PrimeKey PKI Appliance 3.3.0 Released

2019-05-23 - Rubina Akram - 0 Comments - in PrimeKey Release Information

PrimeKey PKI Appliance 3.3.0 Released

PKI Appliance 3.3.0 introduces major updates for EJBCA and SignServer. Additionally, more improvements have been implemented under the hood. The runtime environment for EJBCA, SignServer and WebConf has been updated to Java 1.8 and WildFly 14. Furthermore with this release, we are introducing the availability of a new PKCS#11 implementation to access the HSM. This will allow us, in the future, to add further features and improvements related to the HSM integration.

Below you can find the list of the most relevant updates.

New Features:

* EJBCA Enterprise 7.0.1.4 - Please check out EJBCA release notes for further information: https://download.primekey.com/docs/EJBCA-Enterprise/latest/EJBCA_7.0.1_Release_Notes.html
* SignServer 5.0.0 - Please check out SignServer release notes for further information: https://download.primekey.com/docs/SignServer-Enterprise/current/SignServer_5.0_Release_Notes.html
* Support for PKCS#11 R2. Please note that when updating an existing PKCS#11 R1 installation, it will keep using PKCS#11 R1. The same is true for restoring a backup from a PKCS#11 R1 setup. New installations with PKCS#11 R1 are still possible, but discouraged.
* Support packages can now be generated during the installation process as well.
* WebConf now offers a button to restart EJBCA and SignServer.

Changes and bug fixes:

* The runtime environment has been updated to Java 1.8.0 and Wildfly 14.
* Additional checks are now implemented to confirm that the backups have been completed.
* In case of smart card activated slots with PKCS#11 R2, smart card interactions are retried on failure (eg. wrong PIN) on a best-effort basis.

* PKCS#11 R2: cluster key synchronization package restore does not delete keys, only adds missing keys and overwrites differing keys that have the same alias. To delete a key, it has to be manually deleted on all nodes.

* Randomised passwords are now supported for the internal database.
* The TLS settings have been Hardened in Apache.
* EJBCA and SignServer are executed as unprivileged user.
* Improved robustness of cluster key synchronization package handling.

Known issues and limitations:
* While smart card activated slots are supported with PKCS#11 R2, "FIPS restrictions applied" mode is not.
* When installing updates on a PKI Appliance running 3.2.0, make sure to unplug any USB sticks before performing the update.
* When restoring large backups coming from EJBCA versions older than 6.6.0, after the restore and reboot EJBCA will not be available for some time due to the database schema change and the need to reindex. For a full database of a Model M, it takes about an hour to reindex the database. An additional reboot is required to finalize the change.
* For cluster backups taken on versions 2.4 up to 2.8 - when restoring the first backup onto 3.3.0 version the cluster configuration will be deleted and it is needed to add the IP addresses of all the other nodes manually before
proceeding with the cluster setup.
* Version 3.3.0 does not support restoring backups of versions older than 2.4.0.
* The second generation hardware version offers four ethernet ports. Only two of them are usable at the moment, but support for the disabled ethernet ports will be added in future versions.
* Due to a firmware limitation, the PKI Appliance only becomes reachable when both management and application ethernet ports are successfully connected to a network.
* Ethernet ports might not establish a link if the network cables have been connected after powering on the device.
* PeerConnector setup does not support Diffie Hellman key agreement. To setup a peer system, please switch to RSA algorithm before adding the PeerConnector.
* "FIPS restrictions applied" mode is currently not available on appliances of the second generation hardware version because it is not available on that HSM generation. Operation in FIPS mode will be added in future releases.

Please find the detailed release notes here.