

EAC ePassport ready PKI solution from PrimeKey

EJBCA is an open source Enterprise PKI implementation delivered by PrimeKey Solutions AB. Among its many interesting aspects, EJBCA delivers a complete set of features covering all requirements of an EAC ePassport PKI and the EU common certificate policy for EAC control infrastructure.

EJBCA

EJBCA is used as the certification authority issuing Country Signing Certificates for signing of ePassport data and EAC Verifying Certificates for reading sensitive data from the passport.

SignServer

SignServer is used to create MRTD signatures on-line, making it ideally suitable for issuance of express passports. This is already implemented and operational with the Swedish National Police Board.

Handle CVCA and DVs

Using EJBCA you can set up the infrastructure CAs for EAC. This includes the root CVCA as well as your domestic DVs. You can sign other member states DVs and get your DVs signed by other member states. Naturally, you can also create CVCA link certificates.

Issue IS certificates

You can issue IS certificates to your inspection systems and easily integrate your IS systems with the PKI. Using WebService you can manage the whole life-cycle of IS certificates.

Flexible integration APIs

Using the industry standard, multi-platform web services, EJBCA offers a web service API for issuing IS and foreign DV certificates in an efficient and easy to integrate process.

There are available other options for integration, such as using a Java EJB interface or even creating your own API.

Production ready and tested for interoperability

EJBCA was present at the "ePassports EAC Conformity & Interoperability Tests", in Prague, September 7th - 12th 2008. EJBCA passed all tests - both member states passport issuance and reading of biometric data from other member states passports on the inspection system.

The EJBCA EAC PKI is already in production in Sweden and is selected by other countries where EAC PKI projects have started.

Open Source – open infrastructure

Both EJBCA and SignServer are fully supported open source products, giving you the best of worlds. Using open source you can easily integrate with, and extend, the infrastructure to meet your specific needs. Being fully supported you can be assured that help is available when you need it.

Features related to ePassport

The features are modelled to support the EAC specification and the EU common certificate policy for EAC control infrastructure.

- Supports CVC certificates according to the EAC 1.11 specification.
- Setting up CVCA's.
- Setting up Document Verifiers (DVs).
- Issuing certificates for Inspection Systems (ISs).
- Supports RSA algorithms specified in the EAC specification.
- Supports ECC algorithms specified in the EAC specification.
- Automatic handling of Sequences for identifying the public key of CVC CAs and DVs.
- Automatic handling of EAC roles (CVCA, DV-D, DV-F, IS) when issuing certificates with different certificate profiles and with different country codes.
- DVs signed by own CVCA, or by creating requests to be signed by foreign CVCA's.
- Sign requests from your DVs with your CVCA to send to other member states.
- Sign foreign DVs with your own CVCA.
- Automatic renewal of domestic DVs in EJBCA, generating new keys when DVs are renewed.
- Add ISs as users and issue IS certificates.
- Create CVCA link certificates to change CVCA or roll over keys.
- Web service API for integration and automatic processing of IS, and foreign DV,certificate requests.
- Command line client to test, display, and verify CVC certificates and requests.
- Import and export functionality of CVCA's and DVs when using soft keystores for easy testing and integration with passport manufacturers.
- Support for various HSMs via PKCS#11.

EJBCA and SignServer are cost-effective, flexible and work on all major platforms. They are installed in various production environments with different directories, databases and HSMs, including ePassport installations in EU countries. By choosing EJBCA and SignServer for your ePassport solution you can save time and resources.

For more information please contact:
Lars Bågnert
Manager, Technical Sales
+46 (0) 702 11 08 00
lars.bagnert@primekey.se

Visit us at:
www.primekey.se
and
www.ejbca.org
www.signserver.org