PrimeKey®
Solution Brief

The next level of PKI Infrastructure deployment agility

With the combination of Public Key Infrastructure (PKI) by PrimeKey's EJBCA® Enterprise and Unbound Key Control (UKC) by Unbound Security, it is no longer necessary to deploy and manage a physical Hardware Security Module (HSM). UKC is a pure-software virtual HSM and key management solution that combines the security of a traditional HSM with the flexibility and agility of software.

The connected society enables the availability of massive amounts of data and new disruptive solutions and business models evolve in an agile way. Continuous development, deployment and optimization enables companies to start small and to grow with a successful business case. For the new businesses and new business models, it is important to have the relevant security implemented from the start. Adding security at a later stage often result in a less effective and more costly security solution. This is why IT infrastructure and IT security need to follow this evolution and offer flexible and cost-effective deployment options, adapted to the business models of today.

Unbound Security and PrimeKey have developed a partnership where we together enhance PrimeKey's PKI software EJBCA Enterprise with support for the Unbound Key Control solution. Together, the two products deliver the next level of PKI agility.

unbound security

PrimeKey

Securing the root key of a CA in PKI

When using PKI solutions there is a great need to secure the root key of a Certificate Authority (CA). If a CA's root key is compromised the credibility of the CA is broken, resulting in all issued transactions, processes etc. being compromised. Therefore, in a PKI environment – particularly one integral to business processes, financial transactions, or access controls – it is essential that private keys be guarded with the highest level of security possible. An attacker with knowledge of the private key can create new smartcards/tokens and have unlimited dormant access to the CA's network.

EJBCA Enterprise and UKC

With the partnership between PrimeKey and Unbound, EJBCA Enterprise integrates with UKC to secure the Root CA private key as well as policy, intermediate and issuing CA keys. In addition, EJBCA Enterprise makes use of the UKC for protection of logfile signing keys and TLS key used for secure authentication to and from EJBCA Registration Authority, EJBCA Validation Authority and EJBCA SignServer Enterprise.

Benefits

Elastic and Scalable

A combined solution that follow your needs. No extra hardware needed when expanding your infrastructure.

Transparent and seamless integration

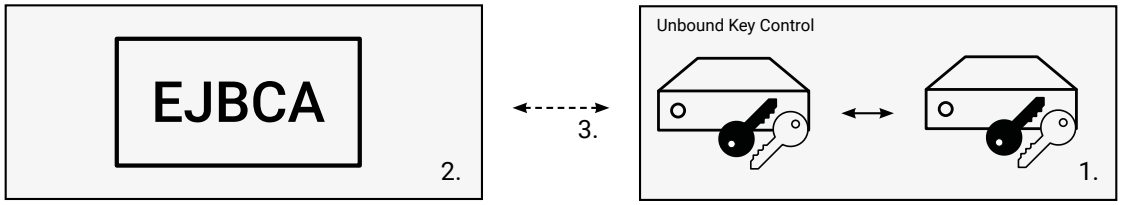
The integration of UKC is the same as with traditional HSMs.

Mathematically proven security guarantee

The key material never exists in the clear throughout its lifecycle including creation, in-use and at-rest.

Multi-site, Multi-Cloud Hybrid IT support

Control and manage keys anywhere; on-premise, in the cloud or in hybrid deployments. QuoVadis provides managed public key infrastructure services for enterprises and governments.



1. Generate private-public key pair (crypto-token)
2. Select the Unbound crypto-token
3. Sign CSR (Certificate Signing Request) with private key stored in UKC

About Unbound Security

Unbound Security equips companies with the first pure-software solution that protects secrets such as cryptographic keys, credentials or other private data by ensuring they never exist anywhere in complete form. The Unbound Distributed Trust Platform stands as a new foundation for trust using secure multiparty computation to ensure secrets are always split into multiple shares and thereby eliminate any single point of compromise.

About PrimeKey

PrimeKey is one of the world's leading companies for PKI and digital signing solutions. With our products EJBCA, SignServer and the PKI Appliance, we deliver the capability to implement an enterprise grade PKI system ready to support solutions such as IoT, e-ID, e-Passports, authentication, digital signatures, code signing, digital identities, and validation; all solutions where digital certificates would be a main enabler.

SALES@PRIMEKEY.COM
+46 873 561 01
WWW.PRIMEKEY.COM

PrimeKey