FIDO® Suite | FIDO® Certified products for mobile biometric authentication

Aware's **FIDO® Suite** is a family of software products for biometric authentication that are certified conformant with the specifications of the FIDO® Alliance and interoperable with other FIDO® certified products.

Aware FIDO® Face Authenticator

Aware FIDO® Face Authenticator allows a user to login to a mobile application of a relying party (such as a banking app) using their face for authentication. It provides robust liveness detection via passive mechanisms and also active interaction with the user, including eye blinking. The captured face never leaves the security boundaries of the authenticator application. Each time the user logs in to the mobile application using FIDO, their face is biometrically verified against the template stored on the device. Once verified, the private key is unlocked from the device and a signature is created on a challenge, which is send to the server. The server verifies the challenge using the stored public key, thus enabling the login process to complete. Aware' FIDO Face Authenticator manifests itself in the form of a simple app that can be deployed on a mobile device. It provides a user interface that enables a user to capture his/her face with liveness detection. The captured face is stored in a template form, and is used for subsequent login to FIDO-enabled servers. The interfaces exposed by Aware's FIDO Face Authenticator are standardized by the FIDO ASM (authenticator-specific module) API. It uses JSON messages to communicate with the FIDO UAF Client residing on the same device.

FEATURES AND FUNCTIONALITY

- Mobile facial recognition, biometric authentication
- Capture and quality assessment of the user's biometric facial image (and PIN)
- Authentication of the user's facial biometrics (and PIN)
- Performs active and passive facial liveness detection
- Maintenance of users' public/private key pairs in a cryptographic keystore for each relying party
- Device camera abstraction
- FIDO® Certified

Aware FIDO® Client

Aware FIDO® Client is the intermediary application that helps to bind FIDO authenticators with the relying party mobile application. A FIDO client can look up all FIDO authenticators on the device, and communicate via JSON messages standardized by the FIDO ASM API. Similarly, a relying party mobile application can look up a FIDO client and communicate with FIDO Client. The messages between a relying party application and FIDO Client are standardized via FIDO UAF Protocol Specification and FIDO UAF Application API specification. FIDO Client can create an UAF Protocol payload, embed it as part of a larger message, and transmit it via the Android intent mechanism to the mobile application layer. The application could embed this message as part of its payload to the relying party server, which then communicates with a FIDO server. FIDO Client serves as the glue that can link any relying party mobile application that requires the FIDO functionality with the different FIDO authenticators on the device, possibly provided by different vendors.

FEATURES AND FUNCTIONALITY

- Communication with a FIDO server using the UAF standard API (JSON objects over HTTP)
- Performs communication with the various authenticators using the UAF authenticator abstraction API
- Is pluggable into a web browser or a mobile application
- FIDO® Certified

Aware FIDO®Server

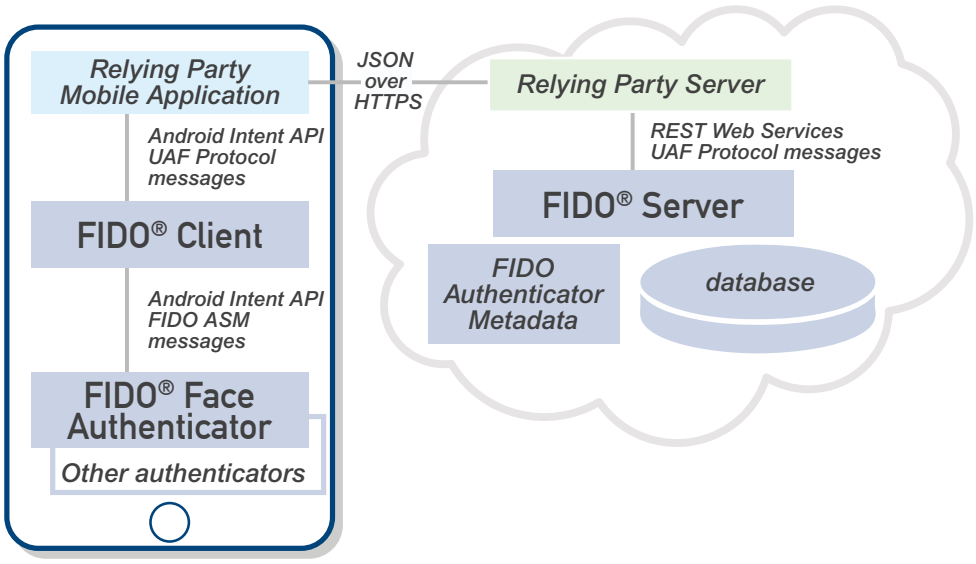
Aware FIDO® Server enables a relying party server to offer FIDO-based login from their mobile applications. FIDO® Server encapsulates the FIDO features required at the server, such as maintenance of the FIDO login policies, management of the public keys, and verification of the signatures created on the mobile device. It exposes REST-style web services that can be consumed by a relying party server to enable FIDO functionality.The messages consumed or generated by the FIDO Server are also governed by the FIDO UAF Protocol Specification. A relying party server and mobile applications act as carriers of the UAF protocol messages.

FEATURES AND FUNCTIONALITY

- Registration service
- Login service
- Deregistration service
- FIDO® Certified

ABOUT FIDO

FIDO specifications aim to define frameworks for authentication online from PCs and mobile devices. There are two sets of FIDO specifications: UAF (Universal Authentication Framework) for password-free authentication, and U2F (Universal 2nd Factor) for second-factor authentication. Aware's FIDO® Suite products are certified compliant with the FIDO specifications for UAF. They include three categories of products: FIDO Server, FIDO Client, and FIDO Authenticators.UAF enables a user to login to a website using biometrics or other means instead of a password. FIDO specifications ensure that private identity information including biometrics is always captured, verified and retained on the user's device and never sent remotely up to a server. FIDO also offers plugability, by modularizing the architectural into various components, each with standardized interfaces that facilitate interoperability. FIDO® is a trademark (registered in numerous countries) of FIDO Alliance, Inc.



HOW IT WORKS – REGISTRATION

FIDO authentication employs a challenge/response mechanism using digital signatures. A user must first access a specific app or website and complete a registration process before using FIDO. The user submits their biometrics and PIN during this registration.For every successful biometric/PIN match during registration, a public key pair is created. The private key is retained on the client in a cryptographic keystore, and the public key is sent to the server, where it is saved in a keystore under the user's ID.

HOW IT WORKS – LOGIN

Upon a login attempt, the FIDO Authentication Server creates a random challenge and sends it to the FIDO Client. The biometrics and PIN are matched locally by the FIDO Authenticator against the biometrics enrolled for that user; they are never transmitted to the server. The user is prompted again to enter his biometrics/PIN. If the match attempt is successful, it unlocks the private key from the FIDO Client keystore. The FIDO Client signs the challenge using the user's private key and sends it to the FIDO Server. The server verifies the signature using the public key received during registration, and the user is permitted to login.

AWARE

781.276.4000 | sales@aware.com | www.aware.com

Aware is a leading global supplier of biometrics software products and solutions since 1993. We provide biometric enrolment SDKs, controls and applications, text and biometric search and match algorithms, and a biometric server platform. Our products are used to build biometric solutions for a variety of applications including law enforcement, border control, access control, credentialing, defense, and intelligence.

©2017 Aware, Inc. All Rights Reserved. This document is for information purposes only and is subject to change without notice. Aware, Inc. assumes no responsibility for the accuracy of the information. AWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. "Aware" is a registered trademark of Aware, Inc.. Other company and brand, product and service names are trademarks, service marks, registered trademarks or registered service marks of their respective holders. DS_FIDO_0117