

Primus HSM JCE API Training

Setup & Usage of JCE API

Description

The course is a “hands-on” workshop and covers the basics of using Securosys Java Cryptographic Extension (JCE) API to connect to the Primus HSM or CloudsHSM and perform cryptographic operations with it.

Since JCE is a quite well-established standard, the course focuses more on the specifics of using Securosys’ unique features like multi-authorization, key attestation, and others.

Contents

- What is JCE “Core”
- Why/how is it extended by Securosys
- Tutorial walkthrough
 - Connecting to Primus HSM
 - Connecting to CloudsHSM
 - Basic cryptographic operations
 - Cryptocurrency functions
 - Multi-authorization with Smart Key Attributes
 - Key Attestation

Details

Audience: Application engineers, HSM integrators / consultants

Prerequisites: Experience in Java / Basic knowledge of HSM application / Completion of Technical Sales Partner Training course recommended

Duration: 2 hours

Language: English

Audience: Technical Pre-Sales, Field Application Engineers

Participants: Up to 6 (on-site/online)

Location: Classroom (Securosys SA in Zürich, Switzerland) or Webinar (teacher-based, see remote training preparations below)

Remote Training Preparations

Due to the high practical focus of the training, it is necessary that the participants have access to a Primus HSM partition in the cloud or on-premise with enabled JCE API.

Please make sure that you have the following infrastructure, setup, documentation and software ready **before the training starts**:

- One (1) configured user partitions on Primus HSM (cluster) on-premises or CloudsHSM. For training purposes Securosys may provide temporary access to Training/Developer HSMs, reachable over the Internet
 - JCE API license installed
 - JCE API enabled on the partition
- HSM connection details and credentials: DNS/IP, Port, User names, and valid Setup Passwords (Note: Setup Password has limited lifetime!)
- Laptop with Installed Java development environment (e.g., IntelliJ IDEA Community Edition), text editor
 - Zoom Client App installed for web-conference (presentations, remote control) <https://zoom.us/download?os=linux>
 - Headset or audio input-/output-device
- Stable Network/Internet connection (2Mbps+) and access:
 - for Zoom conference
 - to Securosys Support Portal, <https://support.securusys.ch> (User Guide, Application Notes and Provider software)
 - to Linux repositories to install additional packages (p11-kit, OpenSC, p11-tools)
 - to your HSMs, CloudsHSM or Securosys remote Training/Developer HSMs
- Download from Securosys Support Portal latest versions of:
 - JCE API User Guide and Examples: primus.doc.zip, primus.samples.zip
 - JCE Provider Software: primusX.jar

Approx. 3 days before the training Securosys will provide the Zoom web-conference link (and connection details to remote Training HSMs).

Please verify that your infrastructure is working properly before the training.