Acceptto FIDO iOS Toolkit Overview

INDEX

1. Introduction

1.1 Purpose

This document provides a general overview of the Acceptto FIDO Toolkit for iOS. It also describes the most relevant aspects of its implementation.

1.2 Scope

This document covers relevant integration guidelines for the components of the Acceptto FIDO Toolkit for iOS.

2. Fido Protocol Overview

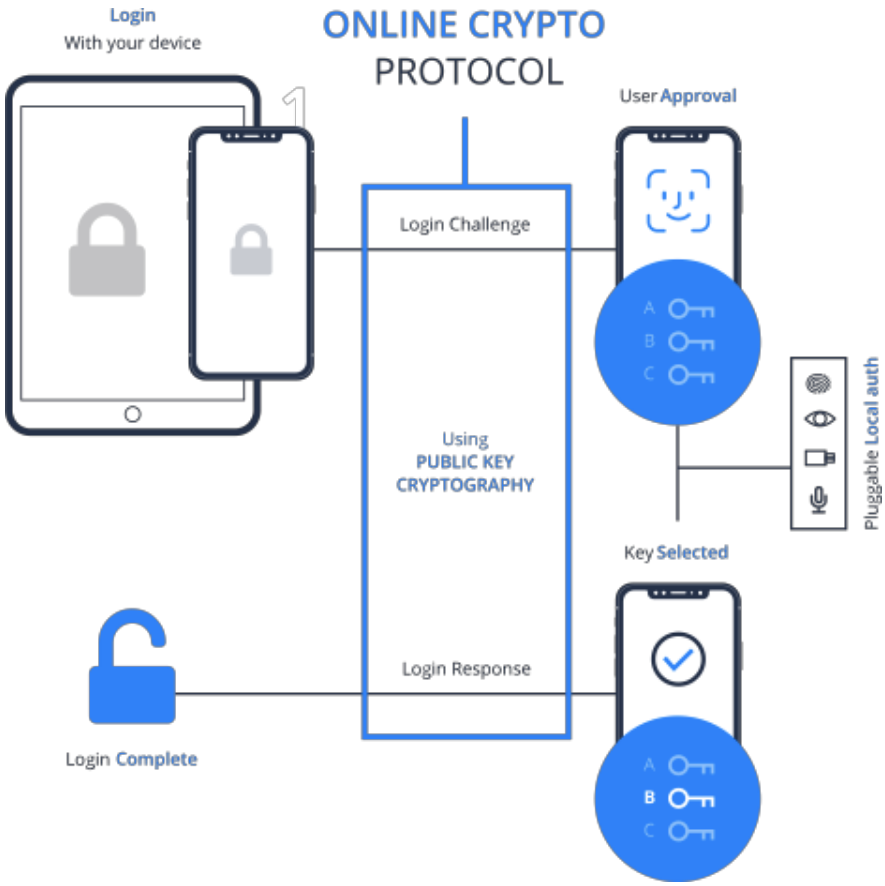
2.1 Functionality

The FIDO protocols use standard public key cryptography techniques to provide stronger authentication. During registration with an online service, the user's client device creates a new key pair. It retains the private key and registers the public key with the online service. Authentication is done by the client device proving possession of the private key to the service by signing a challenge. The client's private keys can be used only after they are unlocked locally on the device by the user. The local unlock is accomplished by a user–friendly and secure action such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second–factor device or pressing a button.

2.2 The Register operation protocol

To perform a register operation, the protocol defines the following steps:

- User is prompted to choose an available FIDO authenticator that matches the online service's acceptance policy.
- User unlocks the FIDO authenticator using a fingerprint reader, a button on a second–factor device, securely–entered PIN or other method.
- User's device creates a new public/private key pair unique for the local device, online service and user's account.
- Public key is sent to the online service and associated with the user's account. The private key and any information about the local authentication method (such as biometric measurements or templates) never leave the local device.



2.3 The Authentication operation protocol

To perform an authentication operation, the protocol defines the following steps:

- Online service challenges the user to login with a previously registered device that matches the service's acceptance policy.
- User unlocks the FIDO authenticator using the same method as at Registration time.
- Device uses the user's account identifier provided by the service to select the correct key and sign the service's challenge.
- Client device sends the signed challenge back to the service, which verifies it with the stored public key and logs in the user.

3. Reasons for implementing FIDO authentication in your business

3.1 Core reasons

The core ideas driving FIDO are (1) ease of use, (2) privacy and security, and (3) standardization. For implementing authentication beyond a password (and perhaps an OTP) , companies have traditionally been faced with an entire stack of proprietary clients and protocols. FIDO changes this by standardizing the client and protocol layers. This ignites a thriving ecosystem of client authentication methods such as biometrics, PINs and second–factors that can be used with a variety of online services in an interoperable manner.

3.2 Benefits

Development and deployment of FIDO Authentication solutions bring myriad benefits to IT vendors, enterprises, service providers and the industry at large, including:

- Stronger account/transaction security
    - This results in lower loss rates and fewer problems to mitigate and will bring the possibility of improved customer loyalty and less churn. Improved authentication will also reduce risk and enable new business models and revenue streams.

- Improved user experience

  - The FIDO solution enables businesses to improve convenience for both customers and employees. As users no longer need to remember complex passwords, user provisioning is therefore simplified and the cost associated with remote password resets will be drastically reduced.

- Improved return of investment in authentication
  - The costs associated with the deployment and support of new solutions will be significantly reduced in comparison to current proprietary approaches which connect a single device type to a single application. System management functionality will be provided by the FIDO infrastructure, rather than having to be built by each application developer.

- Reduced risk of fraud
  - Users of all FIDO-enabled websites and cloud or mobile applications will enjoy a reduced risk of identity fraud, with the convenience of having less reliance upon passwords. Trust in online systems will grow again as a result of consistent user experiences and higher security.

4. iOS Core Libraries overview

4.1 Components

The Acceptto FIDO Toolkit is comprised of three frameworks and a demo app to exemplify all of the main functionalities. With this modular functionality, it's very easy to implement a FIDO authentication on your app. These components are:

4.1.1 Acceptto FIDO Core Framework

- Communicates with the Acceptto FIDO server

- Performs register, authenticate and deregister operations

- Conforms to FIDO protocol

- Automatically manages keyID and login details using the device keychain

4.1.2 Acceptto FIDO Authenticators Framework

- Provides full authenticator functionality for two generic iOS authenticators:

    - PIN authentication
    - Biometric authentication (Touch ID or Face ID)

4.1.3 Acceptto FIDO Manager Framework

- Provides a wizard-like, fully automated interface for enrolling and authenticating in Acceptto FIDO server via iOS

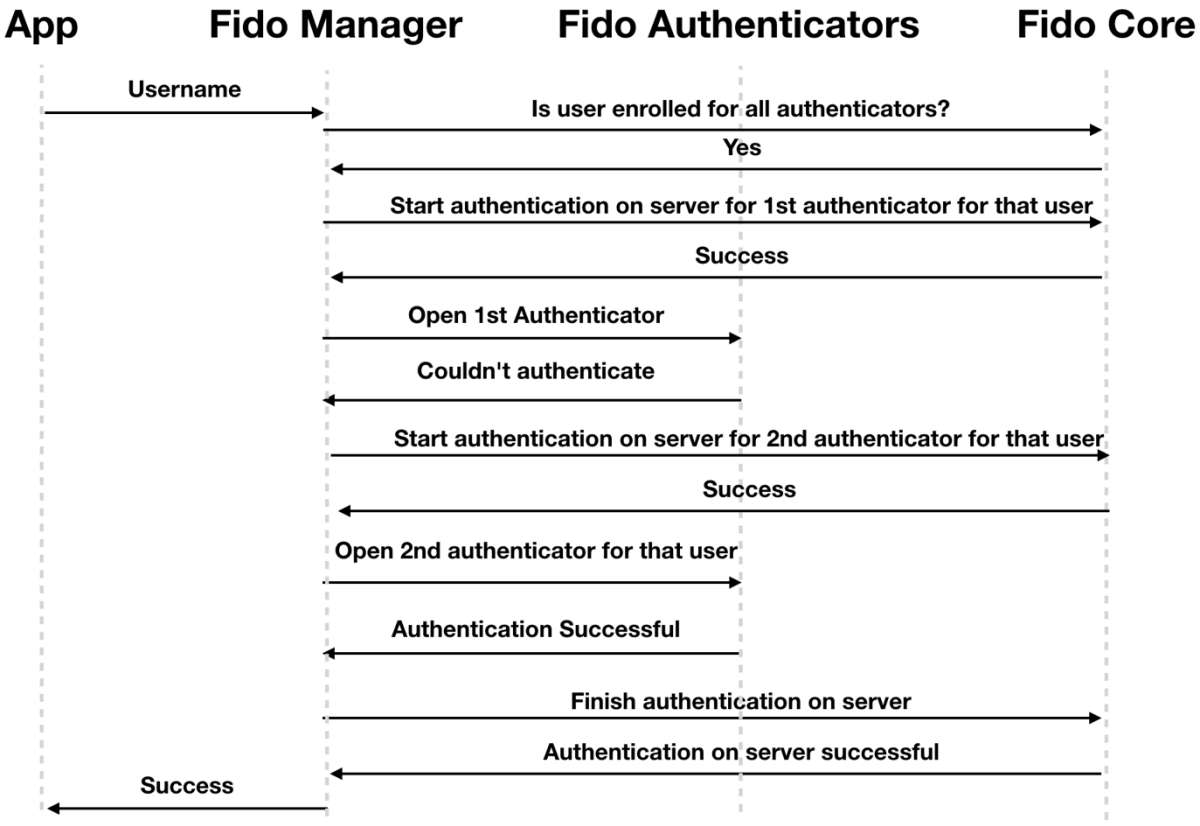
- Manages the authenticators that the user chooses to use, as well as the order in which they should be presented (also fully automated), storing these preferences in the device's app defaults system

4.1.4 Acceptto FIDO Sample App

- Demo app for full functionality of all frameworks above

4.2 Example authentication workflow

This schematic tries to describe an example simple authentication workflow, emphasizing each of the toolkit's components roles in the process. As shown, the libraries will perform all the protocol work for you, and the main app can basically just implement a call to fido manager to have a fully functional FIDO authentication.



4.3 Provided methods and properties

Each of the iOS frameworks provide, among others, methods and properties for the following operations:

- Fido Core Framework
  - Manage the URL of the Fido Server
  - Start a registration process
  - Complete a registration process
  - Start an authentication process
  - Complete an authentication process
  - Manage registered users
  - Perform a deregistration operation
  - Validate user operations

- Fido Authenticators Framework
  - Manage available authenticators
  - Set security preferences for available authenticators
  - Present a biometric authenticator
  - Present a pin authenticator
  - Manage secure pin storage
  - Validate user operations

- Fido Manager Framework
  - Customize the interface colors and text
  - Show a complete FIDO system for registering and authenticating
  - Validate user operations

5. Contact us

For more information you can contact us at info@acceptto.com . You can also visit Acceptto Corporation's Website at http://www.acceptto.com .