can now add a custom AWS URL.
- Virtual keys are now detected and marked in a SmartKey HSM/AWS KMS group during a key sync operation when their source keys are deleted from the HSM/AWS KMS.
- Added quick filter to distinguish between Regular groups and HSM/AWS KMS groups in the Groups table view.
- With this release, the following actions for an App will have zero downtime:
    - You can configure a period of time which the old App API key can continue to work while regenerating a new API Key.
    - You can configure a period of time which the previous authentication method will continue to work while changing to a new app authentication method.
- Under cryptographic policy, when there are no non-compliant keys, selecting “Limit Usage” causes confusion when all the key operations are permitted in the policy. This is resolved by adding more context to the description of the Limit Usage option, changing the order of the section by moving “Handling existing non-compliant keys” above the “Restrict key operations” section.
- AWS/HSM:
    - Fixed an issue where Test Connection was always successful for AWS KMS group when wrong authentication details are provided.
    - Fixed an issue where the Test Connection status is shown incorrectly on another node when the previous node was removed from the HSM node list.
    - Fixed duplicate HSM node ordering value.
    - Fixed an issue where changing an HSM node from Custom CA to Global Root CA was causing the client key to be sent as an empty string instead of null.

    - Fixed issue of two HSMs nodes having the same hsm_order value after one of the HSM nodes is deleted.
    - Copy Key is disabled for AWS KMS virtual keys.
    - Fixed HSM node certificate issues:
        - When Client Certs are added and removed, it does not show a null value.
        - When editing an HSM group's Certificate Configuration, you can save the certificate configuration by entering only the Client Certificate value without the Client Key (Private Key).
    - Fixed issue where the HSM key scan operation failed when you remove a public key from a key-pair in HSM that also contains a private key.
    - Fixed issue where integrating HSMG with nCipher fails with error message "pkcs11: 00000000 Error: Module 1 has failed".
- Fixed issue when restoring the cluster from backup, if a delete operation is performed on the restored data it was unable to delete the data completely.
- Fixed issue where key rotation schedule was drifting by 5 minutes.
- Fixed error code translation for Google EKMS errors.
- Fixed issue where sustained throughput was degraded if the Cassandra audit-log feature is enabled.
- Fixed UI by showing a clear message in the diff window of changes made in Account quorum approval policy and Crypto policy during the quorum approval process.
- Internal NTP docker image updated to Ubuntu 20.04 to address security issues in the previous version.
- Fixed an issue when it was possible to create keys with "App Manageable" permission even when it was disabled in cryptographic policy.
- Fixed bad link in Approval request emails.
- Fixes to etcd certificate renewal.