Registration Authority
For EJBCA Enterprise

A sophisticated toolbox for **certificate enrollment**

The EJBCA RA provides a sophisticated toolbox for a user to enroll for any certificate type, whether for a key pair generated for you and stored on the CA or to sign your own key pair by Certificate Signing Request (CSR).

PrimeKey

Registration Authority
For EJBCA Enterprise

The EJBCA RA provides a sophisticated toolbox for enrollment of any certificate type. As an external entity to the Certificate Authority (CA), it allows for an additional layer of security around the CA.

Why use an RA?
A Certificate Authority is a fine thing to have; it enrollsand issues certificates, it manages their life cycles and it revokes them when needed. Yet a CA has no purpose without a means and a method to interact with the users of its certificates, whether these are machines, people or software. While machines and computers can use online protocols such as CMP and SCEP to enroll, human users need an interface with which to issue a request to the CA, and this is what's called a Registration Authority.In the interest of security, both physical and electronic, it is often desirable to physically separate CA and RA, allowing one to reside in a secure environment with minimal access, while the other can resize in a DMZ or even publicly.
In short, an RA is the CA's face to the world.

Certificate Management
The EJBCA RA provides a sophisticated toolbox for a user to enroll for any certificate type, whether predefined or defined on the CA, either by submitting a Certificate Signing Request (CSR) to have a local key pair signed, or by requesting a certificate based on a key pair stored on the CA. An intuitive interface will guide the user, whether an administrator or the end client, through the entire process. If certificate issuance can't be immediate, users can request to either have their certificates delivered by e-mail or can retrieve them from the RA at a later date using a retrieval code.

Request Management
PrimeKey has implemented a brand new approval process where approvals can be defined as profiles, which in themselves can be partitioned up into segments to be approved by different administrators. Requests can be handled either on the CA or directly on the RA. This provides great value for organizations that needs to map their own workflows to the approval process.

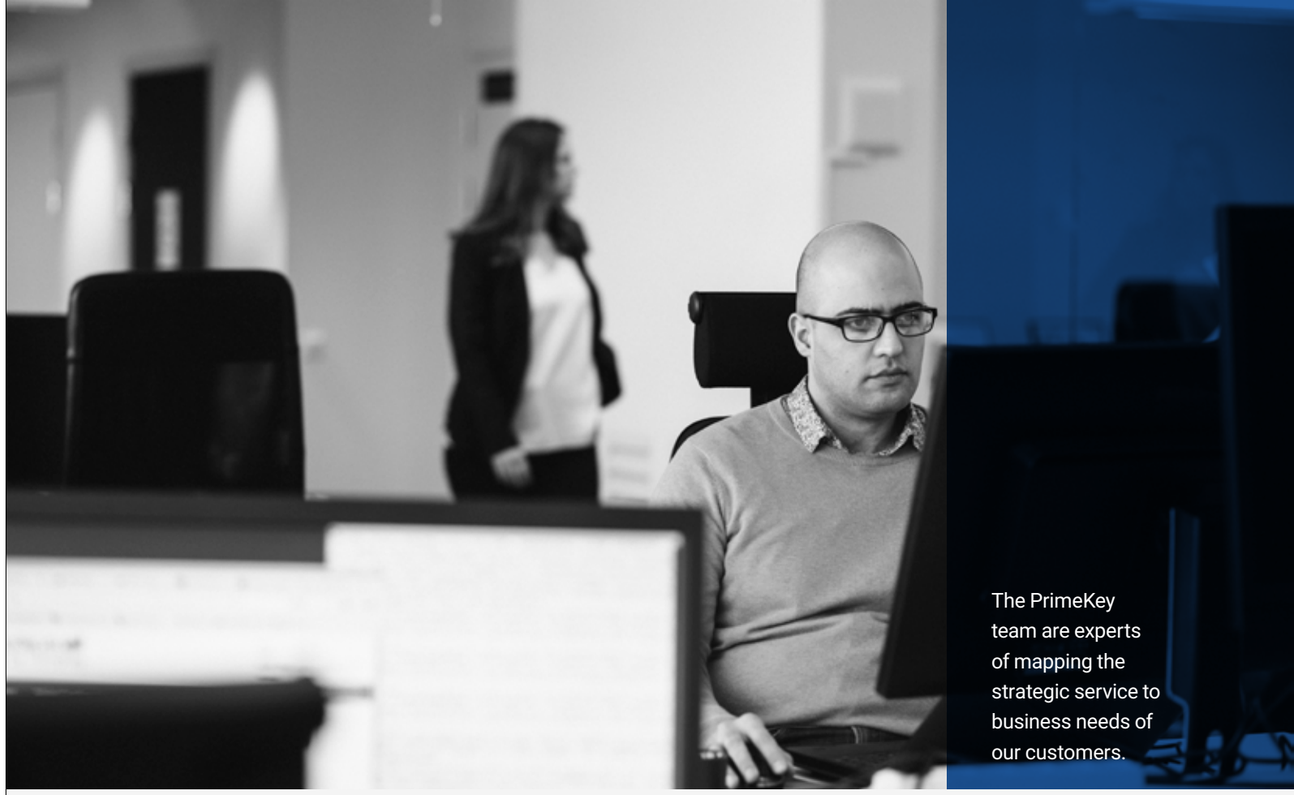
Sophisticated Rights Management
Using the same rights management system as EJBCA, the same RA can service anybody from a public, unauthenticated user, to an authenticated customer, to a local administrator. Each sees only the functionality they have access to, allowing multiple roles to perform duties connected to the same system.

Highlights

- Mutually authenticated TLS connection
- JSF 2.0 based Web UI, including Content Security Policy, protection against CSS, CSRF and other attacks
- Secure object transfer between RA and CA
- Location aware authorization
- Profile based approvals process

Clustering the RA

You can have several RA servers, in order to provide high availability, or increased performance. The RA itself is stateless and therefore any user can access any RA server to perform their tasks, as long as it is an RA with the same privileges. User session against the RA UI uses HTTPS sessions, and are typically pinned to a certain node by a load balancer.



The PrimeKey team are experts of mapping the strategic service to business needs of our customers.

Key Features

Ease of administration
- RA is defined by its identity to CA, not by internal or local configuration
- You can stack identical RAs behind a load balancer to
  - ease the load on the CA, and/or
  - increase performance of RA service.
- An instance of EJBCA RA can be silently swapped out with a minimum of manual interaction

User Experience and branding
- User friendly and purposeful interface
- Possibility to customize interface to specific customer needs
- Possibility to customize interface to customer branding

Physical Security
- Typical installation with CA in secure environment and protected by firewall
- CA initiating all communication allows physical security and geographic separation
- Ability to perform delegated key generation and recovery prevents CA access to access private keys generated on an RA

Logical Security
- Secure tunnel between CA and RA using TLS
- Identity verified by certificates
- Built-in authorization layer

User Authorization

CA Administrators
CA Administrators are granted access to all functionality in the RA, but only to the CAs that are selected in the administrator role. CAs and related end entities and certificates, will be hidden if the administrator does not have access.

RA Administrators
RA Administrators have access to the Enrollment, Search and Manage Requests pages, depending on the selected End Entity Rules. Access is restricted according to the selected CAs and end entity profiles as well. Authorized RA Administrators can perform limited role management, enabling delegated user management.

Supervisors
Supervisors have access to the Manage Requests and Search pages only, in read-only mode.

Auditors
Auditors have access to everything in read-only mode, except for the Enrollment pages which are not accessible.

REGISTRATION AUTHORITY — PKI BY PRIMEKEY

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.

sales@primekey.com
+46 873 561 01

www.primekey.com

PrimeKey