openHPI Course: Digital Identities – Who am I on the Internet?

# Secure Authentication with FIDO

**Prof. Dr. Christoph Meinel**

Hasso Plattner Institute
University of Potsdam, Germany

# Introduction

The concept of FIDO is to provide **alternatives to password based authentication**, especially by means of alternative authentication methods, e.g.

  - □ fingerprint readers, special USB sticks, …

**FIDO** = **F**ast **Id**entity **O**nline

Authentification should be done **locally**, i.e.,

  - □ no secrets are stored centrally

- Use of alternative authentication methods (e.g. biometrics) should be simplified, also as a **second factor**

# Specifications for Alternative Authentication Procedures

FIDO provides a set of specifications for alternative authentication methods

- **Specification** = "**implementation basis**" for all involved parties, e.g. browser manufacturers, end device manufacturers, service providers
- Initial specifications: **U2F**, **UAF**

**FIDO Universal 2**nd Factor (**U2F**)

- Websites can require a strong second factor for registration, e.g. a FIDO Security Key
- FIDO Security Key is a special (certified) USB device that can perform various cryptographic operations, e.g. key generation

Source: https://www.yubico.com/products/

# FIDO UAF and FIDO 2

**FIDO** **U**niversal **A**uthentication **F**ramework (**UAF**)

- Use local authentication methods of end devices for web authentication, e.g. fingerprint via smartphone

**FIDO2 extends FIDO**, integrates W3C Web Authentication specification and extends the Client-to-Authenticator protocols of FIDO

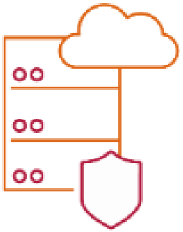
- W3C Web Authentication Specification (**WebAuthN**) specifies a programming interface in web browsers so that **FIDO** can be accessed directly via this interface
- **C**lient-**T**o-**A**uthenticator **P**rotocol (**CTAP**) controls the communication between web browser and so-called **authenticators** for actual authentication

# FIDO Registration and Login

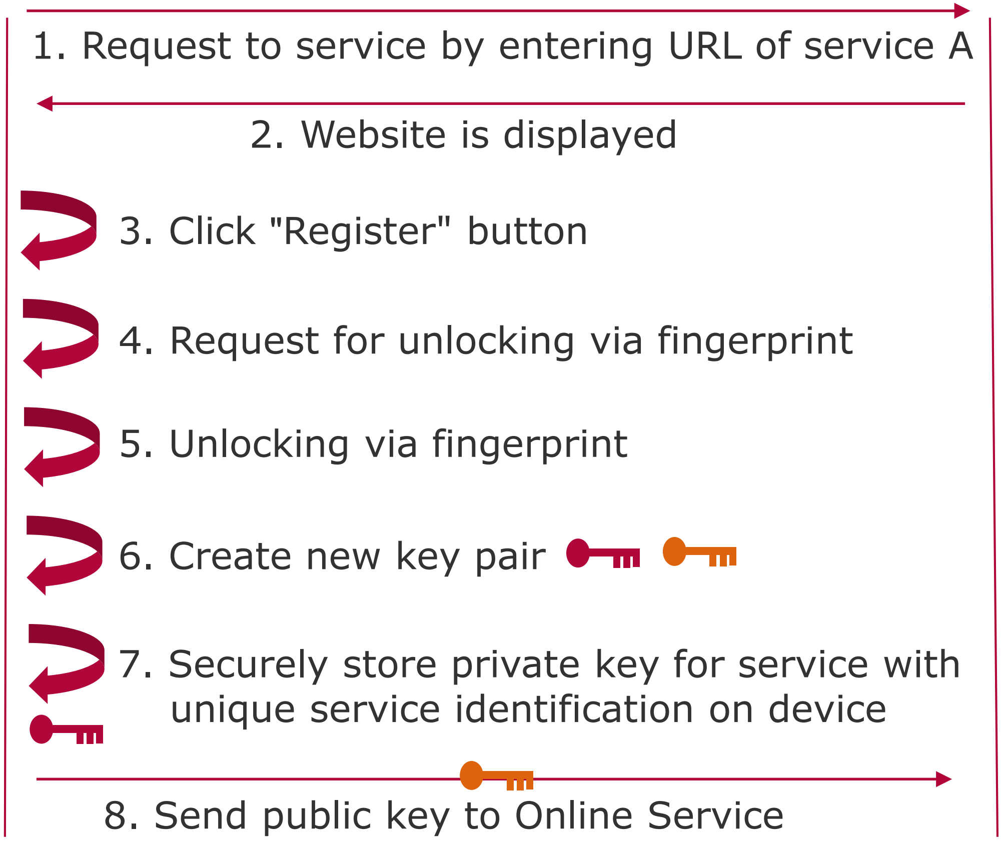
FIDO defines special protocols for the initial registration process and for subsequent authentication with services

- Security is based on **asymmetric encryption**, i.e. with private and public keys
- During registration, the end device creates a new key pair for each new service
  - **private key** is used to sign a so-called challenge
    - key is stored locally on device
    - key only available after unlocking the device, e.g. via fingerprint, secure key, etc.
  - **public key** is added to the service to be used
    - required for verification of the signed challenge
- No secret leaves the end device!

# Example:
# FIDO Registration with Fingerprint



Online Service **A**



1. Request to service by entering URL of service A

2. Website is displayed

3. Click "Register" button

4. Request for unlocking via fingerprint

5. Unlocking via fingerprint

6. Create new key pair 🔑 🔑

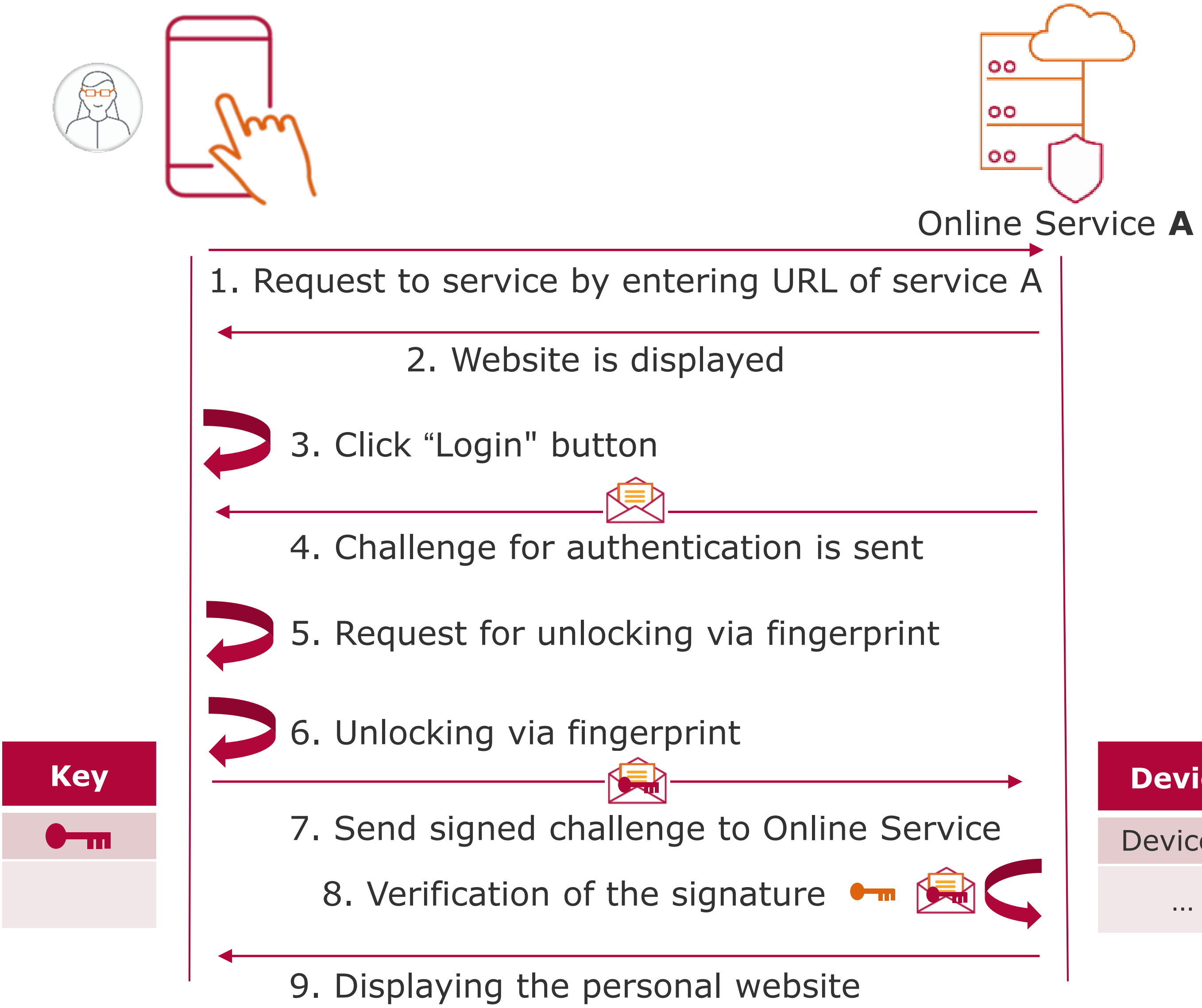
7. Securely store private key for service with unique service identification on device

8. Send public key to Online Service

| Service | Key |
|---|---|
| Service A | 🔑 |
| … | |

| Device | Key |
|---|---|
| Device A | 🔑 |
| … | |

# Example:
# FIDO Authentication with Fingerprint



1. Request to service by entering URL of service A
2. Website is displayed
3. Click “Login" button
4. Challenge for authentication is sent
5. Request for unlocking via fingerprint
6. Unlocking via fingerprint
7. Send signed challenge to Online Service
8. Verification of the signature
9. Displaying the personal website

| **Service** | **Key** |
|---|---|
| Service A | 🔑 |
| … | |

| **Device** | **Key** |
|---|---|
| Device A | 🔑 |
| … | |

# FIDO
## Advantages and Disadvantages

- **Advantages**
  - Secure authentication using multi-factor authentication
  - Easy and fast to use
  - Can replace passwords
  - Effective against phishing attacks, since the authenticator can verify, whether the challenge was sent from a valid source
- **Disadvantages**
  - Special hardware needed
  - Additional authentication step necessary

# FIDO
## Summary

- FIDO is a set of methods for simple and strong authentication
- FIDO offers password-less multi-factor authentication, which is resistant to phishing attacks
- FIDO is based on special hardware (authenticator) which is responsible for…
  - generation of user credentials
  - registration and authentication processes
- Not all, but many online services already support FIDO, e.g. GitHub, Dropbox, Twitter