Methics Product Compatibility Fact Sheet v1.0

About Methics

Methics Oy provides open standard based, innovative and secure software products for Identity Solutions. Our offerings cover Mobile ID, eIDAS compliant Local & Remote Signature solutions. Our products, offered under the Kiuru and Alauda trademarks provide the most complete and flexible mobile signature service solution for authentication and digital signatures

Product details

Kiuru ® - server side products

- Core MSSP servers: HMSSP, AE and ME MSSP
- Signature Activation Module (SAM)
- KDSS: Document Signing server
- Connectivity APIs: SOAP, REST, RADIUs, CSC
- Service Administration: MUTK, AETK, WebManager
- Testing: SIGTK, SimpleCA, wPKI Simulator

Alauda ® - user side products

- Alauda Applet for SIM/eSIM cards: P38, B17, LW, M2
- PBY SDK & Reference App
- OTA server
- AFE server for APP communication over IP

Vendor Compatibility

As a technology vendor Methics products and deployed solutions are reliable and compatible with leading vendors of their respective domains.

UICC Platforms

Alauda applets can be loaded on both SIM and eSIM cards. Methics product compatibility is tested with following UICC vendors:

- IDEMIA
- G+D
- Thales (Gemalto)
- XH Smart Tech

HSMs

Kiuru SAM can work with hardware security module (HSM) of different vendors. Methics product compatibility is tested with following HSM vendors:

- Thales
- Utimaco
- Securosys
- Entrust
- NitroHSM

Servers

Methics solution can be deployed in physical servers or virtual machines, depending on customer needs. Therefore, solution is compatible to run in these environments.

Standards

Methics products are compatible with:

Mobile Signature Services

- ETSI TS 102 203
- ETSI TS 102 204
- ETSI TS 102 206
- ETSI TS 102 207

Digital Signature Services

- Oasis DSS
- Cloud Signature Consortium API specification

Digital Signature Frameworks

- AdES, XAdES, PAdES

Remote Signature Services

- CEN EN 419 241-1/2
- CEN EN 419 211-2

Digital Signature Algorithms

- RSA, RSA-PSS, ECC
- Padding and digest algorithms
- PKCS#1V1.5 and V2.0

Signature Message Formats

- RFC 5652 CMS
- RFC 4210 CMP, RFC 4211 CRMF
- PKCS#7, PKCS#10, PKCS#11
- RFC 5280, RFC 6960 OCSP
- ITU X.509v3
- eIDAS QTSP standards
- GlobalPlatform Messaging Specification
- FiCom recommendations and extensions