Alauda B17 Fortress Applet v1.4

Product Description

The Alauda B17 Fortress is a remote signing applet for standard SIM/UICC cards. Remote signing capability means reduced costs of SIM cards, because SIM cards do not need cryptography accelerators. Additionally all modern cryptography algorithms are available and selected algorithms do not affect wireless communication speed at all. The remote signing technology provides you both cost-efficient Mobile ID service for low risk applications and high assurance with a integrated hardware security module HSM.

Alauda B17 uses a secret sharing mechanism for private key protection. This B17 method splits and distributes the private key between the MSSP and the applet. Therefore, Alauda B17 private keys can be securely managed and both the Signature Activation Module (SAM) and the SIM card must be present when a signature is created. In this way, the applet complies with the high security requirements for electronic signatures of the European Union.

The applet has the following key features:

1. Highly interoperable with card platforms.
   No PKI capabilities are needed.
2. Simple and robust user experience.
   The same as with the Alauda P38 PKI applet.
3. Secure and fast communication with the MSSP.
4. Enables all levels of identity assurance. (LoA2-4)
5. Very small and durable applet memory use.
6. 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 package for selected platforms and feature sets.

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.)

Levels of Assurance

All levels of identity assurance are supported with the applet. The LoA4 requires use of PKI keys protected with PIN and HSM, 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 8 PKI keys
  - Server-side key generation
  - All standard RSA and ECC algorithms
- Up to 8 PINs with online determinable PIN names
- Preloaded UI text sets in up to 7 languages
- SIM Menu for altering applet settings
  (e.g. playtone, changing existing PINs).
- Average applet size is 10 kB + texts (1 kB)
- On UICC card reserves 440 bytes of card RAM.
  On REL5 SIM card reserves 700 bytes of RAM.

Functional Acceptance Tester

When a new SIM card platform is considered, the applet interoperability with the new card platform can be easily verified with the Functional Acceptance Tester tool. The tool is a workstation 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 on functionality errors.

Standards

ETSI TS 102 204 V1.1.4 (2003-08)
CEN EN 419241-2:2019

ETSI TS 102223 V9.0.0 Card Application Toolkit
ETSI TS 102225 V6.2.0 SCP80
ETSI TS 102241 V9.1.0 UICC API for JavaCard
ETSI TS 123038 V9.1.1 Alphabets and Languages
ETSI TS 123040 V13.1.0 Short Message Service
ETSI TS 131130 V6.1.0 USIM API
ETSI TS 143019 V5.6.0 sim.toolkit API

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

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.