

PSL FIDO Solution



Revision History

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **document ID** | **Description** | **Author** | **Reviewed By** | **Approved By & Date** | **Release Date** |
| PSL FIDO Solution V0.1 | Software Components and Use Cases | Amogh Tarcar | Pandurang Kamat | Pandurang Kamat  5/5/2016 |  |
| PSL FIDO Solution V0.2 | Software Components and Use Cases | Amogh Tarcar | Pandurang Kamat |  |  |
| PSL FIDO Solution V0.3 | Software Components and Use Cases | Amogh Tarcar | Pandurang Kamat |  |  |

**Document Distribution**: Persistent Systems Ltd.

**Document Owner**: CTO Org

Contents

# PSL FIDO Solution V 0.3

## Abstract

## Solution Components

## FIDO UAF Protocol

## Updated features

## Use Cases

# PSL FIDO Solution V 0.2

## Abstract

## Solution Components

## FIDO UAF Protocol

## Updated features

## Use Cases

# PSL FIDO Solution V 0.1

## Abstract

## Solution Components

## FIDO UAF Protocol

## Use Cases

PSL FIDO Solution V0.3

# Abstract

This specification describes the PSL Fast Identity Online (FIDO) solution. The solution facilitates creation of FIDO UAF compliant strong cryptographic credentials for relying party mobile applications.

# Solution Components

PSL FIDO Solution comprises of Java based FIDO server and FIDP Mobile application and Relying Party Mobile Application

# FIDO UAF Protocol

PSL FIDO Solution is designed to comply with FIDO Universal Authentication Framework (UAF) Protocol specifications as defined in FIDO UAF Protocol Specification v1.0.

“The goal of the Universal Authentication Framework is to provide a unified and extensible authentication mechanism that supplants passwords while avoiding the shortcomings of current alternative authentication approaches. This approach is designed to allow the relying party to choose the best available authentication mechanism for a particular end user or interaction, while preserving the option to leverage emerging device security capabilities in the future without requiring additional integration effort.”

Source: <https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-protocol-v1.0-ps-20141208.html>

# Updated features

The following features have been improved in V0.3

1. **Relying Party Mobile App Account FIDO Registration And Authentication using PSL FIDO App**

(In V0.2 Relying Party FIDO Registration was supported from RP Website using QR code and Push notification)

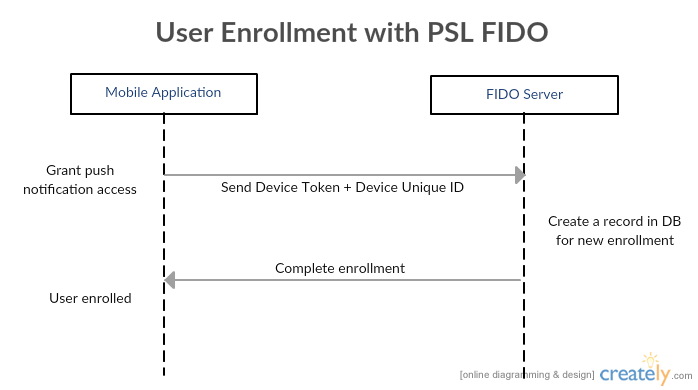
# Use Cases

To start using PSL FIDO solution, the user first installs the iOS mobile application and grants permission to send push notifications to the device. The user then links supported relying party mobile app accounts to PSL Fido iOS application using inter-app communication. As a part of linking process, user generates strong cryptographic credentials which are protected using user specific inputs such as finger print or secure PIN. The user inputs are verified locally. Once linked, user can easily login into relying party mobile app account using PSL FIDO iOS application.

## User Enrollment

In order to enroll with PSL FIDO, user installs the iOS mobile application and provides approval for push notifications.

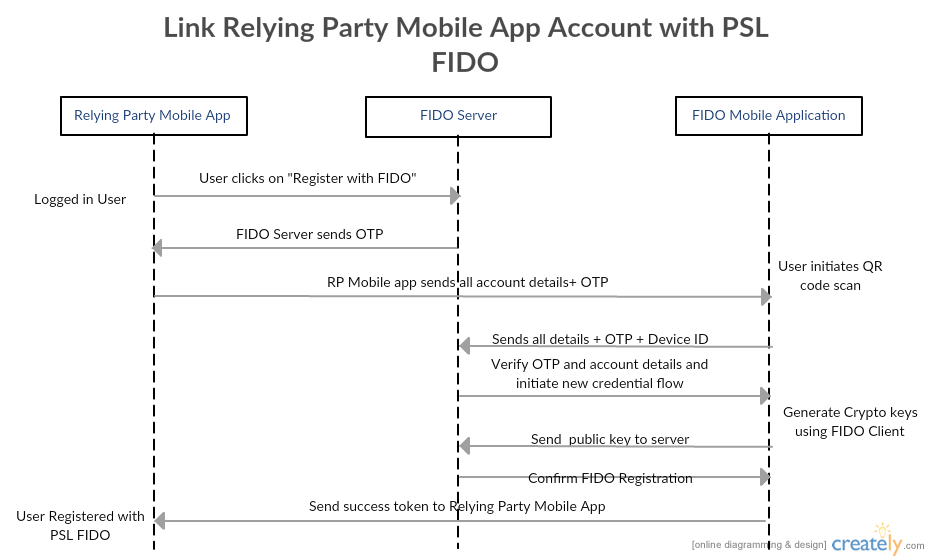
1. On install, the user is greeted with welcome screen and a pop up requesting push notification access
2. User grants push notification access.
3. The application sends device token for push notification and unique id of the application instance to the FIDO server.
4. FIDO server creates a new record for this application instance and completes enrollment.
5. Application displays enrollment completion notification to the user.



## Link Relying Party Mobile App Account

User can link relying party website accounts with PSL Fido in order to use FIDO authenticators as an alternative to password based login. Users can associated accounts with PSL Fido when logged into supported websites.

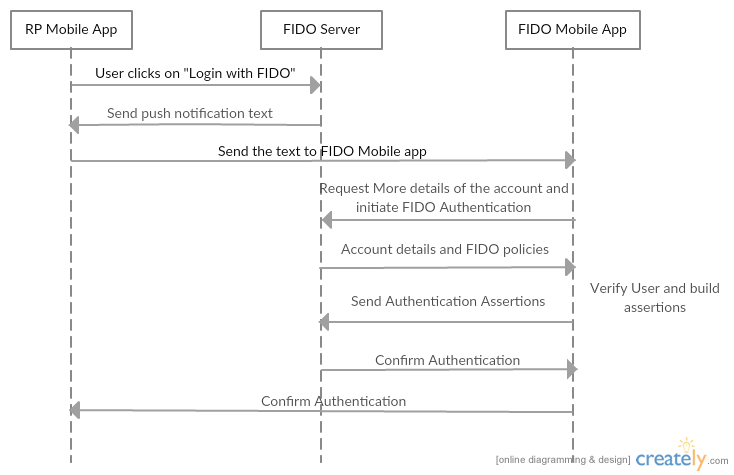
1. For making FIDO credentials for an existing account, the user first clicks on “Register with PSL FIDO” button on the relying party mobile app when logged in.
2. On click, the user is redirected to PSL FIDO Mobile app. Upon launch the app navigates the user through “Make new credentials” flow.
3. The “Make new credentials” flow consists of view account details screen as well as options to choose authenticators supported by FIDO server. User may pick a biometric authenticator such as Apple Touch ID.
4. User picks one authenticator and provides consent to create credentials in accordance with FIDO UAF protocol. The mobile application then creates credentials, maintains its record in its local database and communicates the cryptographic public key to the PSL FIDO server leveraging the UAF protocol.
5. On completing the “Make new credentials” flow PSL FIDO mobile app communicates success to relying party mobile app.
6. User is now back in RP Mobile app and can use PSL FIDO for subsequent login.



## Use PSL FIDO for Login on Relying Party Mobile App

One linked, user can use PSL FIDO for logging into relying party mobile app accounts.

1. For using FIDO credentials for a linked account, the user first clicks on “Login with PSL FIDO” button on the relying party mobile app login screen.
2. On click, the relying party mobile app sends a request to PSL Fido server which sends data to be sent to PSL FIDO mobile app for initiating authentication.
3. The RP mobile app then sends the data to the FIDO mobile app and is navigated to a PSL Mobile app screen in the application which **identifies the authenticator chosen by user and requests consent.**
4. On verification of user consent the mobile application communicates the response via UAF protocol.
5. The server then completes authentication and communicates success to PSL Mobile app.
6. PSL Mobile app sends confirmation to RP Mobile app. On receiving green signal from FIDO mobile app the user is logged in into the relying party mobile app account.



PSL FIDO Solution V0.2

# Abstract

This specification describes the PSL Fast Identity Online (FIDO) solution. The solution facilitates creation of FIDO UAF compliant strong cryptographic credentials for relying party websites.

# Solution Components

PSL FIDO Solution comprises of Java based FIDO server and iOS Mobile application.

# FIDO UAF Protocol

PSL FIDO Solution is designed to comply with FIDO Universal Authentication Framework (UAF) Protocol specifications as defined in FIDO UAF Protocol Specification v1.0.

“The goal of the Universal Authentication Framework is to provide a unified and extensible authentication mechanism that supplants passwords while avoiding the shortcomings of current alternative authentication approaches. This approach is designed to allow the relying party to choose the best available authentication mechanism for a particular end user or interaction, while preserving the option to leverage emerging device security capabilities in the future without requiring additional integration effort.”

Source: <https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-protocol-v1.0-ps-20141208.html>

# Updated features

The following features have been improved in V0.2

1. **User enrollment based on unique app instance ID**

(In V0.1User enrollment was carried on by using phone number as input from user with SMS OTP as verification method.)

1. **Relying Party FIDO Registration using QR code as primary component**

(In V0.1Relying Party FIDO Registration was carried on by sending push notification to the device.)

1. **Fast authentication by focusing on acquiring single input interaction in iOS application**

(In V0.1 authentication was developed with multiple user inputs.)

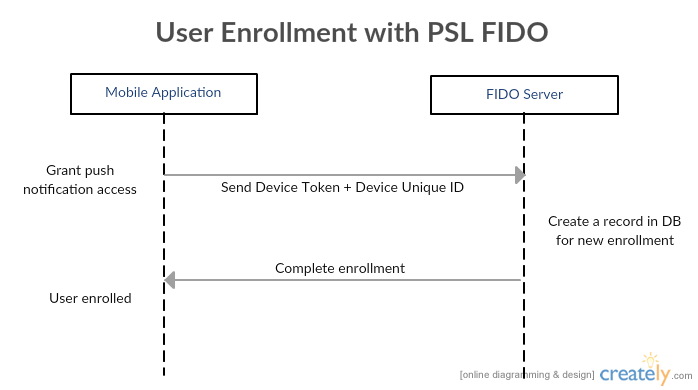
# Use Cases

To start using PSL FIDO solution, the user first installs the iOS mobile application and grants permission to send push notifications to the device. The user then links supported relying party websites to PSL Fido iOS application using QR code. As a part of linking process, user generates strong cryptographic credentials which are protected using user specific inputs such as finger print or secure PIN. The user inputs are verified locally. Once linked, user can easily login into relying party websites using PSL FIDO iOS application.

## User Enrollment

In order to enroll with PSL FIDO, user installs the iOS mobile application and provides approval for push notifications.

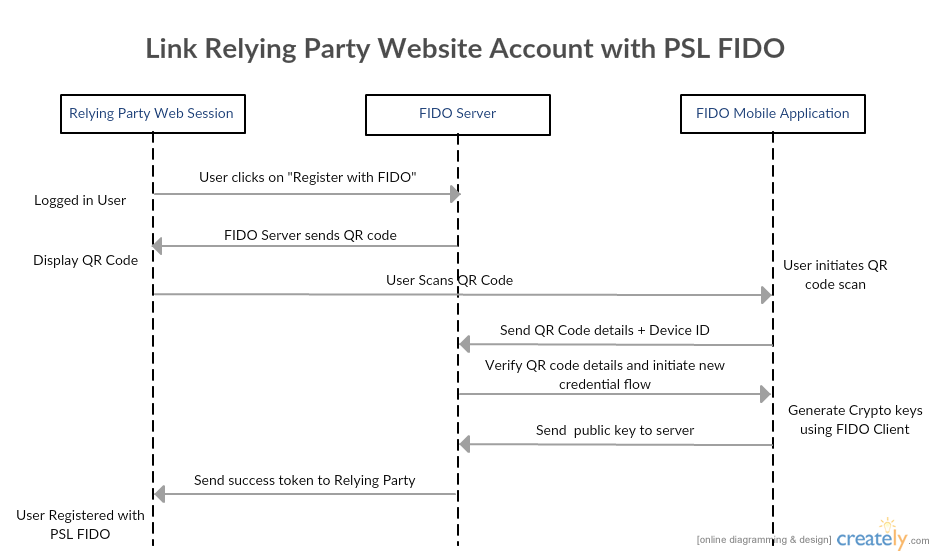
1. On install, the user is greeted with welcome screen and a pop up requesting push notification access
2. User grants push notification access.
3. The application sends device token for push notification and unique id of the application instance to the FIDO server.
4. FIDO server creates a new record for this application instance and completes enrollment.
5. Application displays enrollment completion notification to the user.



## Link Relying Party Website Account

User can link relying party website accounts with PSL Fido in order to use FIDO authenticators as an alternative to password based login. Users can associated accounts with PSL Fido when logged into supported websites.

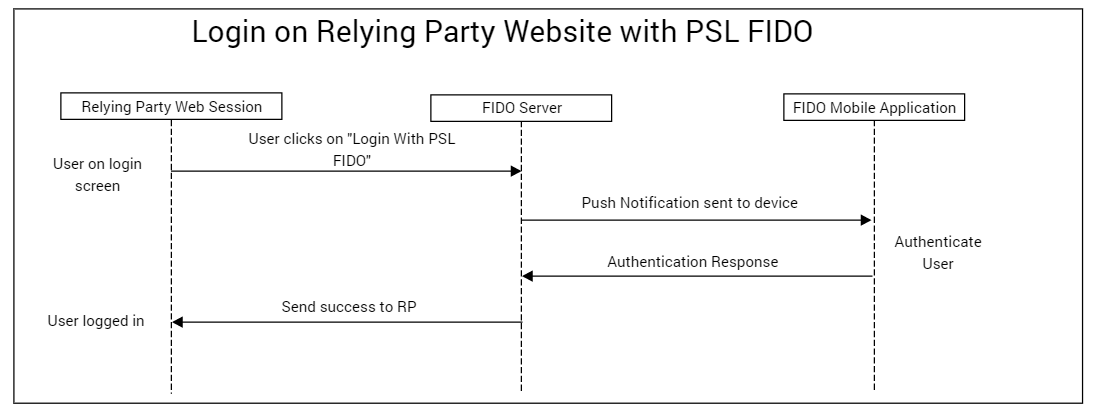
1. For making FIDO credentials for an existing account, the user first clicks on “Register with PSL FIDO” button on the relying party website when logged in.
2. On click, a QR code is displayed to the user on the relying party web site.
3. User opens the phone and taps associate new account, upon which he is navigated to add new account screen which has a button to scan QR code.
4. User than scans the QR code, application adds unique application id to the QR contents and sends request to the PSL FIDO Server. **FIDO server connects the Relying Party account to the enrolled user using unique id and validates the QR code contents**. On successful validation server sends affirmative response to the application which navigates the user through “Make new credentials” flow.
5. The “Make new credentials” flow consists of view account details screen as well as options to choose authenticators supported by FIDO server. User may pick a biometric authenticator such as Apple Touch ID.
6. User picks one authenticator and provides consent to create credentials in accordance with FIDO UAF protocol. The mobile application then creates credentials, maintains its record in its local database and communicates the cryptographic public key to the PSL FIDO server leveraging the UAF protocol.
7. On completing the “Make new credentials” flow PSL FIDO server communicates success to relying party website. User can now use PSL FIDO for subsequent login.



## Use PSL FIDO for Login on Relying Party Website

One linked, user can use PSL FIDO for logging into relying party website accounts.

1. For using FIDO credentials for a linked account, the user first clicks on “Login with PSL FIDO” button on the relying party login screen.
2. On click, the relying party website send a request to PSL Fido server which sends a push notification to registered mobile device for initiating authentication.
3. User then taps the push notification and is navigated to a screen in the application which **identifies the authenticator chosen by user and requests consent.**
4. On verification of user consent the mobile application communicates the response via UAF protocol.
5. The server then completes authentication and communicates success to relying party website.
6. On receiving green signal from FIDO server the user is logged in into the relying party website.



PSL FIDO Solution V0.1

# Abstract

This specification describes the PSL Fast Identity Online (FIDO) solution. The solution facilitates creation of FIDO UAF compliant strong cryptographic credentials for relying party websites.

# Solution Components

PSL FIDO Solution comprises of Java based FIDO server and iOS Mobile application.

# FIDO UAF Protocol

PSL FIDO Solution is designed to comply with FIDO Universal Authentication Framework (UAF) Protocol specifications as defined in FIDO UAF Protocol Specification v1.0.

“The goal of the Universal Authentication Framework is to provide a unified and extensible authentication mechanism that supplants passwords while avoiding the shortcomings of current alternative authentication approaches. This approach is designed to allow the relying party to choose the best available authentication mechanism for a particular end user or interaction, while preserving the option to leverage emerging device security capabilities in the future without requiring additional integration effort.”

Source: <https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-protocol-v1.0-ps-20141208.html>

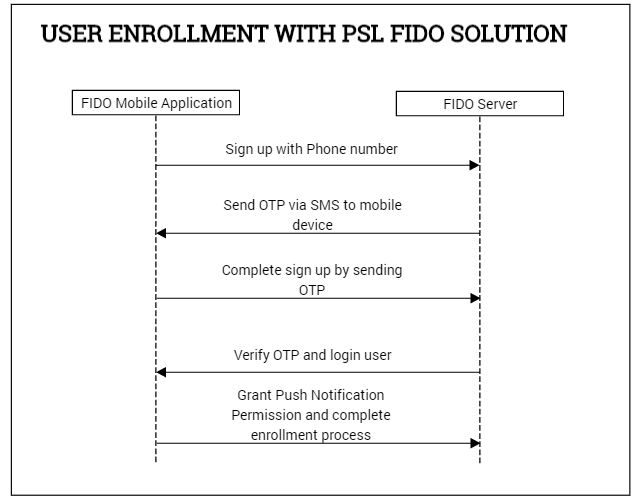
# Use Cases

To start using PSL FIDO solution, the user first installs the iOS mobile application and completes the sign up process. One set up, user can link biometric credentials such as finger print with supported relying party website accounts to his profile. Once linked, user can easily login into relying party websites using strong biometric authentication.

## User Enrollment

In order to begin enrolment with PSL FIDO, user installs the iOS mobile application and is then navigated through the sign up process.

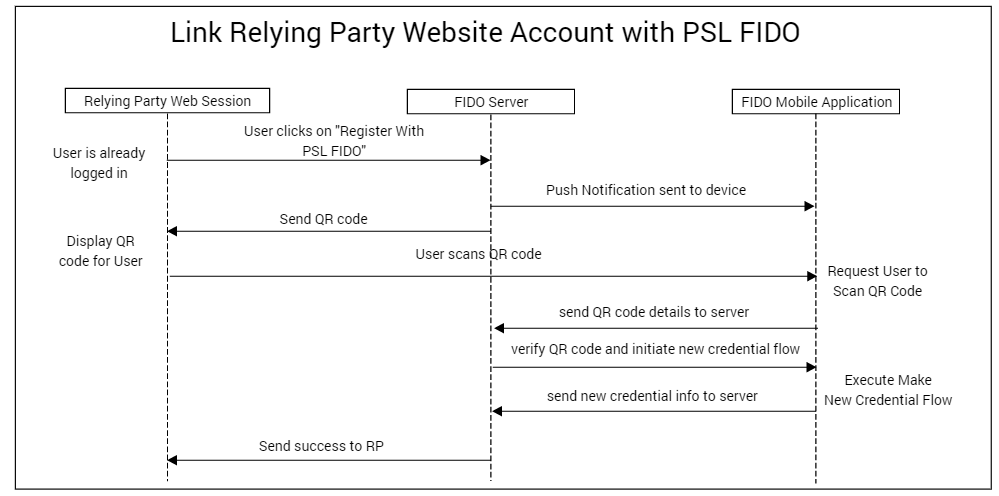
1. On install, the user is greeted with a Sign Up screen which requests the user to provide phone number being used on that device.
2. User then enters mobile phone number and initiates sign up process.
3. Server processes this phone number and sends a One Time Passcode (OTP) to the provided number via SMS service.
4. User completes sign up process by entering the received SMS OTP.
5. Once logged in the user is prompted for permission to receive push notifications from PSL FIDO server.
6. User grants permission which completed the enrolment process.
7. As an outcome of user enrollment process, the FIDO server creates a profile for the user and uniquely identifies his device. The user login state is persisted until he logs out.



## Link Relying Party Website Account

User can link relying party website accounts with PSL Fido in order to use FIDO authenticators as an alternative to password based login. Users can associated accounts with PSL Fido when logged into supported websites.

1. For making FIDO credentials for an existing account, the user first clicks on “Register with PSL FIDO” button on the relying party website when logged in.
2. On click, a QR code is displayed to the user on the screen and a push notification is sent to the registered device.
3. User then taps the push notification and is navigated to a screen in the application which displays information about the website account he is trying to link and a button for QR code scanner.
4. User than scans the QR code, the result is sent to the PSL FIDO Server which navigates the user through “Make new credentials” flow.
5. The “Make new credentials” flow consists of allowing user to pick authenticator and provide consent to create credentials in accordance with FIDO UAF protocol. User may pick a biometric authenticator such as Apple Touch ID.
6. The mobile application then creates credentials, maintains its record in its local database and communicates the cryptographic public key to the PSL FIDO server leveraging the UAF protocol.
7. On completing the “Make new credentials” flow PSL FIDO server communicates success to relying party website. User can now use PSL FIDO for subsequent login.



## Use PSL FIDO for Login on Relying Party Website

One linked, user can use PSL FIDO for logging into relying party website accounts.

1. For using FIDO credentials for a linked account, the user first clicks on “Login with PSL FIDO” button on the relying party login screen.
2. On click, the relying party website send a request to PSL Fido server which sends a push notification to registered mobile device for initiating authentication.
3. User then taps the push notification and is navigated to a screen in the application which displays linked accounts with PSL FIDO.
4. On selecting the account he is navigated through UAF FIDO authentication flow which requests consent using the authenticator associated during linking phase.
5. On verification of user consent the mobile application communicates the response via UAF protocol.
6. The server then completes authentication and communicates success to relying party website.
7. On receiving green signal from FIDO server the user is logged in into the relying party website.

