FIGI Security Clinic

Part III: Public Private Sector Adoption of FIDO

Abbie Barbir, Cvs Health
Rolf Lindemann, Nok Nok Labs

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

Authentication

Authentication Categories

1. **Who you are**
   - biometric, behavioral attributes
2. **What you know**
   - Shared secrets, public and relationship knowledge (S/D KBA)
3. **What you Have**
   - Devices, tokens (hard/soft, OTP)
4. **What you typically do**
   - Behavioral habits that are independent of physical biometric attributes
5. **Context**
   - Example location, time, party, prior relationship, social relationship[and source

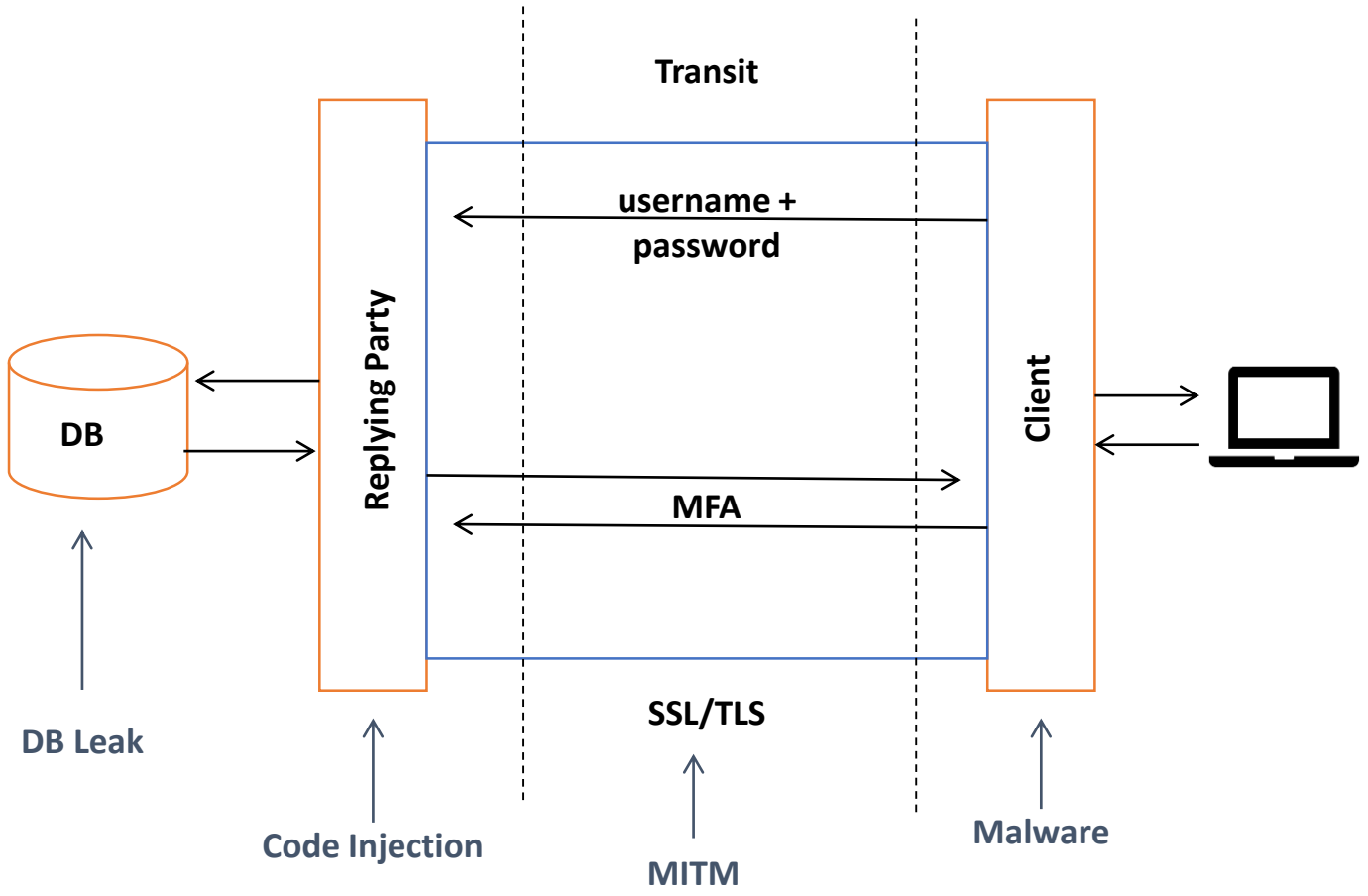
Strong Authentication

European payments are changing

- Payment Services Directive (PSD2) regulation requires Strong Customer Authentication (SCA) for many online payments
- Strong customer authentication (SCA) is a requirement of the EU Revised Directive on Payment Services (PSD2) on payment service providers within the European Economic Area.
- Ensures that electronic payments are performed with multi-factor authentication
- The SCA requirement comes into force from 14 September 2019
- Need better definition of SCA

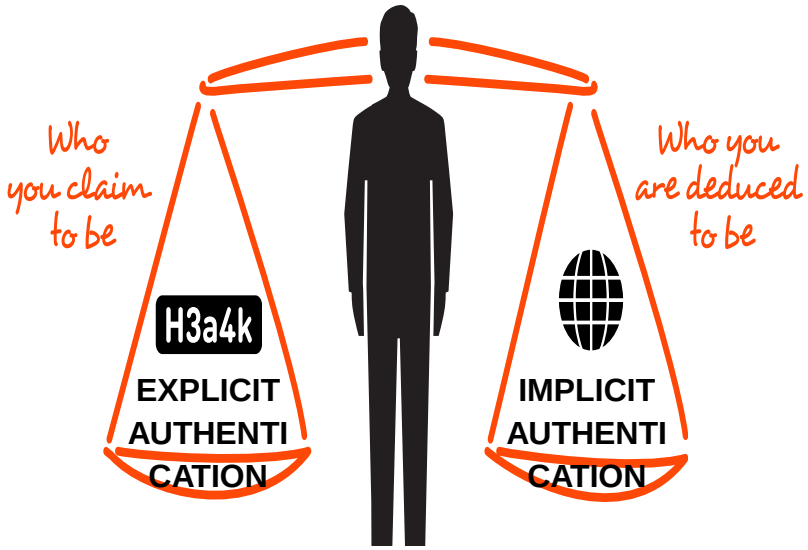
MFA issues

- Passwords
  - Based on Shared Secret
  - Account Take Over risks
  - KBA is easy to overcome
    - Data Breaches
- MFA
  - One of factor from each auth categories
  - Still Phishable
- Device Binding
  - Browser Fingerprinting (BFP)

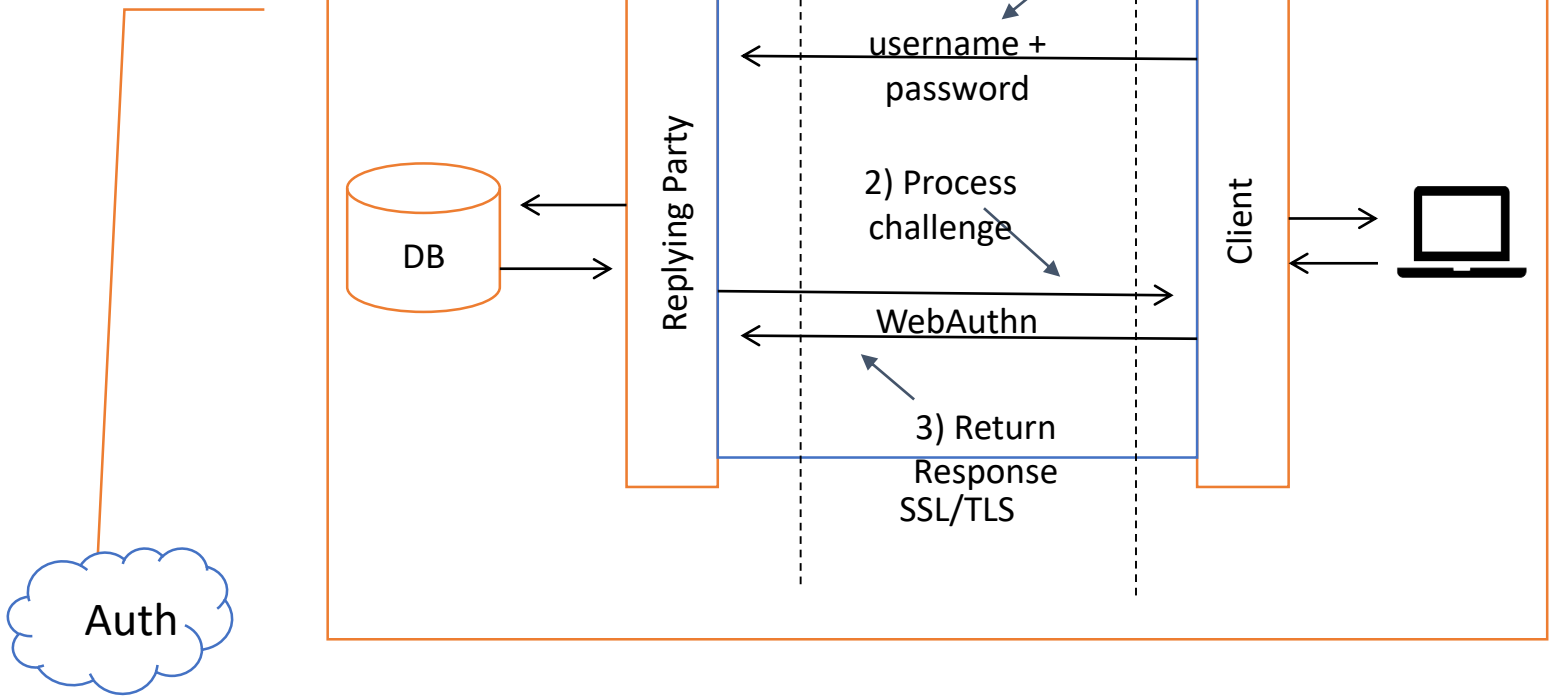


Source: Reece Guida

Real Strong Authentication - FIDO



- MUST eliminate symmetric shared secrets
- Address poor user experiences and friction
- FIDO is a building block



Need for Certification

1. FIDO compliance and certification Categories
2. Authentication modules
   - Biometric FAR/FRR