Primus HSM PKCS#11 Provider Training

Setup & Usage of PKCS#11 Provider

Description

The course is a "hands-on" workshop and covers the basics of installing, configuring and integrating the Securosys PKCS#11 Provider to connect to the Primus HSM or CloudsHSM Service and perform cryptographic operations.

Contents

- Introduction, architecture overview
  - PKCS#11 standard (slot/token, credentials), HSM partitions/cluster), documentation
- Initial provider installation on Linux
- Basic provider configuration and connectivity test
  - Adapt configuration files
  - HSM connectivity, fetching permanent secret (ppin tool)
  - Basic test tools (ppin, testPrimus, pkcs11-tool), logs and error analysis
- Advanced provider topics
  - Multiple HSMs and partitions
  - HSM clusters, CloudsHSM, load balancing, performance optimization
  - Provider update
- Intro application landscape (based on p11-kit)

Details

Audience:	Application engineers, HSM integrators, Consultants, Technical Pre-Sales
Prerequisites:	Linux knowledge (installation, access rights, OpenSSL, etc.), Basic knowledge of PKCS#11 Standard Conceptual knowledge of Primus HSM (Operator training recommended)
Duration:	2 hours
Language:	English, German (documents and online content in English)
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 Primus HSM partitions in the cloud (or on-premise) with enabled PKCS#11 API.

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

- For training purposes Securosys provides temporary access to Training/Developer HSMs, reachable over the Internet or
  Two (2) configured user partitions on Primus HSM (cluster) on-premises or CloudsHSM.
  - PKCS#11 license installed, and PKCS#11 API enabled on these partitions
  - Key Invalidation disabled on these partitions
- HSM connection details and credentials: DNS/IP, Port, User names, and valid Setup Passwords (Note: Setup Password has limited lifetime!)
- Laptop/PC with Linux and graphical desktop installed, root access (or within VM) (CentOS/RHEL 8, Ubuntu 20, Debian 10)
  - Zoom Client App installed for web-conference (presentations, remote control) https://zoom.us/download or https://zoom.us/download?os=linux (or use separate Windows PC for Zoom conference)
  - Headset or audio input-/output-device for Zoom conference
- Stable Network/Internet connection (2Mbps+) and access:
  - for Zoom conference
  - to Securosys Support Portal, https://support.securosys.com (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:
  - PKCS#11 User Guide: PrimusAPI_PKCS11-UserGuide_UG-Enn.pdf
  - PKCS#11 Provider Software: PrimusAPI_PKCS11-v1.x.x.zip
  - Application Note "Primus PKCS#11 Integration into P11-Kit": PrimusHSM_P11-Kit-Tool_AN-Enn.pdf

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.