

## Kiuru MSSP Release 6

### Product Fact Sheet v1.6

#### Product Description

Kiuru MSSP is a Mobile Signature Service (MSS) platform for orchestrating services and secure Mobile ID. Kiuru MSSP provides mobile signature service functionality for applications and operators to establish open standard based and secure channel between end users and business applications. Kiuru MSSP handles communication between infrastructure parties and connects wirelessly to the end users' mobile devices.

Kiuru MSSP software is based on modern Java technology and system design. Kiuru MSSP provides interfaces and tools for service monitoring, remote logging and billing reporting. Kiuru MSSP server provides high messaging and validation scalability and high availability for signature services.

#### Key Features

##### *Mobile Signature Messaging*

Kiuru MSSP routes MSS signature requests received to end users. End users can sign the requests by using their mobile phones with Alauda PKI and Alauda PBY clients. Kiuru MSSP handles MSS roaming, signature validation and routing back to the signature requestor.

##### *Mobile User Profile Management*

Kiuru MSSP provides a MSS registration request interface (MReg) for provisioning Mobile User, App User and/or SIM card and smartphone information. MReg supports multiple simultaneous registration processes against different CA's for complete User Management.

##### *Support for Multiple PKI Systems*

Kiuru MSSP has a concept of WPKI Profile, which allows you to define WPKI properties for end users or PKI clients. When WPKI Profiles are in use, Kiuru MSSP can support multiple different WPKI systems and versions at the same time.

##### *Integration*

Kiuru MSSP provides multiple open integration points. All MSSP data sources can be external, routing rules can access JDBC, LDAP, HTTP, SAML2 and SPML2 data sources and all external MSSP interfaces are based on open standards.

##### *Reporting and Logging*

Kiuru MSSP reporting tool extracts technical MSS transaction data to business transactions. This provides an integration point to fraud control systems, document management and billing systems. Kiuru MSSP supports system logging (log4j) and audit logging (DB). You can fine tune logging files and content or even use remote

logging host.

##### *Configuration*

Kiuru MSSP has only one configuration file, which can be split into various subsystem configuration files. You just include these new subsystems configurations in MSSP configuration.

MSS and DSS message routing is also configurable. You can build various rules how to make routing decisions. For example you can select different routes for each application provider, define new restrictions for some application providers etc.

##### *Supported PKI Keys*

Kiuru MSSP supports both RSA & ECC for signatures in Local (SIM/eSIM) & Remote (App) signatures. Supported RSA key sizes from 1024 bits to 4096 bits, and ECC key size of 256 and 384 bits (NIST-P256r1 and NIST-P384r1 curve keys). Key properties are defined in a key generation request.

##### *Modular Software and Additional Modules*

Kiuru MSSP has the same flexible module architecture as Servlet engines. You can include new binary modules and use them in your configuration.

##### *Support for Batch Signing*

Kiuru MSSP provides the option to bulk sign documents using Batch Signing feature. Batch signing can be done from Alauda clients e.g Alauda P38 or Alauda PBY.

##### *Clustering and Geographical Redundancy*

Kiuru MSSP supports clustering. You can do active-passive or active-active cluster. The cluster shares common databases and you can run tens of servers in the same cluster. The cluster provides you real performance and high-availability for you service.

Additionally you can run the servers in a geo-redundant configuration. The geo-redundant system has a build-in data replication and system state monitoring and you can run the geo-redundant system in single-node, active-active or active-passive mode.

#### Environment

##### *Operating Environment*

Kiuru MSSP is a Java 8 server application. Supported server platforms are various Linux distributions and SELinux.

##### *Configuration and Databases*

Kiuru MSSP uses a single configuration folder for overall system configuration. Supported databases are PostgreSQL 9 or later and Oracle 11g.

##### *Performance*

Throughput for signature transactions is up to 150 txn/s

on a single x86 platform. Performance can be increased linearly, depends on the CPU and the used message routing scenario.

### Security

Kiuru MSSP supports TLS/SSL connections for all services. SSL certificates and certificate revocation lists can be managed without service breaks.

### Routing

Kiuru MSSP provides flexible rule-based message routing. Routing can be done based on signature message elements or external routing services like number portability.

### Audit Logging and Monitoring

Kiuru MSSP reporting tool provides remote audit logging. Open audit log interface is based on JDBC. System monitoring is based on SNMP. All MSSP interfaces and routing rules can be monitored.

### Standards

#### PKI

Kiuru MSSP includes a component for signature validation as per RFC 5280. Signature validation is done on FIPS 140 certified validation software module. Proof-of-Possession (PKCS#10, CRMF) and validation additional services are supported. Kiuru MSSP PKI features include CA connectivity with LDAP(S) and HTTP(S) for CRL checking, OCSP, Time Stamping and signature and certificate verification.

### ETSI M-COMM & OASIS DSSX Standards

Kiuru MSSP supports all functions of ETSI TS 102 204 and DSSX. Both interfaces are listed in ETSI as the key protocol specifications when implementing eIDAS compliant service. Both synchronous and asynchronous messaging-modes for signature requests are supported.

Kiuru MSSP transaction roaming is fully compatible with ETSI TS 102 207. Kiuru MSSP is fully compliant with the FiCom recommendations and extensions.

### Software

Kiuru MSSP is based on Java 8 software technology and it uses Java Security Manager tools. The platform uses Servlet 3 framework. Platform provides a secure, and user-friendly software platform for QTSPs/TSPs/CAs to implement and deliver managed digital signature services to application providers.

### 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. 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.

