

EJBCA^{PKI} Training

***Build up your strength!
Be able to lift up heavy
PKI implementations.***



Any serious PKI deployment has to be properly administered and maintained, for which organizations need to have skilled PKI administrators. The best and most cost-efficient way to learn about EJBCA is to attend courses from the folks that have created it and have deployed and maintained numerous installations.

The courses are designed by Henrik Andreasson from WM-data/Logica and Joakim Bågnert from PrimeKey Solutions. Henrik has, among other skills and experiences, worked with diverse PKI implementations over the years, helping customers install, run and maintain large-scale PKI systems. Joakim is product specialist from PrimeKey, where he has participated in many projects involving EJBCA.

The course program is divided into following areas:

- *Installation*
- *Administration*
- *Advanced topics*

Installation

All courses are designed so that the participants learn practical skills, and while EJBCA would run on any operating system that has support for Java and a J2EE application server, for the purpose of the

EJBCA Training courses, Windows XP client system is assumed, and SUSE Linux ES 10 for the CA server.

The installation course goes through all steps needed to have EJBCA installed and running, including installation and setup of MySQL database, JBoss application server, Ant build system, and finally, EJBCA itself.

In the end, each trainee has a setup with an operational PKI, an Apache server with own generated certificates, and a client system that can access the EJBCA web interface.

Administration

The Administration course continues from where Installation course ends (A VMware image is provided for those who wish to skip the Installation course.)

In the beginning of the course, one has a walk trough of the EJBCA interfaces (public web, admin web and command line interface). The next two topics deal with steps for creating CAs for authentication certificates and for SSL certificates. After this comes management of End-Entities (search, revoke, renew) and CRLs (issuance, scheduling).

The course rounds off by a session where one learns how to separate different administrative roles and

how to create groups for CA administrators, RA administrators, Supervisors, and Super Administrator.

Advanced Topics

This course assumes knowledge from the Installation and Administration courses. Attendees have a smorgasbord of topics that provide comprehensive coverage of real life situations, and it usually takes two days to go through them all.

Adjusting EJBCA with property files

- EJBCA, database, web, mail, cmp, ocspl, protection and xkms property files

Smart cards issuance

- CA tokens on a smart card based HSMs.

Key Recovery

- Configuration of the system and profiles as to enable key recovery. A scenario with lost card is simulated, with steps for recovering keys, and comparing the recovered token with the original one.

EJBCA command line interface (CLI)

- batch command
- ca command with options: info | init | listcas | getrootcert | createcrl | getcrl | listexpired | exportprofiles | importprofiles | importca | importcert | republish | activateca | deactivateca
- other CLI commands: ra, adduser, setpwd, setclearpwd, revokeuser, deluser, unvokeuser, setuserstatus, listnewusers, listusers, finduser, keyrecover, keyrecovernewest, setsubjectdirattr, setup, template, ocspl, asn1dump.

Certificate lifetime from the CLI perspective

Approvals

- Change settings for CA and RA administrative groups as to require Approvals.

Creation and configuration of Publishers

Microsoft smart card logon

- Setup a Microsoft Active Directory compatible certificate and end-entity profiles.

The EJBCA Training courses can be adjusted as to fit best your organization's specific needs. The courses can be held either in Stockholm, at location of the customer's choice, or on-line. For on-line courses the number of attendees is limited to 3 per session.



Our friends Thomas Weber, Michael Herren and Sven Kaegi from Trivadis, Zurich, after a series of hands on sessions. In the lower left smiles Joakim Bågnert, coauthor of EJBCA Training. Opposite of him sits the person responsible for that EJBCA came about, Tomas Gustavsson.

Making EJBCA server more secure
High availability for a PKI installation
Syscheck to monitor EJBCA server

EJBCA Healthcheck

Backing up the EJBCA's database

System documentation

- Certificate policies and CPS
- Profile-, Server-, Physical- and Routine documentation

Log signing

- Configure, verify

External EJBCA Interfaces

- CMS, CMP, SCEP, External RA, XKMS, Web Services

Certificate status control

- Internal OCSP, External OCSP

Services

- CRL Issuer, Certificate Expiration Checker, Custom Service

Troubleshooting

Certificate and End-Entity profiles

- Creating S/MIME CA, Sign CA and VPN CA
- Creating End-Entity certificate profiles for S/MIME, Sign and VPN

NTP

Hard Token Management Framework

- User data sources
- PIN and PUK Management