Alauda P38 Lightning Applet for UICC/eUICC v1.2

Product Description

The Alauda P38 Lightning is a wireless PKI Java Card applet for SIM/UICC/eSIM cards. A WPKI client is needed for Trust Service Providers to implement mobile phone user's PKI service. PKI service is a part of Mobile Signature Services used in secure services like Mobile ID and EUDI Wallet.

The P38 applet has the following key features:

1. Highly interoperable with card platforms.
2. Simple and robust user experience.
3. Secure and fast communication over OTA.
4. Enables all levels of identity assurance. (LoA2-4)
5. Support multiple keys
6. Small and durable applet memory use.
7. Comes with Functional Acceptance Tester

Key Features

Card Platforms

The applet binary versions are available for following target platforms:

- Java Card 2.2.1, 3.0.1, 3.0.4, 3.0.5
- SAT/CAT Toolkit Release 5, Release 6

Methics generates the applet with source code preprocessing to select platform and feature sets which are available for the target platform.

User Experience

A long experience has shown that security interface user experience must be simple, and consistent. There is a well defined set of texts that user sees. These text sets in multiple languages are part of the applet.

Communication Security

The messages to the applet are sent using SCP80 messaging. Responses are similarly encrypted with Alauda Transport Encryption, which keys are created online without the need for special provisioning.

Communication Speed

The lowest latency in communication is possible when a request is delivered in a single message, and a response is a single message. The applet is optimized for minimum number of message segments (usually 1.)

All Levels of Assurance

All levels of identity assurance are supported with the applet. The LoA4 requires use of PKI keys protected with PIN, and lower levels can use PKI solution as well. For the lowest level, the "Click-OK" interaction without PIN query is also supported.

Technical Features

- Up to 4 PKI keys
    - On-board key generation
    - RSA 1024 to 2048 bits
    - ECC keys on NIST-P256r1 etc curves
- Up to 4 PINs with online definable PIN names
- Preloaded UI text sets in up to 7 languages
- SIM Menu for settings and changing PINs.
- Average applet size is 16 kB + texts (1 kB)
- On UICC card reserves 840 bytes of card RAM. On REL5 SIM card reserves 1100 bytes of RAM.
- Support for PUK code, batch signing and click-ok

Functional Acceptance Tester

When a new SIM card platform is considered, the applet interoperability at the new card platform can be easily verified with the Functional Acceptance Tester tool.

The tool is a workstation Java software. Install the applet on the SIM card, plug the card on ISO-7816 card reader, and run the tool. The tool reports the interoperability status, or gives details of possible functional errors.

eSIM Profile

Alauda P38 product package comes with per-generated applet eSIM profile with SSD definition. You can easily load the profile to your eSIM management platform, fine tune it and test compliance with your eSIM services.

Standards

Mobile Signature Service

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

UICC Card Standards

These are used minimum levels of each API:
ETSI TS 102223 V5.0.0 Card Application Toolkit
ETSI TS 102225 V9.0.0 SCP80
ETSI TS 102241 V9.1.0 UICC API for JavaCard
ETSI TS 123038 V9.1.1 Alphabets and Languages
ETSI TS 123040 V9.3.0 Short Message Service
ETSI TS 131130 V6.1.0 USIM API (For Release 6)
ETSI TS 143019 V5.6.0 sim.toolkit API (For Release 5)

Other Standards

Java Card 2.2.1, 2.2.2, 3.0.1, 3.0.4, 3.0.5
GlobalPlatform Card Specification
PKCS#1 v1.5, v2.0, v2.2
IEEE 1363, ANSI X9.62
NIST FIPS-140-2, RFC 5652
GSMA; RSP Technical Specification, V2.3

About Methics

Methics Oy provides open standard based, innovative and secure software products for Mobile ID and Mobile Connect Services. Kiuru MSSP is high performance and modular authentication server and Alauda is feature rich and small footprint SIM card applet for secure WPKI.