Alauda OTA server v1.2

Product Description

The Alauda OTA server provides a secure and fast wireless communication channel between an MSSP and the Alauda applet on a SIM/eSIM. The Alauda OTA is a built-in server component in the Kiuru MSSP.

The Alauda OTA server encodes Alauda PDUs to the SCP80 (GSM 03.48) command packets and sends concatenated (GSM 03.40) messages to the SIM card over an SMS transport. The server receives messages sent by the applet, it reassembles received messages and sends them to the MSSP or a specified application defined by a service short number.

The Alauda OTA does not implement the Remote File Management or any applet loading functionality.

Wireless communication

The Alauda OTA server is connected to SMSC service by using SMPP communication links. The SMPP client implementation are based on the Twitter's Cloudhopper libraries. That means that the SMPP client implementation has very high performance and its very reliable.

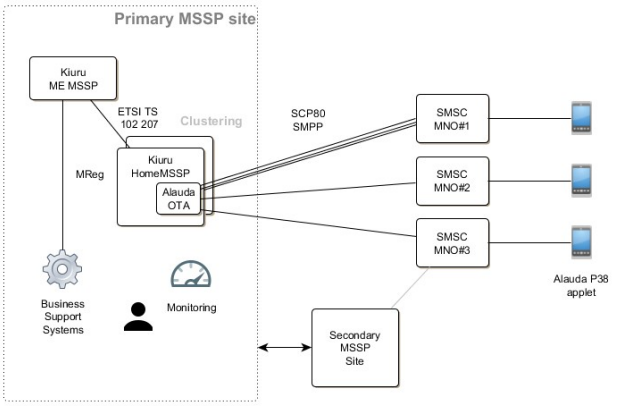
The server supports many simultanous SMSC server connections. The server sends all SMS segments belonging to the same message over the same SMSC link. This is the most interoperable way to reliably communicate with various SIM card platforms.

SCP80 keys and counters are managed in the SIM card database. These keys and counters are secured and can be managed in the same way as any other SIM card data.

Alauda OTA can also be used to receive incoming plain text messages to trigger for example Registration Flow for the given mobile MSISDN.

Multi channel support

The Kiuru MSSP uses the Alauda OTA as any other OTA adapter, and the Kiuru MSSP can support unlimitted number of OTA links. All OTA links can be configured independently, and an Alauda OTA link can hold any number of SMSC connections.



Correct mobile network operator's OTA link is selected by using Kiuru MSSP routing rules. These rules can use WPKI profile-, IMSI- or MSISDN lookup or execute some other mobile network resolver.

Key Features

- Secure communication with an applet on the SIM card
- Supports WPKI profile mechanism for OTA channel configurations. KIC and KID codings are defined in WPKI profile.
- Large number of SPI configurations supported (except the DS mode).
- Separate counters for each KIC key.
- Secure key material and counters input/export for service migration

Standards

Mobile Signature Service

ETSI TS 102 204 V1.1.4 (2003-08)

Over-The-Air

3GPP TS 23.040: "Technical Realization of the Short Message Service (SMS)"
3GPP TS 23.048: "Security mechanisms for the (U)SIM application toolkit"
ETSI TS 102 225: "Secured packet structure for UICC based applications"
ETSI TS 102 226: "Remote APDU Structure for UICC based applications"
3GPP TS 31.115: "Secured packet structure for (U)SIM Toolkit applications"

High-availability support

The Alauda OTA is part of the Kiuru MSSP server and it inherits all Kiuru platform's database connectivity, security, clustering and geo-redundancy functionalities. Additionally Alauda OTA supports SCP80 key and Alauda transport key selection so that there can be two separate key indexes communicating with the same Alauda applet. This feature enables geo-redundant MSSP sites.

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 provides 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/eSIM applet and a Smartphone app.