Requirements for advanced authentication in Fintech and DFS

Showcase of FIGI Security, Infrastructure and Trust working group on Authentication

Vijay Mauree, Programme Coordinator, ITU
&
Arnold Kibuuka, Project Officer, ITU

Financial Inclusion Global Initiative (FIGI)

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Global Goal – UFA 2020

FIGI 3X3X3

Implementation Principles, Recommendations, Guidelines

PAFI Guiding Principles + ITU DFS Focus Group Recommendations + Level One Design Principles

BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

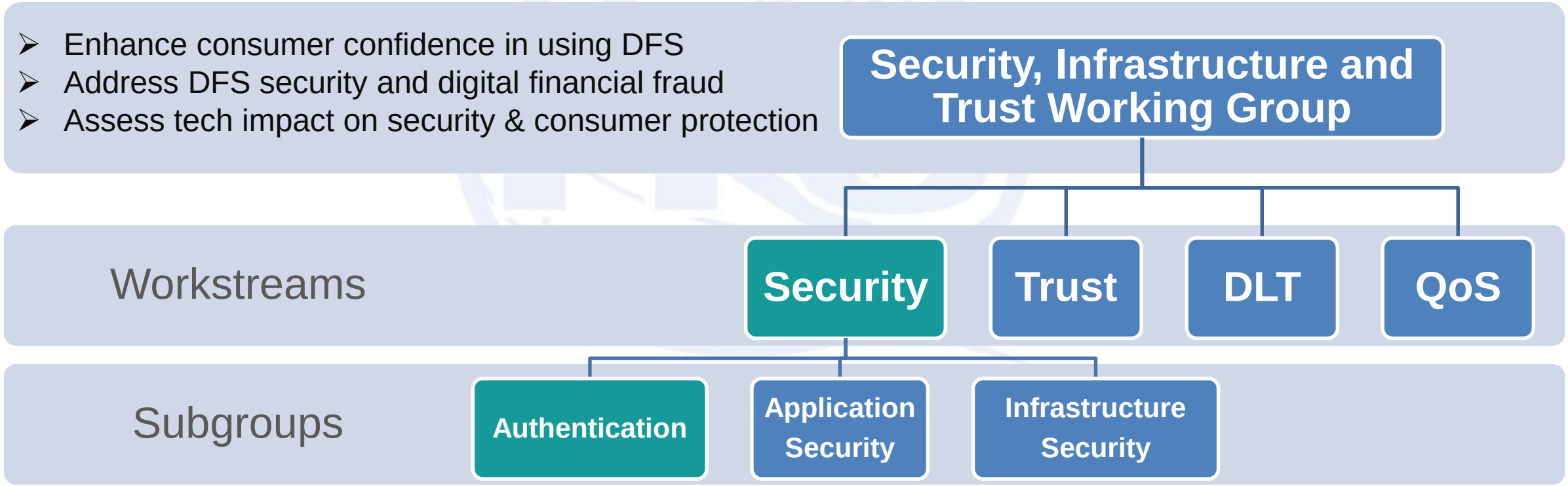
ITU

BILL & MELINDA GATES foundation

International Standards

Background: ITU FIGI SIT Working group

- Enhance consumer confidence in using DFS
- Address DFS security and digital financial fraud
- Assess tech impact on security & consumer protection



Authentication Subgroup

Scope and focus

- Investigate strong authentication technologies for digital financial services (DFS)
- Identify SCA use cases (mobile & national solutions;- Aadhaar in India, IFAA – China etc)
- Report on Secure Authentication Technologies
- Provide strong authentication resources that can be used by developers

Current Issues

- Passwords
- SMS delivered codes are vulnerable
- Threat landscape dynamic
- How to improve user experience and improve security assurance

DFS and Fintech need both

- Strong authentication
- Advanced authentication systems

Objectives Strong Consumer Authentication (SCA)

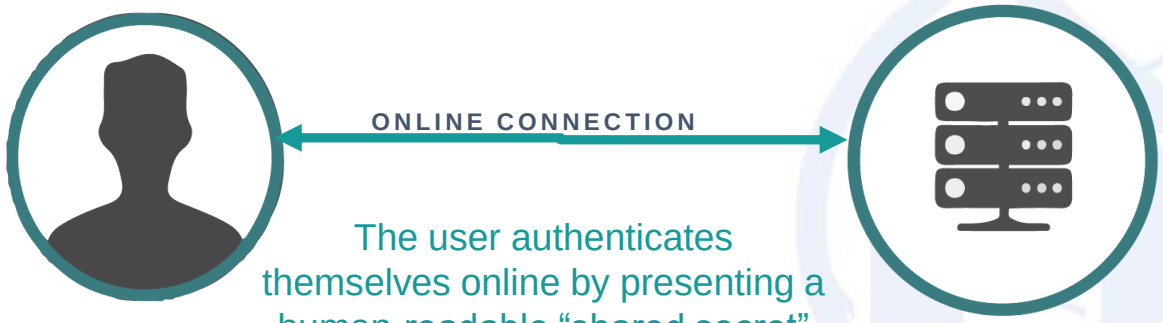
- Being confident that a previously-enrolled user is actually that user.
- Applying access control and authorization policies to that authenticated user.

Examples of technical implementations for SCA

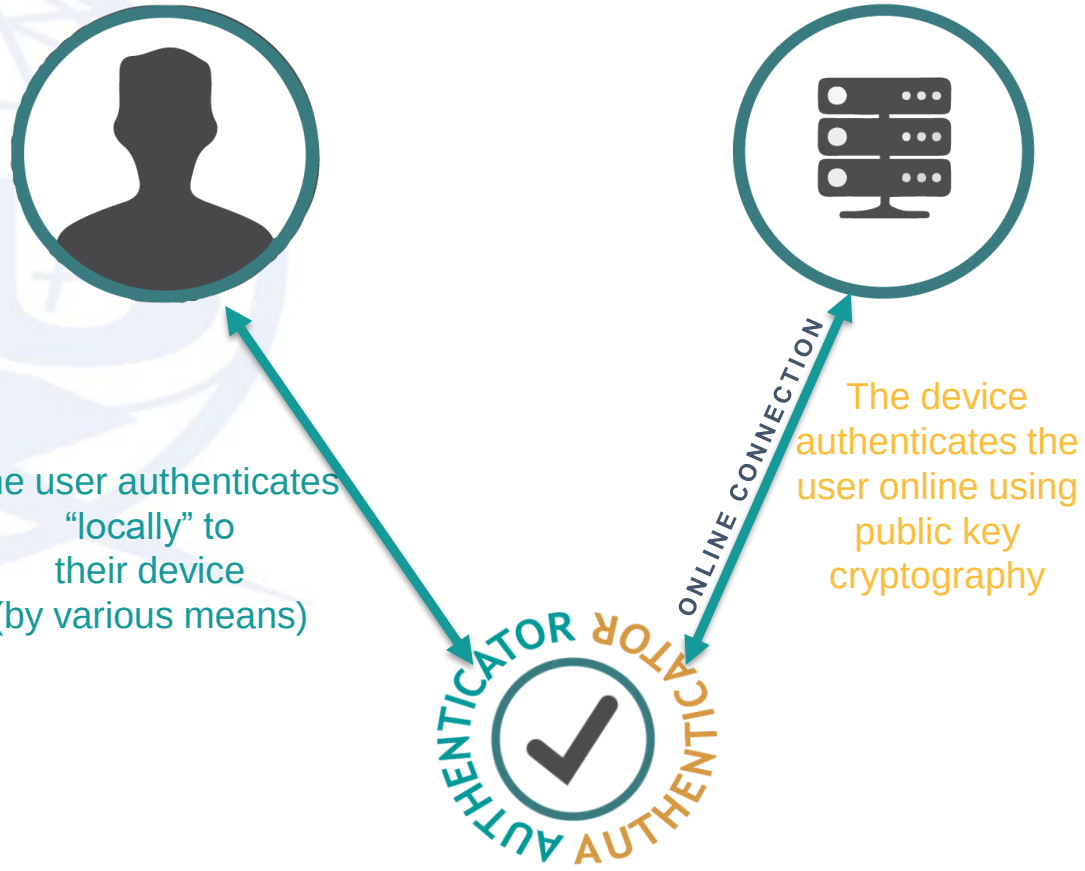
- ❑ IFAA – biometric
- ❑ Aadhaar Authentication
- ❑ Mobile Connect
- ❑ **FIDO Authentication**

Password vs FIDO

Password Authentication



FIDO Authentication



FIDO (Fast IDentity Online)

- Proposed by the FIDO Alliance: an open industry association of over 250 organizations.

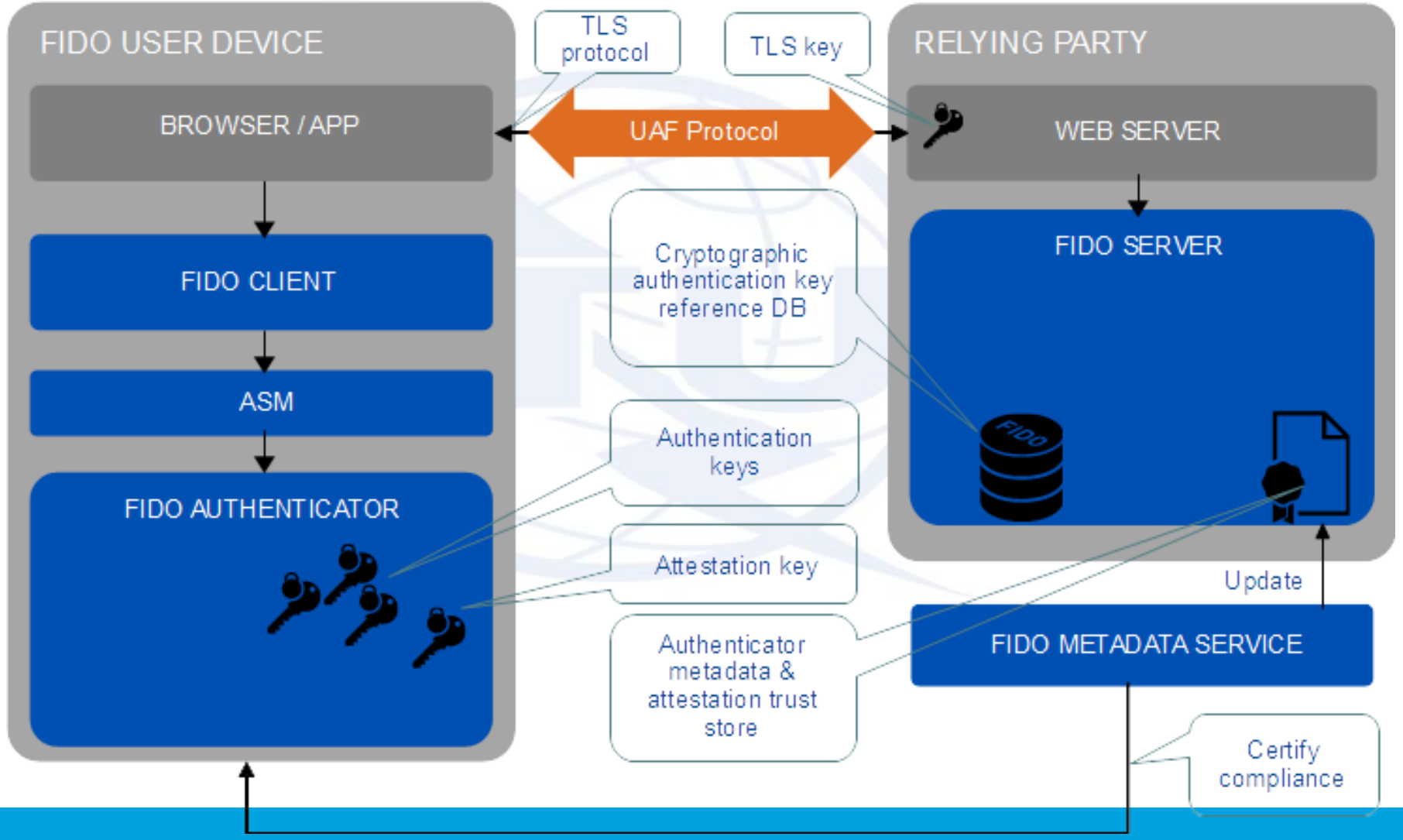
- FIDO authentication uses public key cryptography to enable simpler, faster and stronger user authentication.

- Specifies 3 major protocols (FIDO Universal 2nd Factor Authentication, FIDO Universal Authentication Framework and WebAuth)

FIDO UAF

- The authenticator – the device which stores the keys
- The server which registers users and validates authentication requests.
- The client which acts as a multiplexer and policy enforcer between multiple servers and multiple authenticators
- The protocols which defines message formats, cryptographic keys flowing between the authenticator and the client.

FIDO UAF



Source: FIDO Alliance

How it works..

- During registration, client device creates a new key pair it retains the private key and registers the public key with the online service.
- During authentication: User device proves possession of private key by signing a challenge. The private key is unlocked locally on the device
- Private keys are bound to the device.

Protection of User Personal Data

- The UAF protocol generates unique asymmetric cryptographic key pairs on a per-device, per-user account, and per-relying party basis. Cryptographic keys used with different relying parties will not allow any one party to link all the actions to the same user.

- The UAF protocol operations require minimal personal data collection: at most they incorporate a user's relying party username. This personal data is only used for FIDO purposes, for example to perform user registration, user verification, or authorization.

Protection of User Personal Data

- In UAF, user verification is performed locally. The UAF protocol does not convey biometric data to relying parties, nor does it require the storage of such data at relying parties.

- Users explicitly approve the use of a UAF device with a specific relying party. Unique cryptographic keys are generated and bound to a relying party during registration only after the user’s consent.

Advanced Authentication Systems

- Eliminate reliance on passwords
- Multimodal user authentication
- Real time analysis of user behavior
- Continuous authentication of user, software and device
- Dynamic risk scoring of authentication confidence
- Consistency across all devices and channels for the authentication confidence

ITU FIDO authentication resources

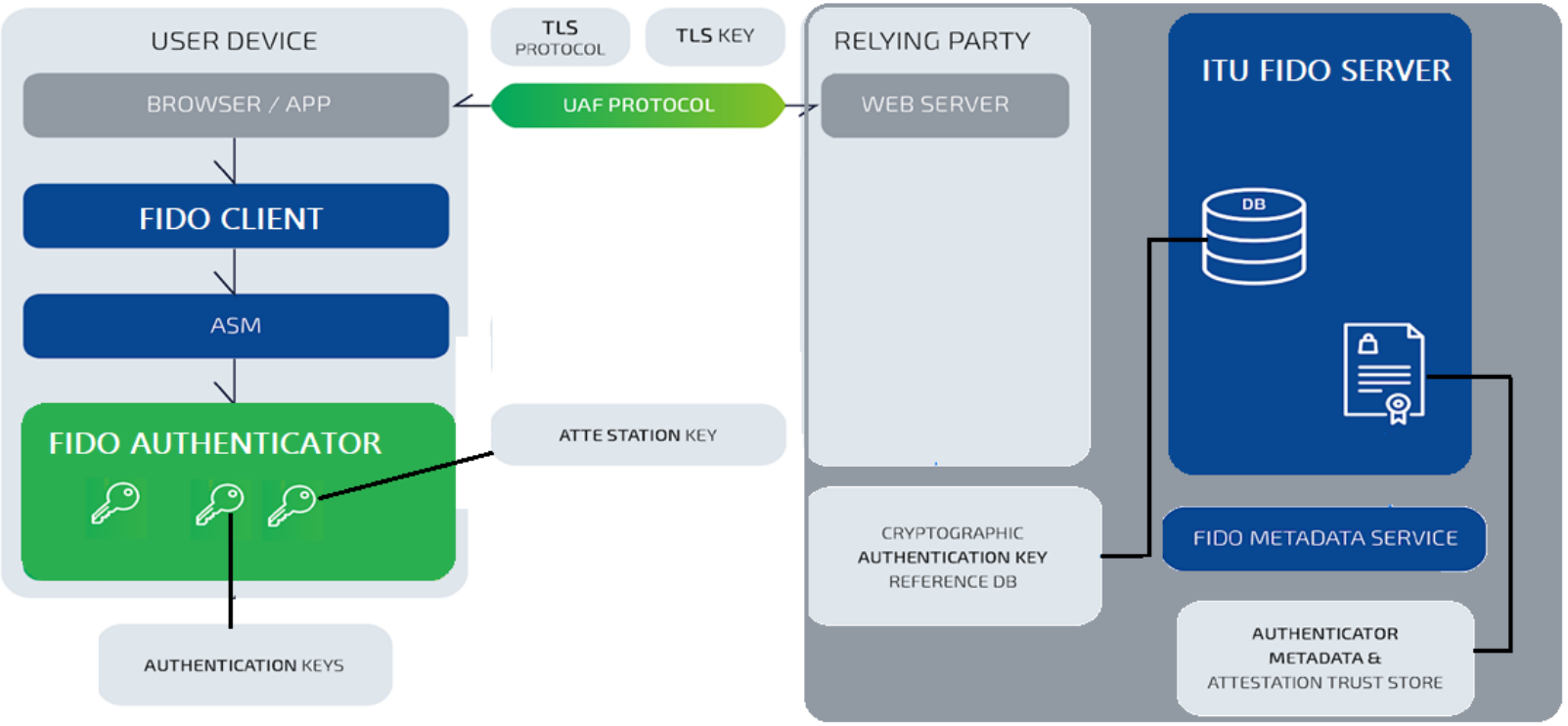
Two major changes to implement FIDO

1. Modifying the login and registration screens of their app
2. Setup a FIDO server

Resources

- Step by step guide for deploying FIDO UAF on a native app.
- A FIDO UAF compliant server to test FIDO authentication.
- Sample Android and iOS FIDO demo app with user registration, deregistration, and transaction authentication.
- *https://www.itu.int/en/ITU-T/extcoop/FIGIresources/authentication/Pages/default.aspx*

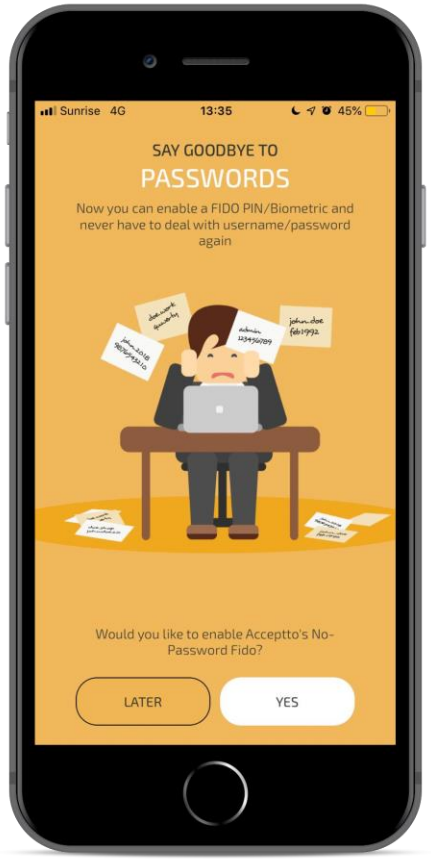
ITU FIDO authentication server and application



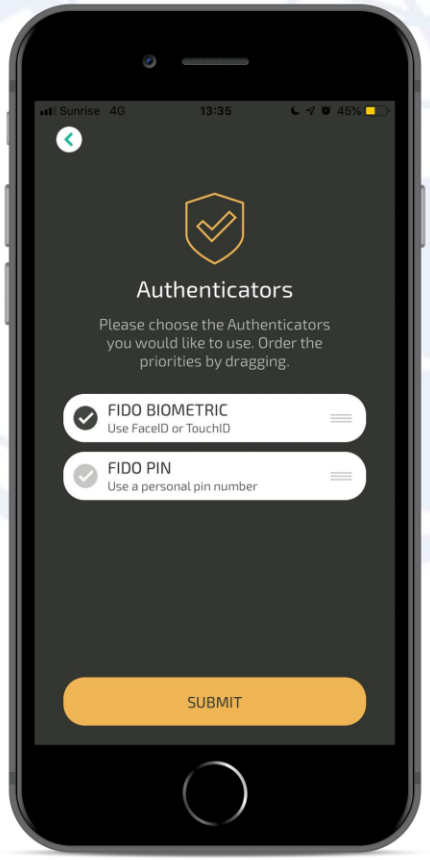
Show endpoints for register, authenticate and deregister operations using the FIDO UAF protocol specification

FIDO Demo app: User Registration

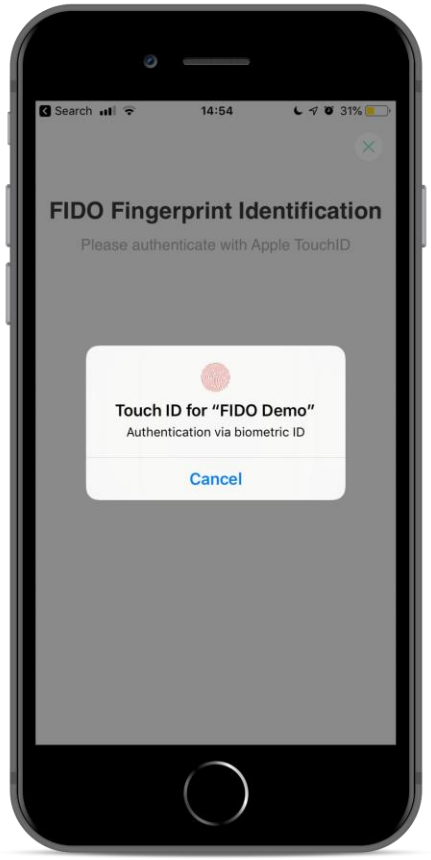
①



②

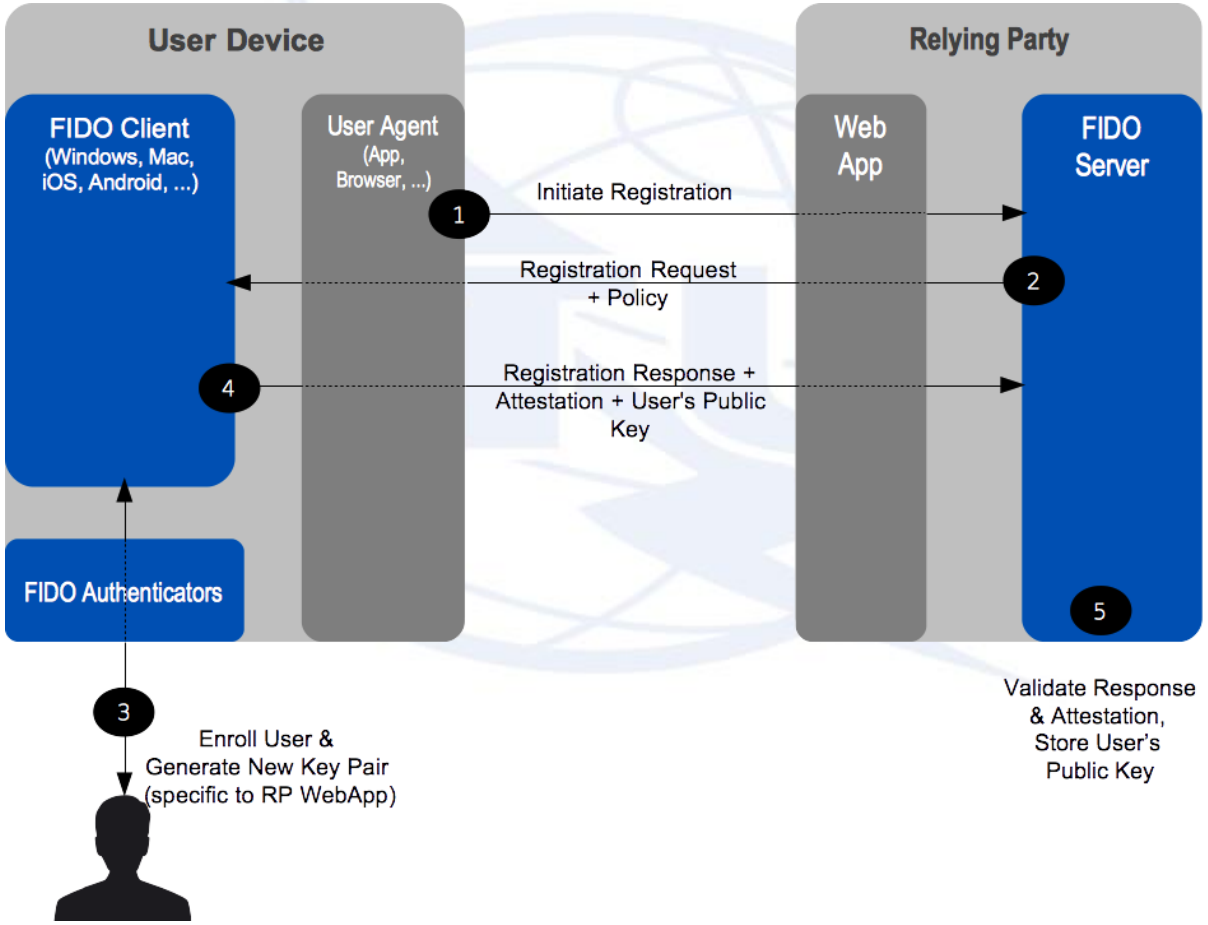


③

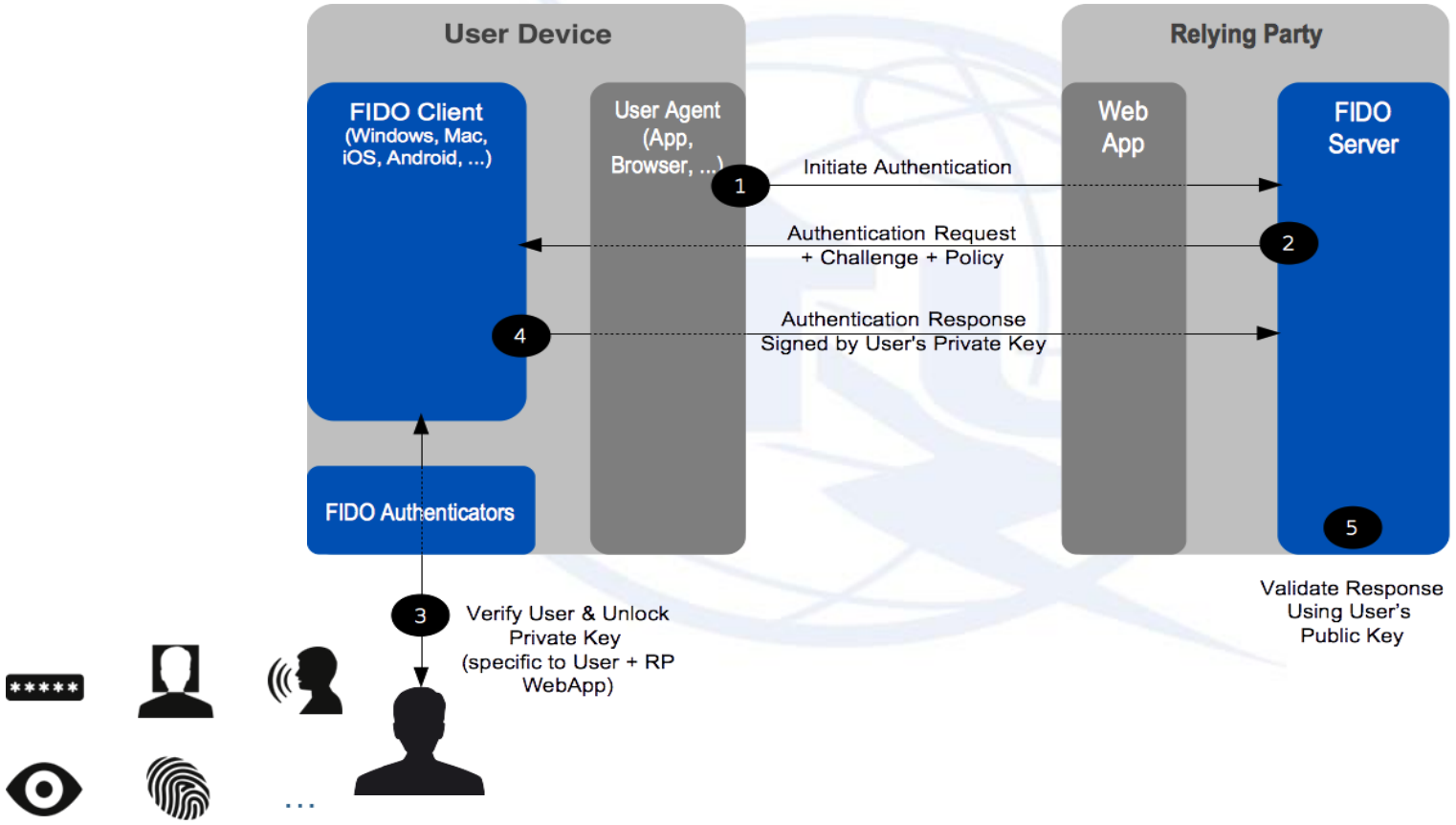


Download on Google play

FIDO UAF user registration protocol conversation

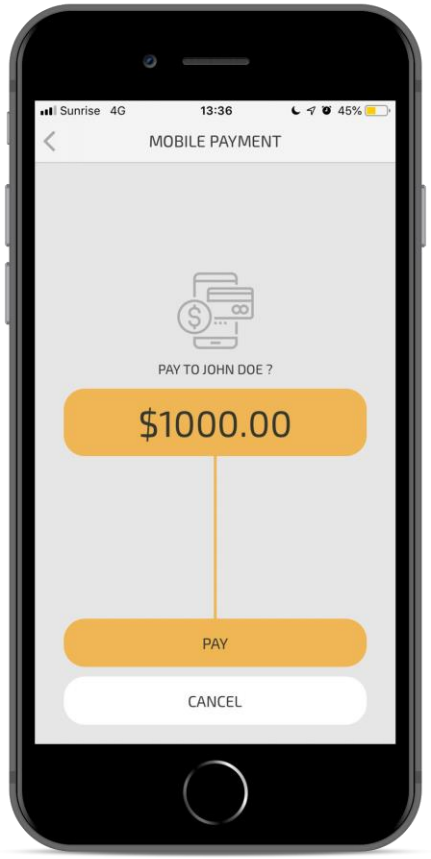


FIDO UAF user authentication conversation

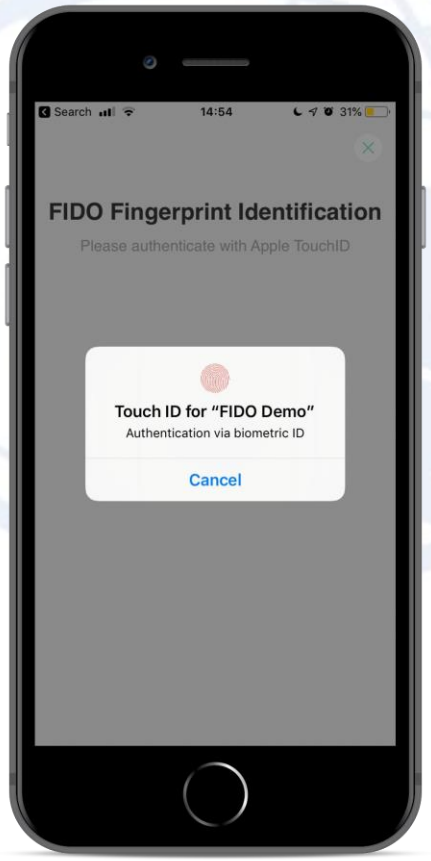


FIDO UAF Demo app: Transaction confirmation

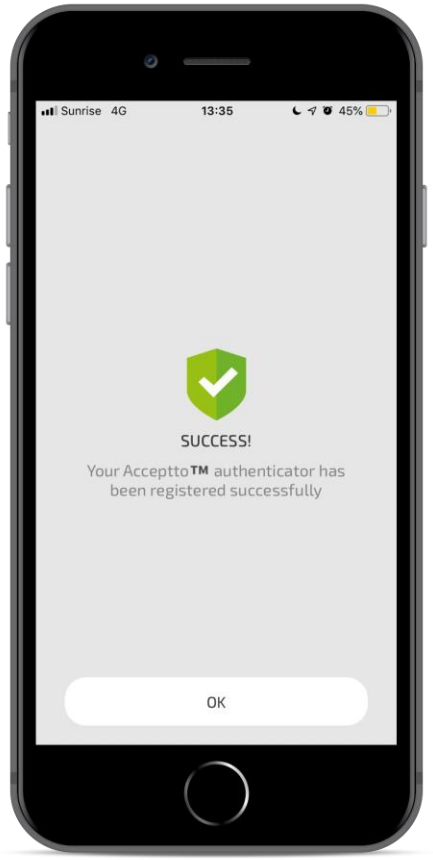
④



⑤

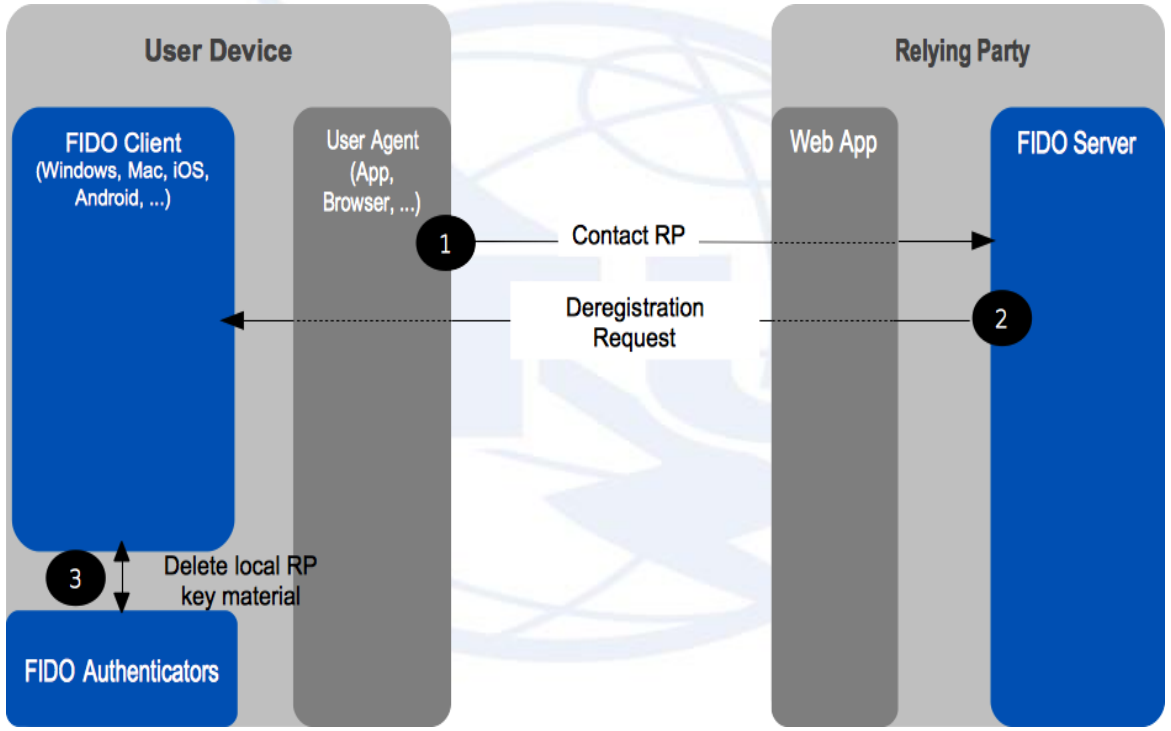


⑥



Download on Google play

FIDO UAF deregistration



ITU FIDO resources
https://www.itu.int/en/ITU-T/extcoop/FIGIresources/authentication/Pages/default.aspx

FIDO demo app
https://play.google.com/store/apps/details?id=com.acceptto.fidodemonstration

For more information on testing FIDO using ITU server contact: vijay.mauree@itu.int

Thank You