

# PKI Appliance by PrimeKey

# PKI Appliance Model specification

With PrimeKey PKI Appliance you will get your PKI projects done in time and on budget. PrimeKey's purpose-built PKI Appliance is the all-in-one solution for a Public Key Infrastructure with built-in high availability and reliability functionality. It provides a ready to use EJBCA Enterprise with an integrated Hardware Security Module (HSM) and a comprehensive management interface.



# PKI Appliance Model Specification

PrimeKey PKI Appliance is the easiest and most efficient way to deploy and manage an enterprise PKI system. With a pre-packaged solution you are quickly up and running without the hassles of complex installation and integration procedures.

PrimeKey PKI Appliance offers a complete feature set needed to operate a full blown, highly available PKI. It is based on PrimeKey EJBCA Enterprise, with easy to use management functions, high-performance hardware and a built-in FIPS 140-2 Level 3 certified Hardware Security Module (HSM).

Depending on the requirements PrimeKey offers four different PKI appliance models to address different needs.

## Small

PKI Appliance Small includes EJBCA Enterprise with a core library for Certificate Authority (CA) functionality for an unlimited number of CAs. EJBCA Enterprise is certified with Common Criteria EAL 4+. The Small model supports operating multiple, independent PKI hierarchies within one installation and a Registration Authority (RA) with role based access control and approval mechanisms. PKI Appliance Small is ideal for an offline Root CA in a PKI deployment.

## Medium

In addition to the functionality of PKI Appliance Small, the Medium model also includes highly flexible integration interfaces based on web services, REST API

and support for CMP v2 RFC 4210, SCEP, EST. Certificate data is synchronized in real-time between CA and VA, and between CA and RA instances via dedicated secure channels called Peer Systems.

## Large

The largest model of PKI Appliance includes all functionality you find in the two previous models and an extended capacity when it comes to certificate storage. PKI Appliance Large supports 20 million certificates.

## Validation Authority (VA)

The PKI Appliance VA model includes support for CRL distribution and OCSP. Revocation information is synchronized in real-time between CA and VA via dedicated secure channels called Peer Connectors. Utilizing dedicated VA Appliances can massively increase security of an infrastructure as it is best placed in the DMZ and isolated from the CA Appliances allowing only one way secure connections from CA to VA instances.

PKI Appliance	Small	Medium	Large	Validation Authority
Software stack	PrimeKey EJBCA Enterprise & Prime LFS*	PrimeKey EJBCA Enterprise & Prime LFS*	PrimeKey EJBCA Enterprise & Prime LFS*	PrimeKey EJBCA Enterprise & Prime LFS*
<b>Protocols &amp; API's</b>				
OCSP	-	☒ -	-	✓
SCEP	-	✓	✓	-
CMP	-	✓	✓	-
EST	-	✓	✓	-
WebServices API	-	✓	✓	✓
REST API	-	✓	✓	-
CLI	✓	✓	✓	✓
<b>Key Features</b>				
Certificate Capacity	<100	8 M	20 M	N/A
Secure & Automated Backup Mechanism	✓	✓	✓	✓
2 Factor Authentication	✓	✓	✓	✓
FIPS 140/2 Level 3 validated HSM inside	✓	✓	✓	✓
Dedicated Mng & App Interfaces	✓	✓	✓	✓
Clustering	-	✓	✓	✓
Dual power supply	✓	✓	✓	✓
SNMP, Syslog, Audit Log	✓	✓	✓	✓
<b>Accessories</b>				
SmartCards	10	10	10	-
PinPad Reader	1	1	1	-
HSM Backup batteries	-	✓	✓	-
External Battery adapter	✓	-	-	-
<b>Performance (opp/sec)</b>	<b>Cert. issuance</b>			<b>Responses</b>
	<b>Audit log on/off</b>			<b>Audit log off</b>
RSA 1024 SHA 1 with RSA	5/30	28/101	28/101	450
RSA 2048 SHA 256 with RSA	1/10	26/79	26/79	80
RSA 4096 SHA 512 with RSA	0,5/0,5	9/11	9/11	11
EC secp256r1 SHA256withECDSA	5/43	25/98	25/98	490
EC secp384r1 SHA384withECDSA	4/21	24/95	24/95	380
EC secp521r1 SHA512withECDSA	3/9	23/88	23/88	190
<b>Technical specifications</b>				
Form Factor	2U			
Dimensions	88,4 x 430 x 633mm (3 1/2 x 17 x 25 inch)			
Weight	12,5kg (27.5lb)			
Operational Environment	+10°C - +50°C (+50°F - 122°F)			
Storage Environment	-10°C +55°C (+14°F - 131°F)			
Safety Agency Approval	CE, RoHS, FCC			
Power Supply	Dual 500W			
AC Power	110/240V, 50/60Hz			
Power Consumption	typ. 80W, max 135W			

For testing purposes, it is possible to run CA, VA and RA on one single instance of the appliance

\* = PrimeKey Linux From Scratch

## About PrimeKey

PrimeKey Solutions AB is one of the world's leading companies for PKI solutions. PrimeKey has developed successful solutions, such as EJBCA Enterprise, SignServer Enterprise and PrimeKey PKI Appliance. PrimeKey is a pioneer in open source security software that provides businesses and organisations around the world with the ability to implement security solutions such as e-ID, e-Passports, authentication, digital signatures, unified digital identities and validation. PrimeKey has its head office in Stockholm, Sweden.

© PrimeKey Solutions AB  
All rights reserved  
sales@primekey.com  
+46 873 561 01

[www.primekey.com](http://www.primekey.com)

