Kiuru SAM Release 6

Product Fact Sheet v.1.1

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.

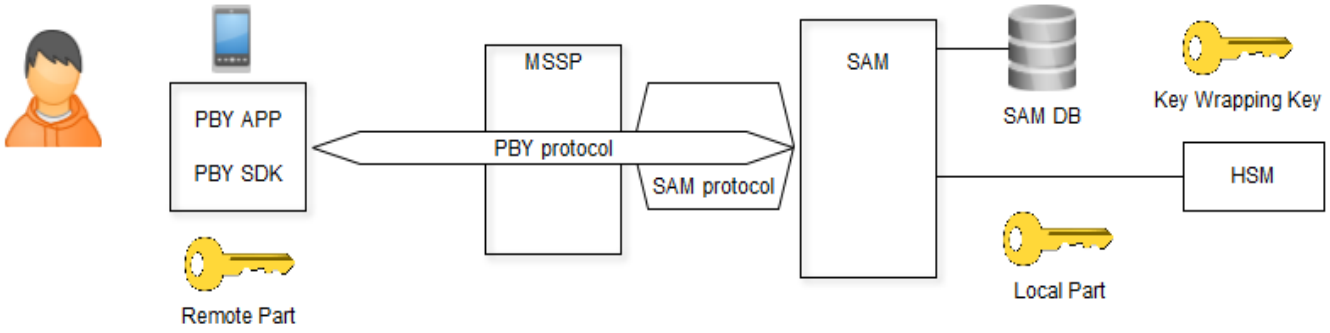

Figure 1: Kiuru SAM architecture.

Components

Kiuru SAM consists of the following main components:

Signature Activation Module Protocols

- SAP - PBY protocol for App connection
  - B17 protocol – key splitting protocol for signer sole control of the signing key.
  - SRP6 protocol – Secure remote binding of signer with the signature activation data.
- SAM protocol for service orchestration

SAM services

- Signature activation, audit logging, key management, clustering

SAM DB

- Database for the SAM service. Database connection and content is encrypted.

HSM Interface

- Unified HSM service interface (PKCS#11 or equivalent) for generating signing keys and create digital signatures.

Certification

The product is certified in accordance with certification scheme requirements defined by standard en 419241-2:2019 and ISO 15408. Date of the certification is 2021-07-13.

Security

Kiuru SAM runs in a dedicated tamper protected bare-metal SE Linux server. All communications are via a secure trusted channel. Kiuru SAM provides a end-to-end 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 Linux 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 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.