Eliminate the Threat of Compromised CA Keys

Open Source PKI Software and Hardware-Backed Security for Critical Data

PrimeKey and Yubico together simplify and secure the management of cryptographic keys with PrimeKey's EJBCA, an open source public key infrastructure (PKI) certificate authority (CA), and the YubiHSM 2, a cost-effective ultra-portable hardware security module (HSM). PrimeKey EJBCA enables customers to leverage the YubiHSM 2 for a range of PKI solutions within their organization.

Alex Yakubov, VP Partner Marketing:

"Collaborating with PrimeKey for support of EJBCA on the YubiHSM 2 introduces our technology to organizations where open source is preferred or even required. The YubiHSM 2 now supports two certificate authorities—Microsoft Windows CA and EJBCA— offering greater flexibility to organizations looking to secure their most important data with an HSM."

IT security breaches are impacting not just the end-user's credentials, but also secrets stored on corporate servers. Breaches involving lost/compromised CA keys can lead to significant financial and reputational damage.

Among the organizations who have experienced security incidents of this nature, the biggest negative impact results in disrupted business activities, followed by reduced employee productivity, and the impact on IT staff having to triage and remediate the security incident[1]. Security breaches are also expensive costing companies an average of $3.86 million per breach in 2018[2].

In PKI, the secure generation and usage of CA keys are fundamental to the overall security of the digital identities issued to people, software, IT infrastructure components, and devices. Together, Yubico's YubiHSM 2 and PrimeKey EJBCA Enterprise combine hardware-backed cryptographic protection with flexible PKI software to keep critical data safe.

PrimeKey EJBCA Enterprise is a PKI software that customers can use with the YubiHSM 2. The CA keys that are stored in YubiHSM 2 are generated and protected by the cryptographic hardware, which mitigates the risk for the keys to be compromised or stolen.

In addition, PrimeKey and Yubico proactively engage with the developer community. Both offer open source software and tools for implementing PrimeKey's EJBCA and the YubiHSM 2. EJBCA Community is PrimeKey's free PKI Software, an outstanding tool for those who don't require more advanced PKI features or guaranteed certifications and regulations.

Robust Open Source PKI Security & Hardware Protection for Cryptographic Keys

Customers can now leverage PrimeKey's open source EJBCA to secure cryptographic keys in the YubiHSM 2 both in high security governmental applications and various industries in the private sector.

Storing cryptographic keys in the YubiHSM 2 offers superior hardware-based security, and eliminates malware and remote attackers from being able to copy them.

[1] Cybersecurity Trends 2017 Spotlight Report, ISC2

[2] 2018 Cost of Data Breach Study, Ponemon Institute Research Report

PrimeKey | yubico

Designed for Flexibility, Scalability & Ease of Integration

The inherent design of EJBCA opens up a highly scalable, multipurpose PKI solution that enables the management of several parallel PKI hierarchies within the same deployment. The ultra portable YubiHSM 2 enables organizations to leverage the security of an HSM in environments where traditional HSMs could not fit.

Both designed for security and scalability, the YubiHSM 2 and EJBCA provide open source resources for developers to easily and seamlessly implement support for the joint solution. Developers can access the features of the joint solution using the open source YubiHSM 2 software development kit (SDK) and setup tool for EJBCA.

Expanded Use Cases & Integration Scenarios

Customers looking for an affordable and reliable joint HSM and PKI software solution now have easier access than ever before. By offering an alternative to the Microsoft Windows CA, PrimeKey's open source EJBCA Enterprise and the YubiHSM

2 allow organizations to leverage standard protocols and interfaces, including for example CMP, SCEP, EST and ACME, and development APIs to enable and address a broad range of use cases and integration scenarios.

Get Started with YubiHSM 2 + PrimeKey EJBCA Community:
https://www.yubico.com/works-with-yubikey/catalog/prime-key-ejbca-community/

Get Started with YubiHSM 2 + PrimeKey EJBCA Enterprise:
https://www.yubico.com/works-with-yubikey/catalog/prime-key-ejbca-enterprise/

> **Chris Job, Team Leader, PrimeKey Professional Services:**
>
> "The priorities for us in developing PrimeKey's EJBCA have always been flexibility and the ability to support different use cases. With the YubiHSM 2, we enable a cost efficient and portable HSM alternative that simplifies the process to secure your CA keys."

Joint Features & Benefits

Strong Security
The YubiHSM 2 and PrimeKey's EJBCA come with open source and standards-based cryptographic toolboxes to enable strong protection of cryptographic keys.

Practical Deployment
The size of the YubiHSM 2 is ideal for non-traditional scenarios where HSMs were never previously considered and security may have been potentially sacrificed. Its seamless integration with Common Criteria certified PrimeKey EJBCA Enterprise makes deployment easy for industries that prioritize IT security and integrity.

Support New Use Cases
PrimeKey EJBCA enable organizations to leverage the YubiHSM 2 for non-traditional applications and modern use cases, such as IoT environments. Because of the reduced cost and complexity, organizations of various sizes can start to test the benefits of the YubiHSM 2 for their products.