Alauda PBY App v1.3

Product Description

The Alauda PBY app is a secure signature creation application for smartphones. The Alauda app is used to implement mobile subscriber's mobile PKI service. Mobile PKI service is a part of Mobile Signature Services [MSS] technology used in Mobile ID services.

Key features are:

- Secure electronic authentication
- Secure signature creation device
- Multi-factor authentication up to 3FA
- Offer highest industry assurance level up to LoA4
- Remote signing, HSM Support
- Support for Batch signing
- Out-of-band transaction approval
- EU eIDAS Regulation and PSD2 Directive

Benefits

Straightforward activation

Activating Mobile ID is as easy as downloading an app, starting registration and scanning a QR code. Thereafter, the user can start using their Mobile ID authentication app.

Secure identity

The Alauda PBY use PKI technology that requires a fingerprint or PIN to use the keys. Additionally, no PIN values are stored. Private keys are protected with HSM and with a key splitting mechanism.

Standard integration

Integration is performed using open standards. Authentication and remote signing can be integrated via REST or SOAP API. Mobile ID API libraries are also available in SDK format for integration in your app.

Multi-authenticator and device support

Alauda PBY operates on various devices (smartphones, tablets, etc.) without the need for additional software or hardware. The user simply receives a push notification on their mobile when they want to authenticate or sign.

Corporate branding

App can be customized for local brand.

App Distribution

Distributor digitally signs the app and distributes it via official distribution channels (Google Play and Apple App store).

User Experience

Alauda PBY app has a similar UX to Alauda SIM card applets. Therefore, its easy to guide users regardless of their mobile ID client.

Communication

Low latency, trustworthy communication and low phone battery consumption are crucial. Therefore, the app uses both notification services and direct communication – whichever provides better service.

Communication Security with End-to-End encryption

The messages to the app are sent using both TLS and Alauda Transport Encryption, providing end-to-end encryption, offering highest communication security. Encryption keys are exchanged dynamically during activation.

All Levels of Assurance

All levels of identity assurance are supported with the app. Multiple Hardware Security Module (HSM) vendors are supported. Both software and HSM based keys can be supported.

Authentication and PKI private key

Alauda PBY uses open cryptography standards and mechanisms, which are free of patent infringement threats.

Key splitting

The PKI key pair is generated at the HSM. The key generation is initiated by a KeyGen operation requested by the Alauda app. After key pair generation, the HSM encrypts the private and HSM exports the encrypted key to the server. The server splits the encrypted key into two parts:

- Local Part is stored in database at the server side,
- Remote Part is sent to the smartphone

When the App receives the KeyGen response, it asks the user to define a PIN.

Key splitting guarantees that both the App and the MSSP must be present when signing.

Zero-knowledge and PIN verification

PIN verification is based on a zero-knowledge proof. The zero-knowledge proof is a method by which the App can prove to server (the verifier, in this case MSSP) that user knows the PIN value, without conveying any information of the actual PIN value.

The protocol Alauda PBY uses is the Secure Remote Password (SRP) protocol. Alauda uses SRP6(b) version.

SRP6 is a secure password-based authentication and key-exchange protocol. It solves the problem of securely authenticating users without exchanging PIN values over the network. This way, even if the entities are compromised, it would not allow the attacker to impersonate the client. In addition, SRP6 exchanges a cryptographically strong secret as a by-product of successful authentication, which enables the two parties to communicate securely.

Technical Features

Alauda PBY App

- Up to 8 PKI keys
  - Remote key generation
  - RSA 1024 to 4096 bits
    - With online option to define public exponent for key generation
    - RSA-PSS and PKCS#1v1.5
  - ECC keys with various curves.
- Up to 8 PINs with online definable PIN names
- Support for fingerprint and FaceID
- Support for PUK code
- Distributed over Google Play or Apple AppStore
- Available also as a SDK and a reference app

AFE server

- RPM packaging
- Monitoring, logging, scalability and high-availability utilities similarly with Kiuru MSSP
- Optional Twilio OTP support
- Google Firebase Notification service

SAM server

- RPM packaging
- Monitoring, logging, scalability and high-availability utilities similarly with Kiuru MSSP
- Verifiable audit trail
- Support for built-in soft-HSM, PKCS#11.
- Compatibility with current HSM vendors: Thales, Utimaco, Securosys.ch, Entrust nCipher, etc.

Alauda PBY SDK (Custom App Versions)

Methics offers customers to build their own app version with local branding and languages. In our delivery package we provide technical development guide allowing to customize PBY SDK. Therefore, the app core libraries and example source codes are available for Methics customers.

Standards and Conventions

Mobile Signature Service

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

Android and iOS

https://developer.android.com/
https://developer.apple.com/

Communication

https://firebase.google.com/
https://developer.apple.com/
Ecma International, "The JSON Data Interchange Format", ECMA-404
RFC 6455 The WebSocket Protocol

Other Standards

PKCS#1 v1.5, v2.0, v2.2 , IEEE 1363, ANSI X9.62
NIST FIPS-140-2, RFC 5652,
ISO/IEC 18004:2015, RFC 5054 (SRP6b)

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 client app.