Kiuru SAM Release 5
Product Fact Sheet

v.1.0

Product Description

Kiuru SAM is a Trustworthy System Supporting Server Signing (TW4S) that offers remote digital signature capability for a Mobile Signature Service Platform. It ensures that the signing keys of a signer user are only used under the sole control of the signer for the intended purpose. Kiuru SAM provides a remote service to the signer from which he can obtain digital signatures.

The functionality and security features of the Kiuru SAM are centered around protecting this operation, the signer, and the keys used for the signature generation.

Environment

Kiuru SAM locates in a dedicated tamper protected environment (figure 1).

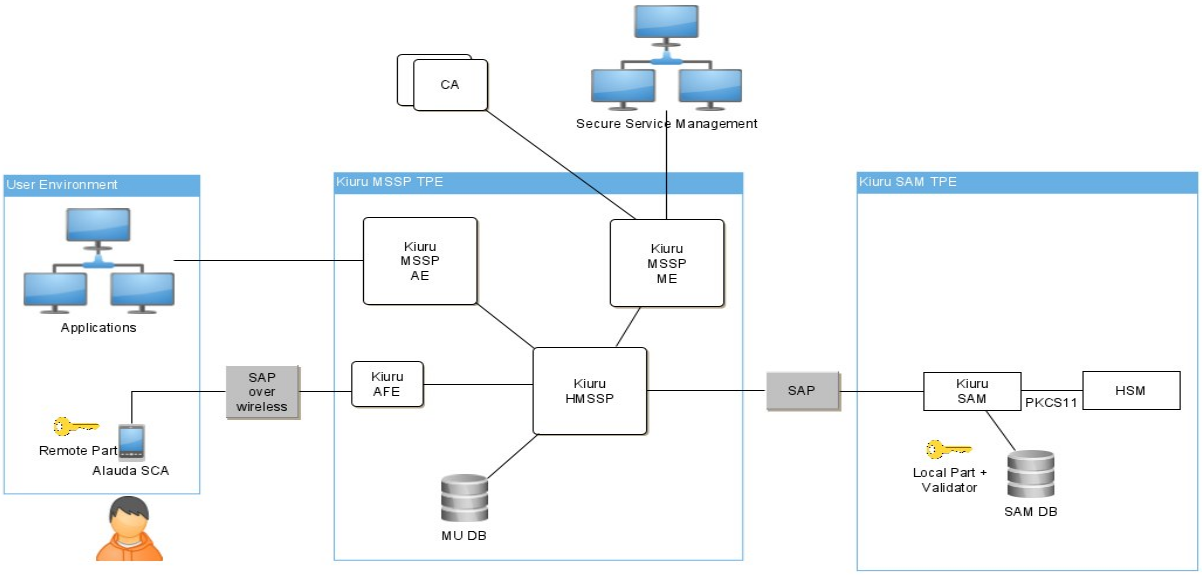

Figure 1: Kiuru SAM Environment

Components

Kiuru SAM consists of the following main software components:

- Signature Activation Protocol (SAP)
  - Protocol interface with the MSSP server.
  - B17 protocol – key splitting protocol for signer sole control of the signing key.
- SAM services
  - SRP6 validator – Secure remote binding of signer with the signature creation data.
- SAM DB
  - Database for the SAM service
- SAM HSM
  - Unified HSM service interface (PKCS#11 or equivalent) for generating signing keys and to create digital signatures.

Security

Kiuru SAM exists in a dedicated tamper protected environment. All communications are via a secure trusted channel.

Kiuru SAM provides a transport encryption mechanism for securing all traffic between the SAM and the signature creation application (SCA).

Supported Signature Creation Applications

Kiuru SAM supports signature creation using the following SCA using the signature data provided by Kiuru SAM communication protocol (Signature Activation Protocol SAP):

- Alauda PBY App for smartphone
- Alauda B17 Fortress Applet for SIM card

Packaging

Kiuru SAM is delivered as a digitally signed RPM installation package for a SELinux server platform.

Standards

Kiuru SAM provides a remote Qualified Electronic Signatures and Seals (referred to collectively as QES) according to:

- Remote QES according to eIDAS Regulation No 910/2014; and
- Sole Control Assurance Level2 (SCAL2) according to sec. 5.4 of EN 419241-1.

About Methics

Methics Oy provides open standard based, innovative and secure software products for Mobile ID and Mobile Connect Services. Our products, offered under the Kiuru and Alauda trademarks provide the most complete and flexible mobile signature service solution for authentication and digital signatures. Kiuru MSSP is a high performance and modular mobile signature service platform and Alauda is a highly secure PKI client available as a SIM card applet and a Smartphone client app.