2023 INTERNET2 TECHNOLOGY exchange

Passwordless Authentication

Peter Balcirak, CESNET & Masaryk University

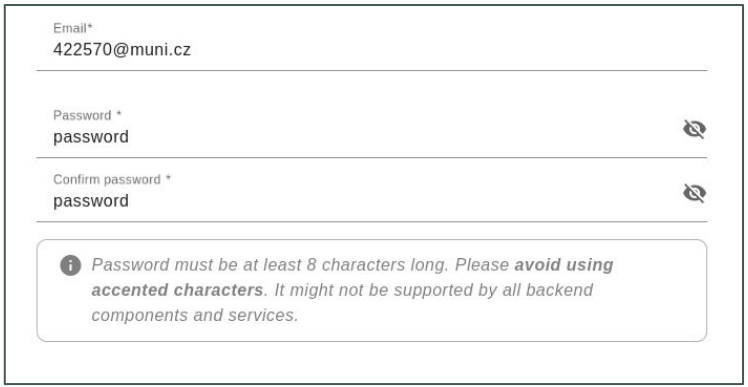
Authentication

- Validation process of proclaimed identity
- Factors
  - Something you **know**
  - Something you **have**
  - Something you **are**

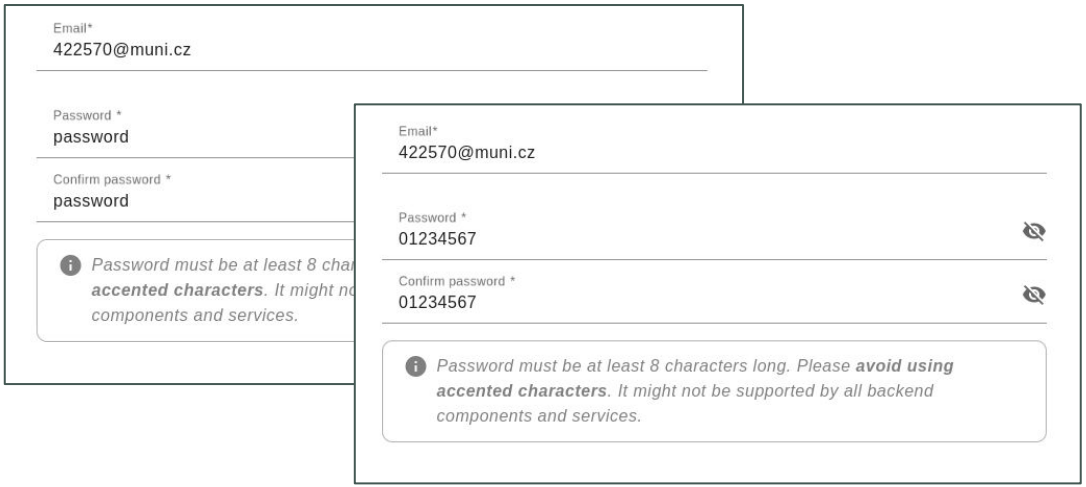
Passwords

- Easy to use
- Easy to implement
- Relatively secure on server side
- Not secure on user side

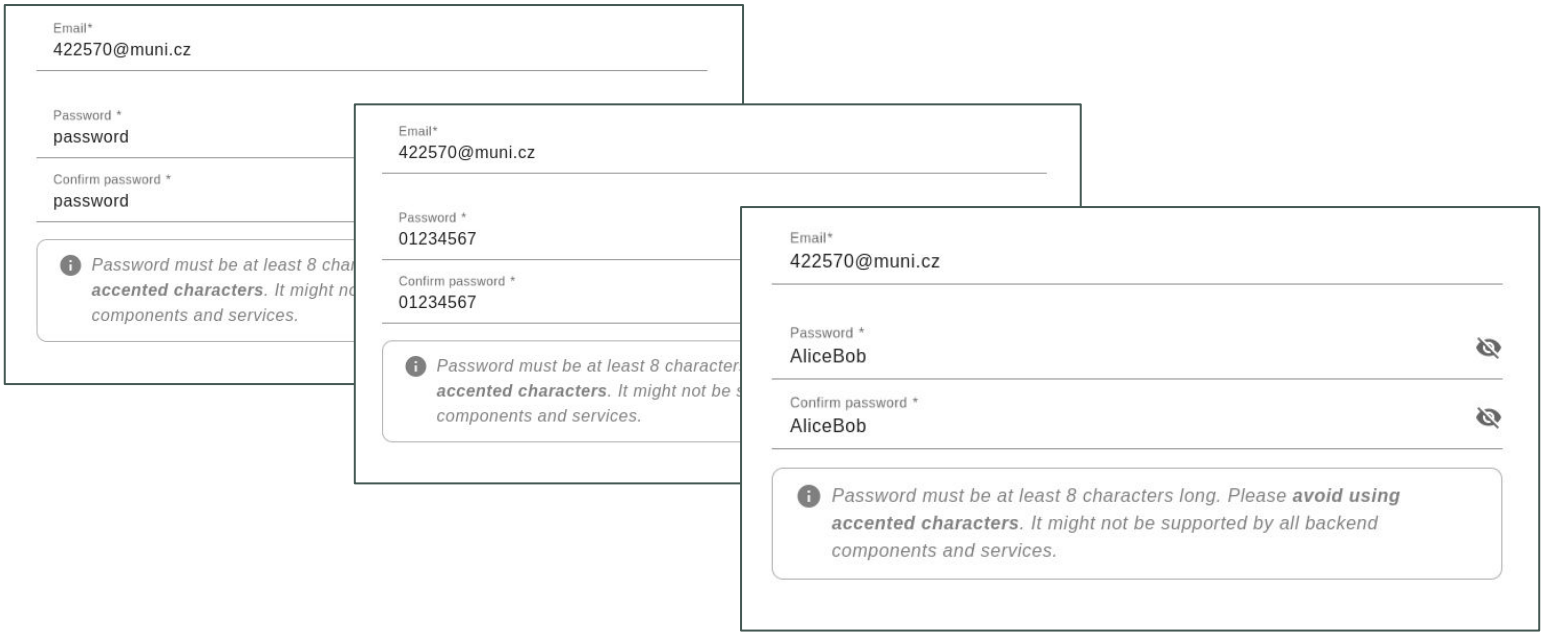
Passwords - Easy to break



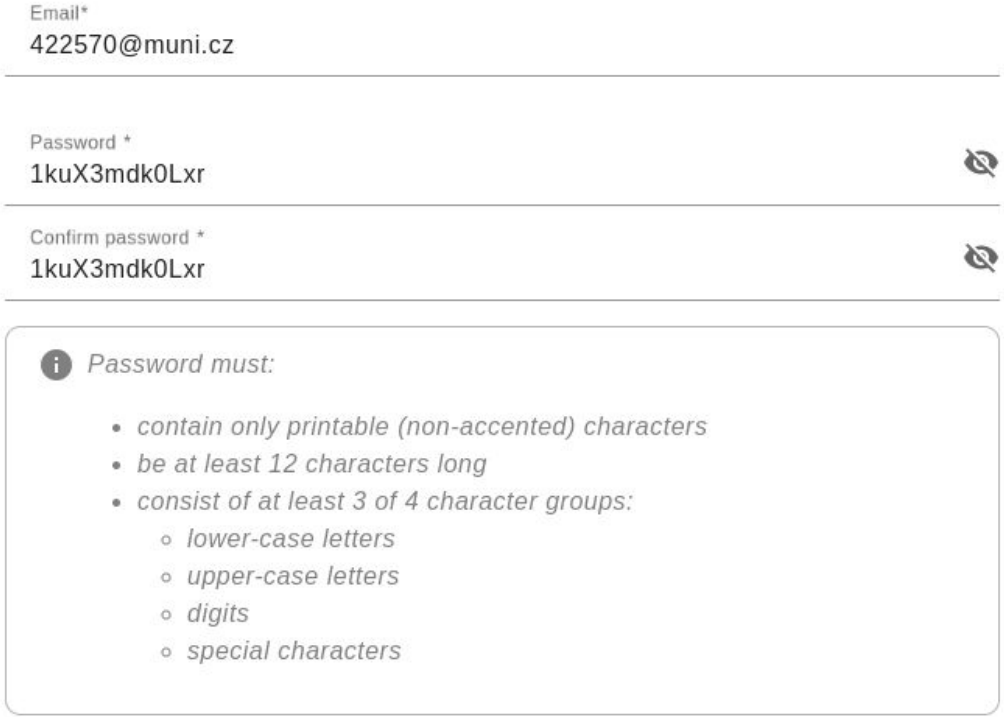
Passwords - Easy to break



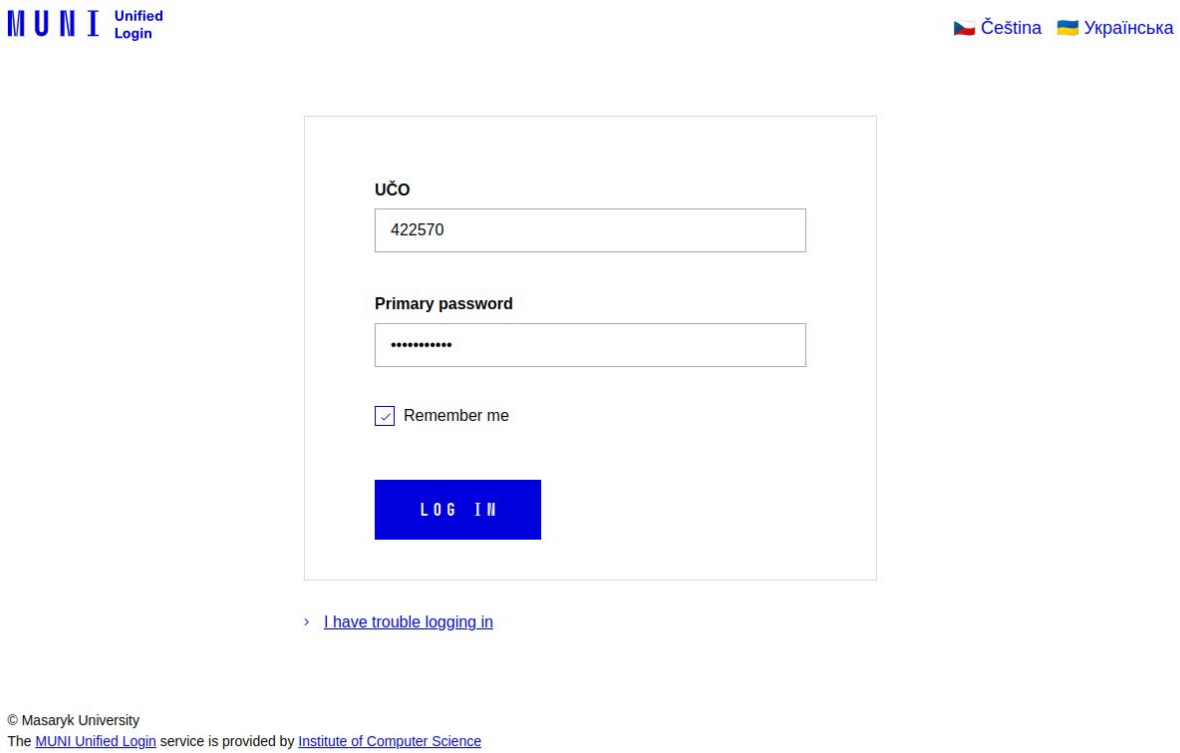
Passwords - Easy to break



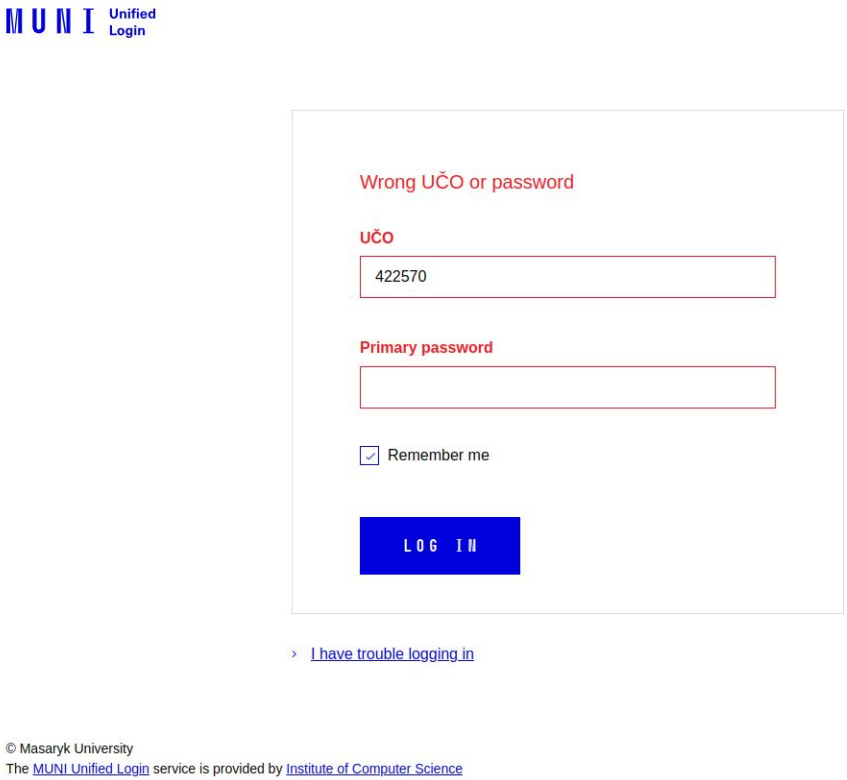
Passwords - Easy to forget



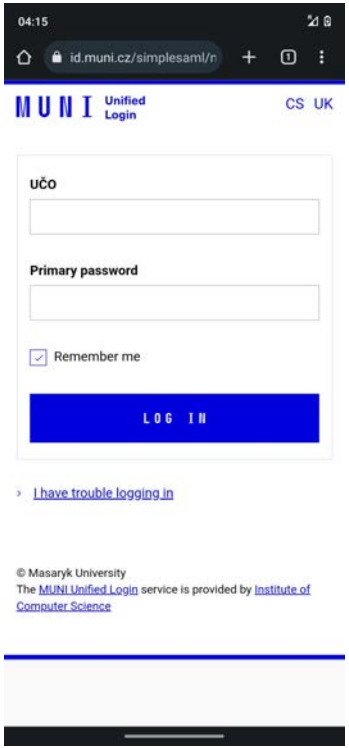
Passwords - Easy to forget



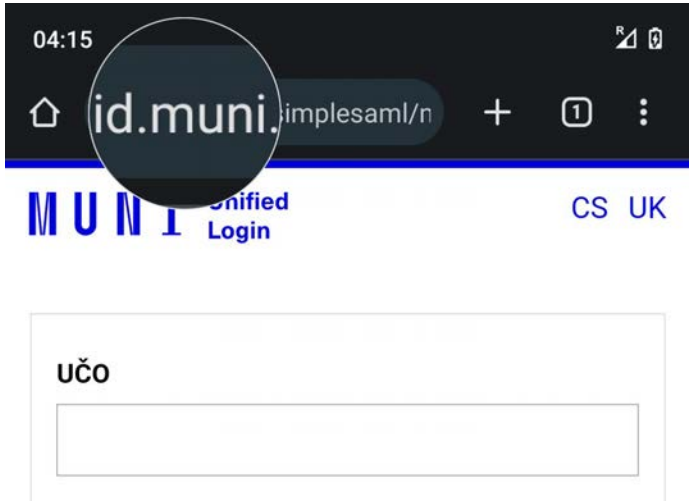
Passwords - Easy to forget

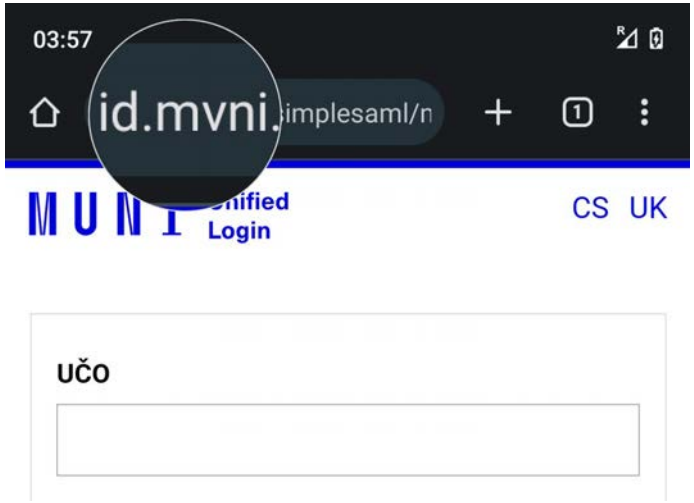


Passwords - Phishing



Passwords - Phishing





What can we do?

- Increase password requirements
- Implement weak pass check
- Force to use password managers

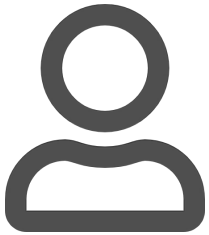
What can we do?

- Increase password requirements
- Implement weak pass check
- Force to use password managers
- Enable Multi-Factor Authentication (MFA)

MFA

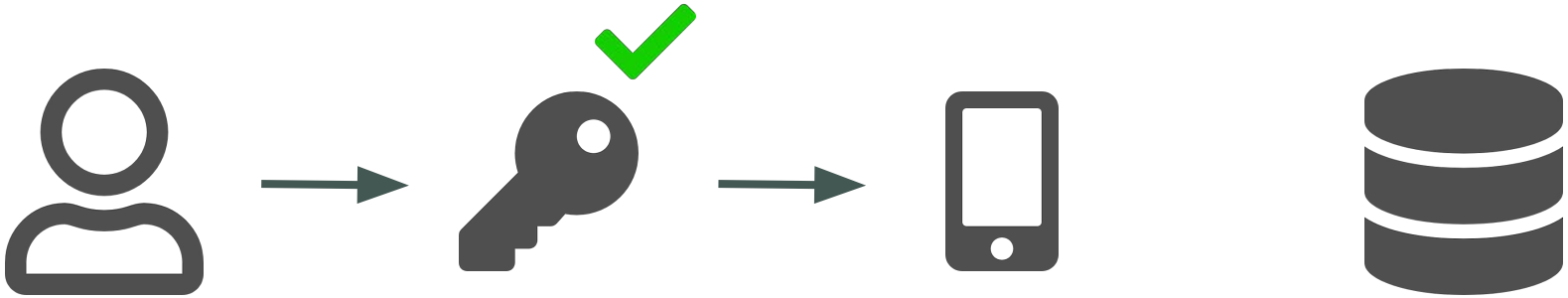
- Combines more authentication factors (at least 2)
- Usually something you know + something you have
- Improves security
- Should not be difficult for users

MFA - User flow

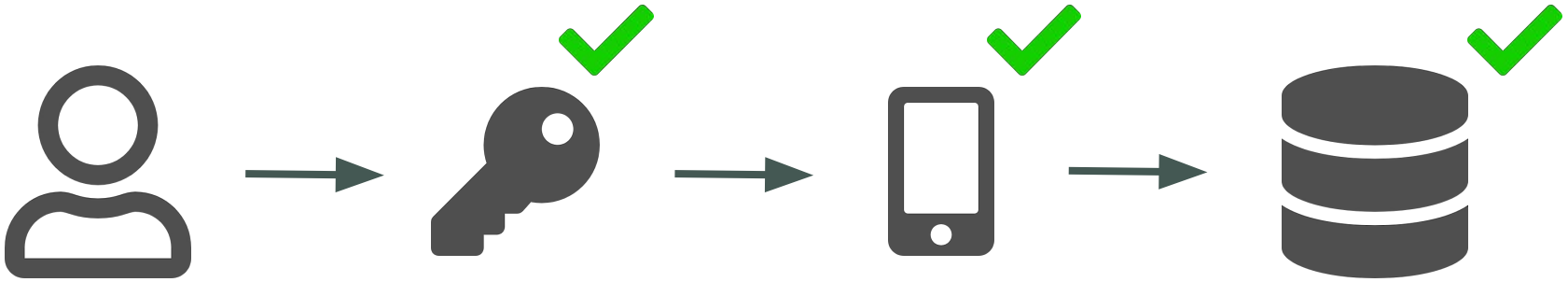


MFA - User flow

MFA - User flow



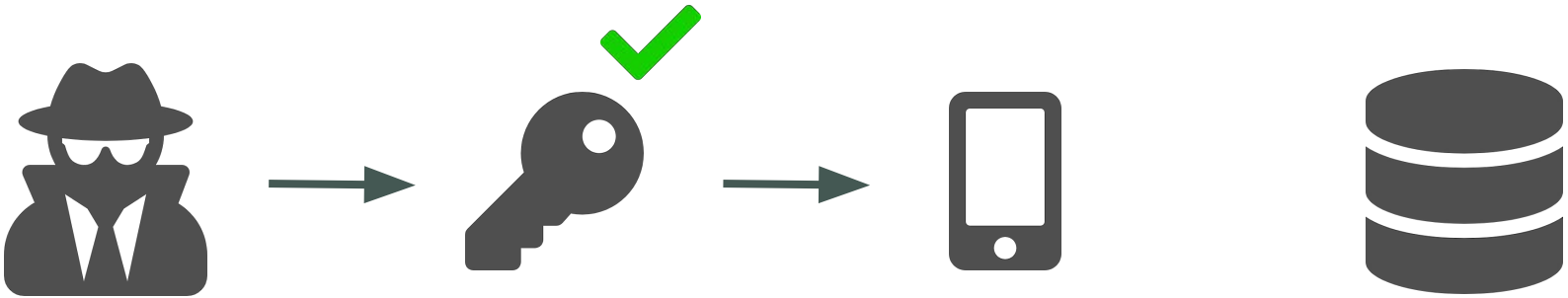
MFA - User flow



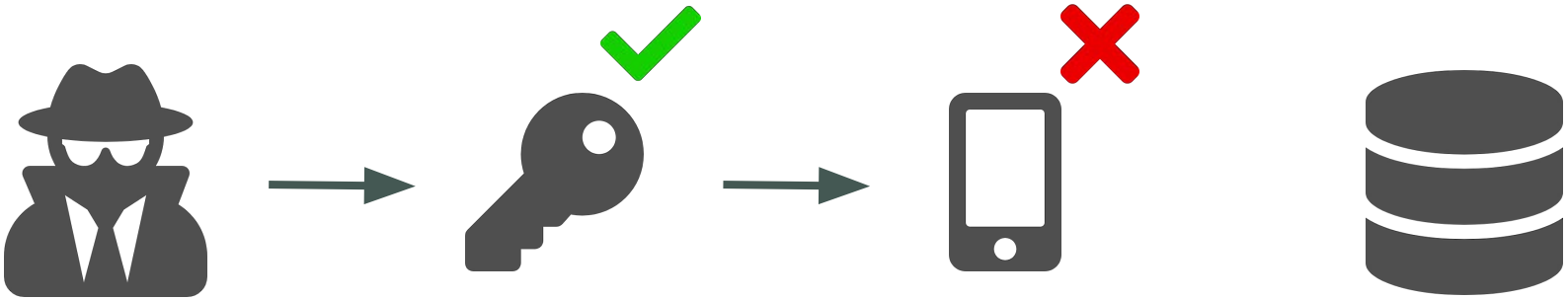
MFA - Attacker flow

MFA - Attacker flow

MFA - Attacker flow



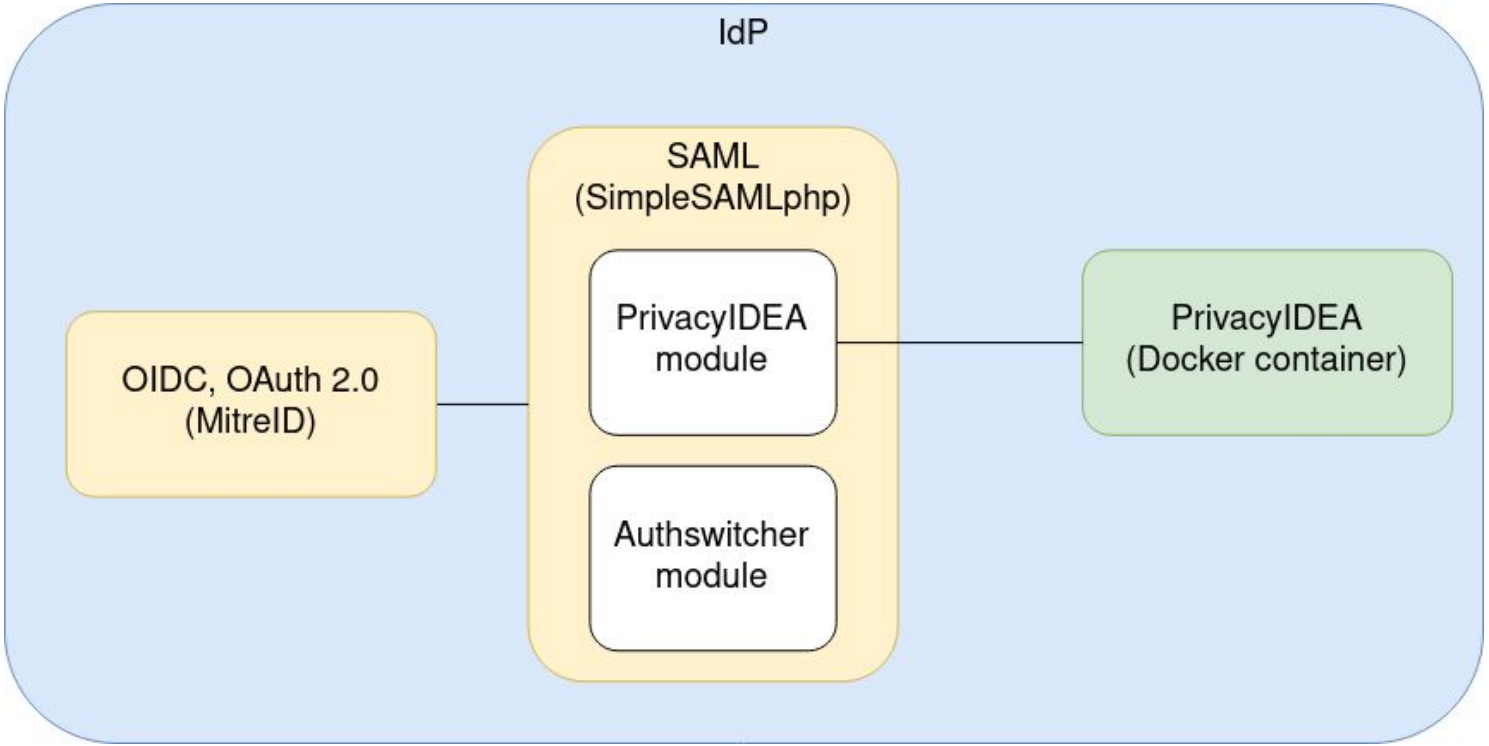
MFA - Attacker flow



MFA - Our solution

- Built on top of the PrivacyIDEA
  - Open-source project
  - Easy to integrate and extend
  - Large community
  - UI for token management
  - API for authentication
- Solution follows the REFEDS MFA Profile
- Currently supports TOTP and WebAuthn

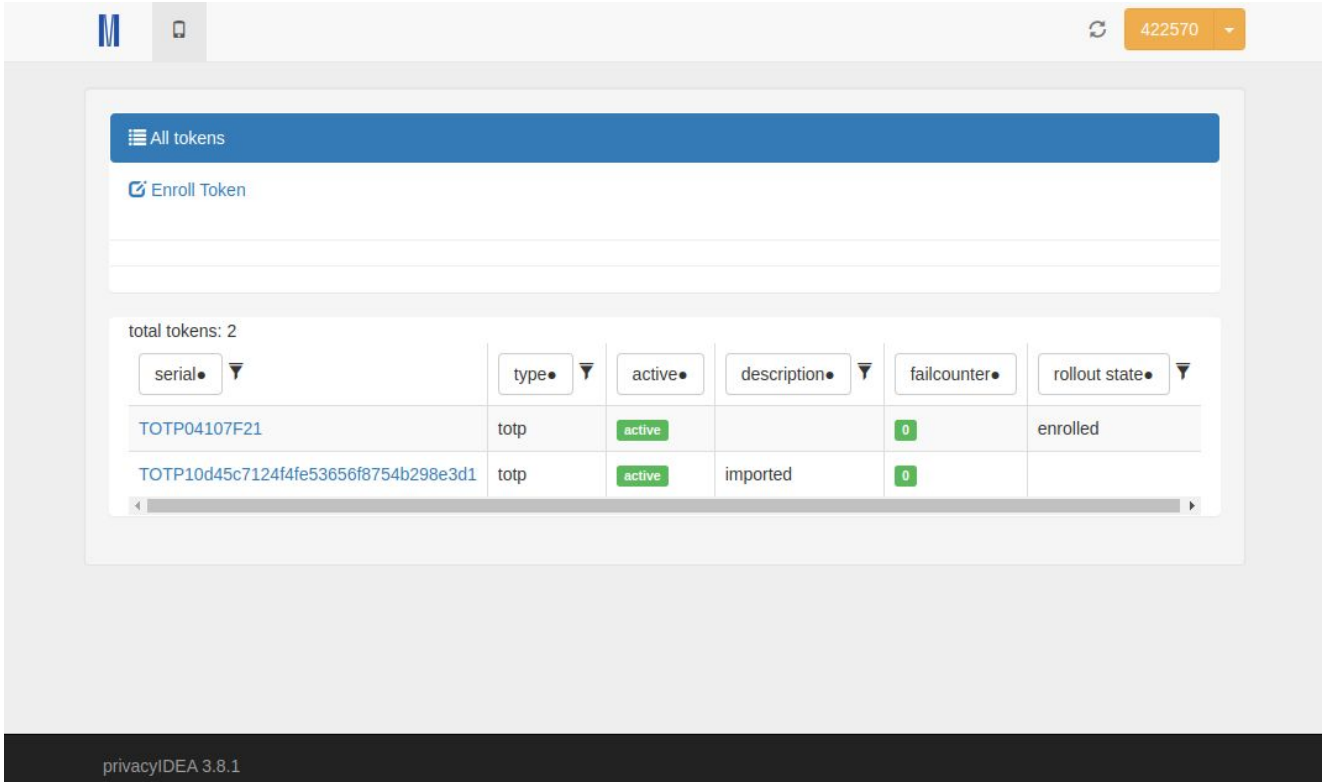
MFA - Architecture



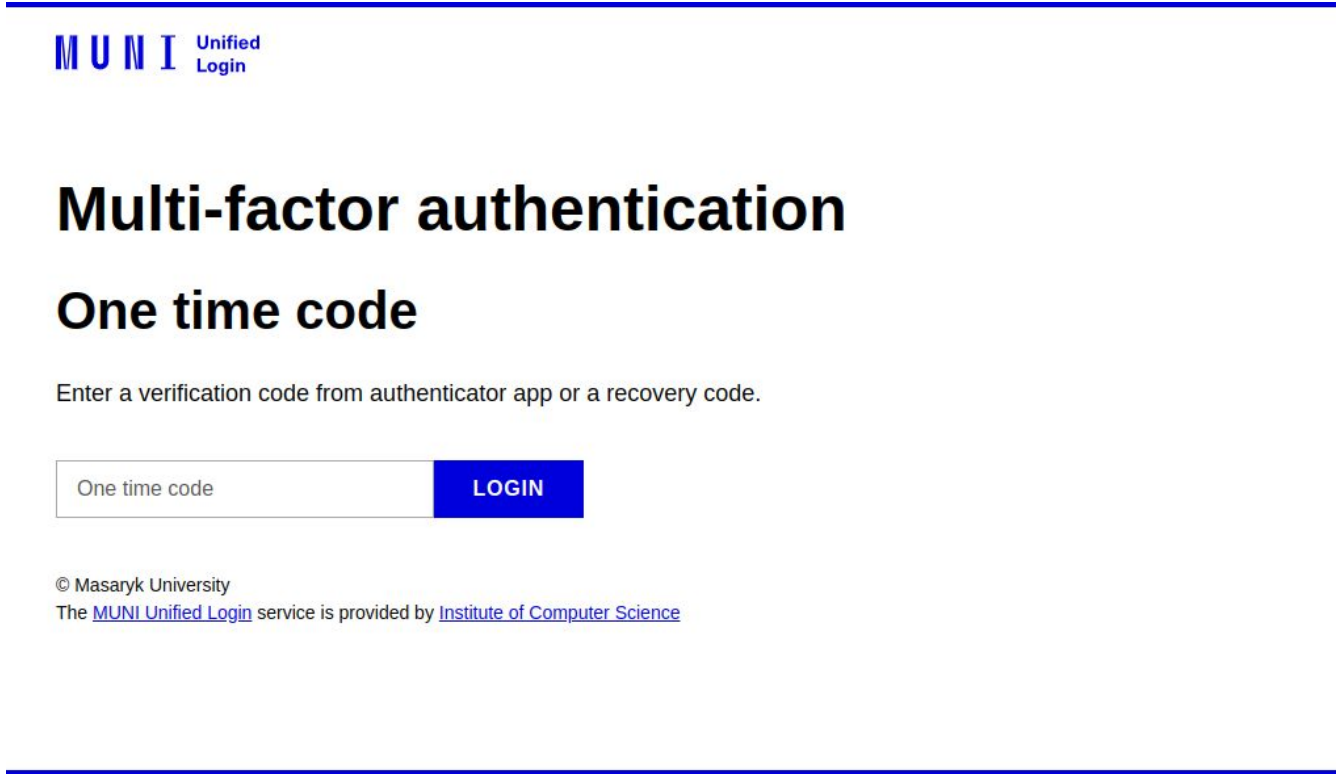
MFA - PrivacyIDEA SimpleSAMLphp module

MFA - Authswitcher SimpleSAMLphp module

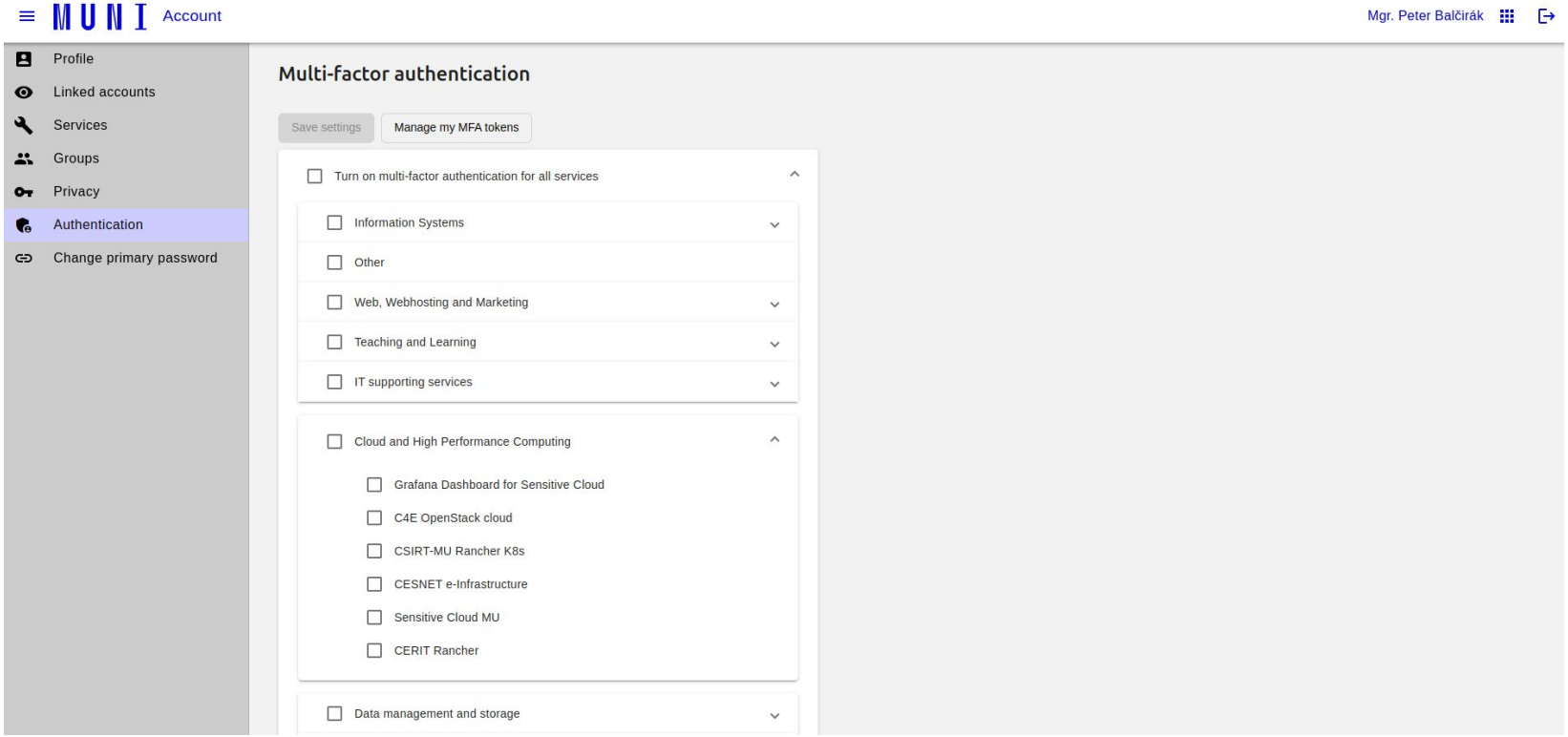
MFA - Token management



MFA - Authentication page



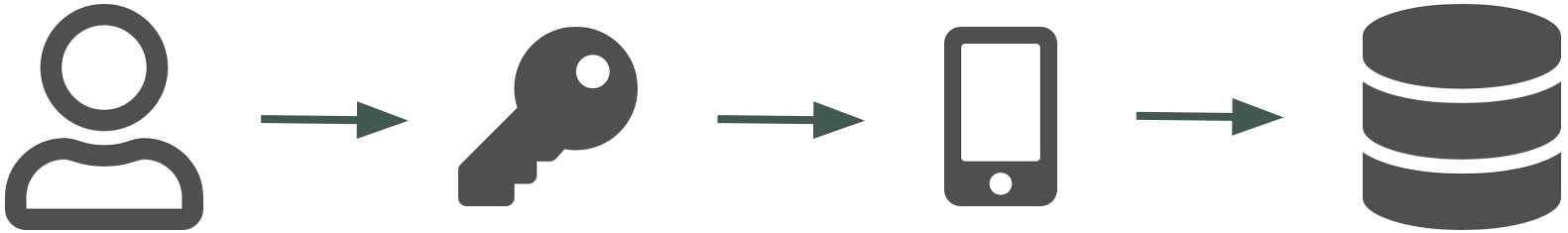
MFA - Services management (end user)



MFA - Summary

- Is it secure?
- Is it user friendly?
- Is it necessary?

MFA - User flow



Passwordless - User flow

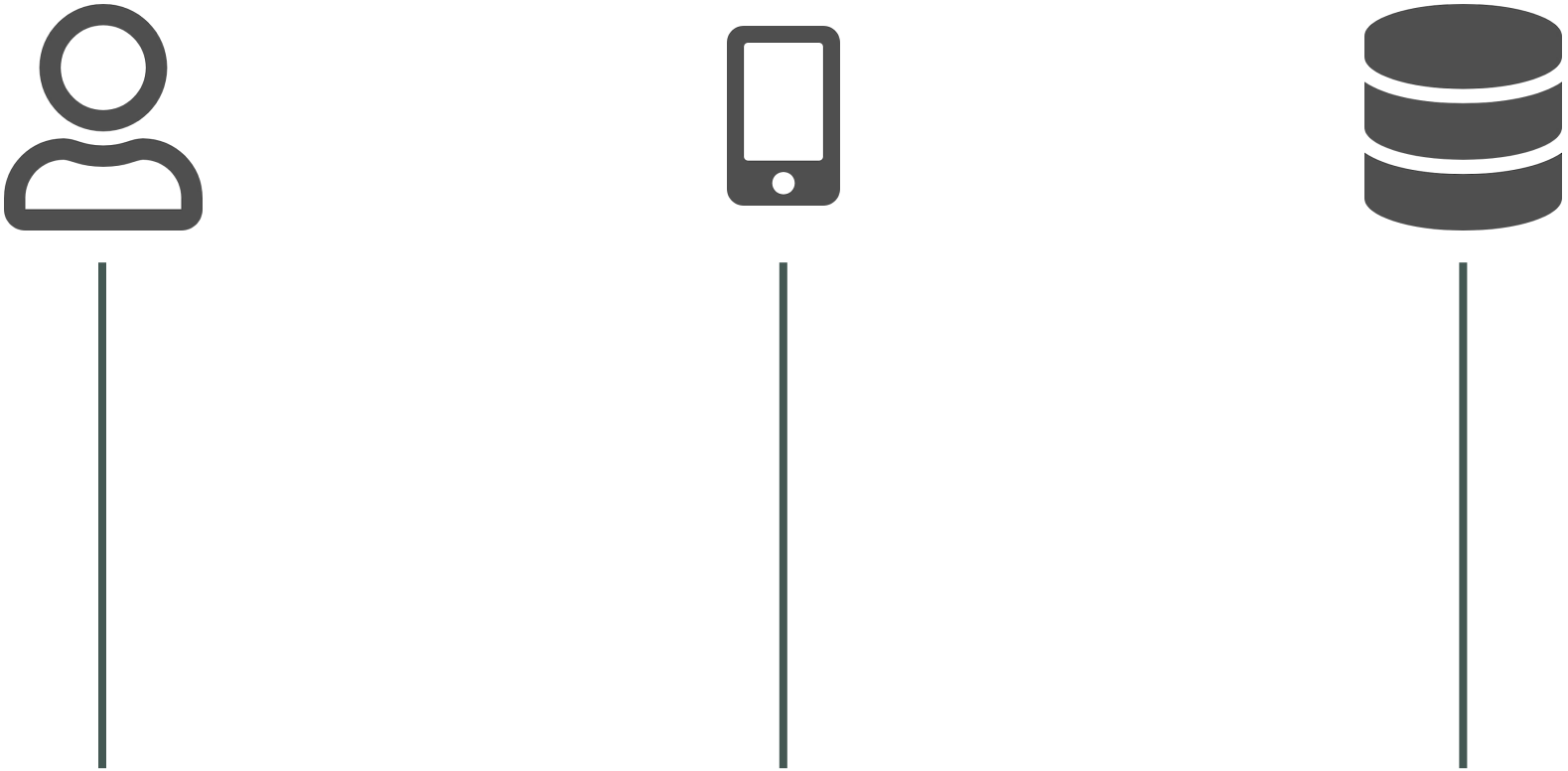
Passwordless

- Based on something user has
- Trade-off between security and user experience?
- Eliminates the most common vector of attacks

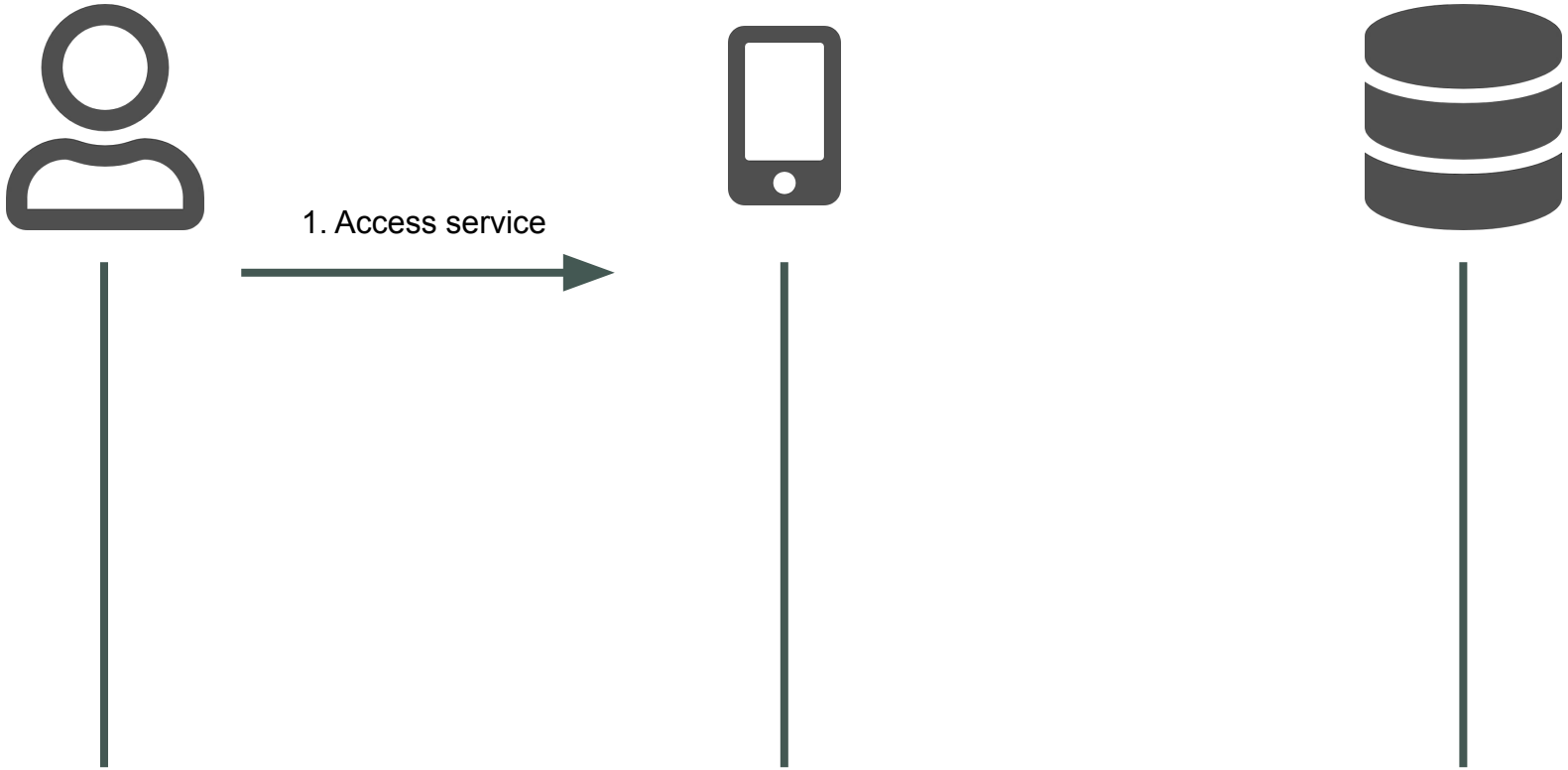
Passkeys

- Created by W3C and FIDO alliance
- Built on top of the WebAuthn standard
- Can be synchronised between devices
- Does not necessarily require username
- Highly phishing resistant

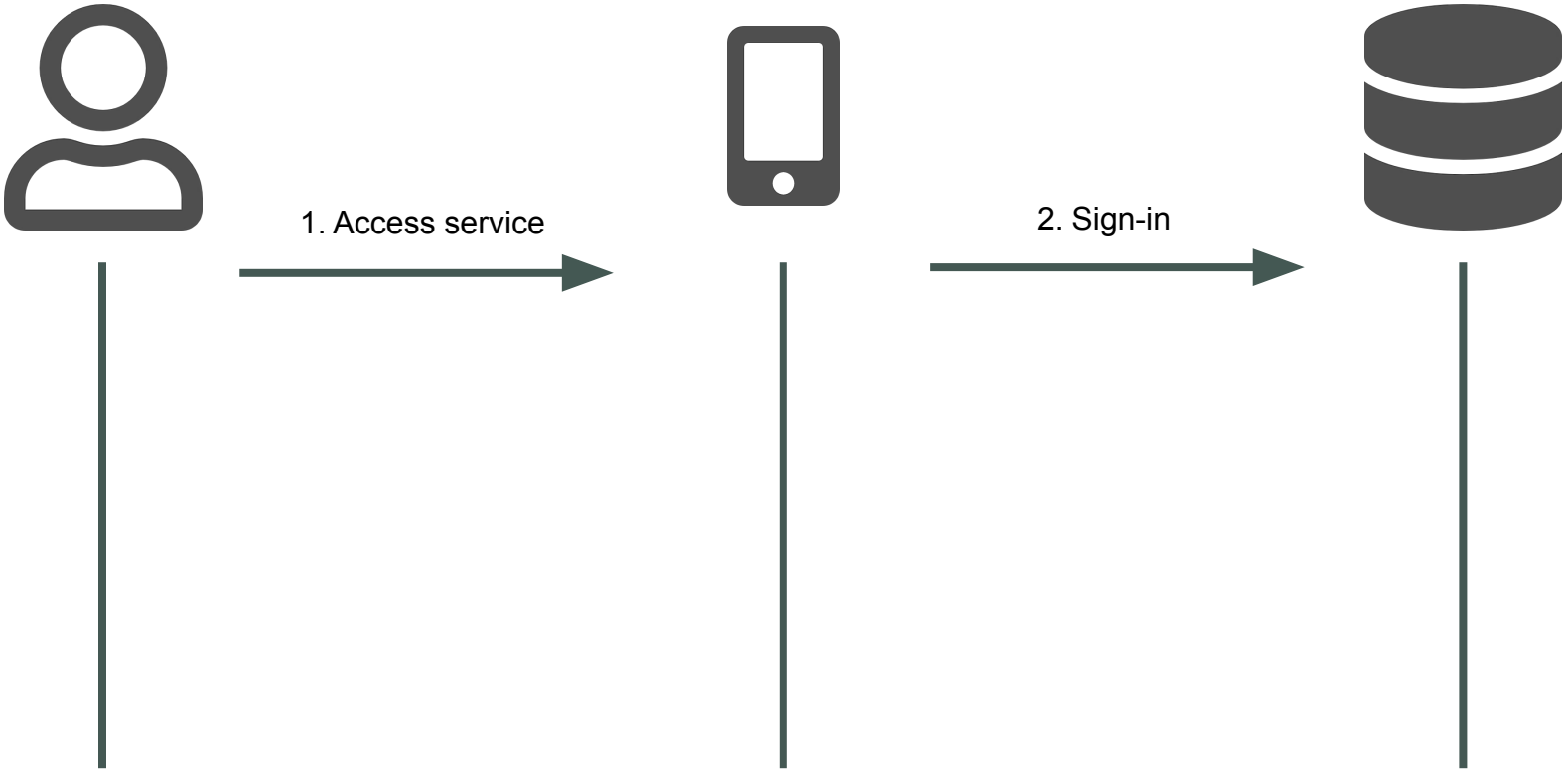
Passkeys - Registering a new passkey



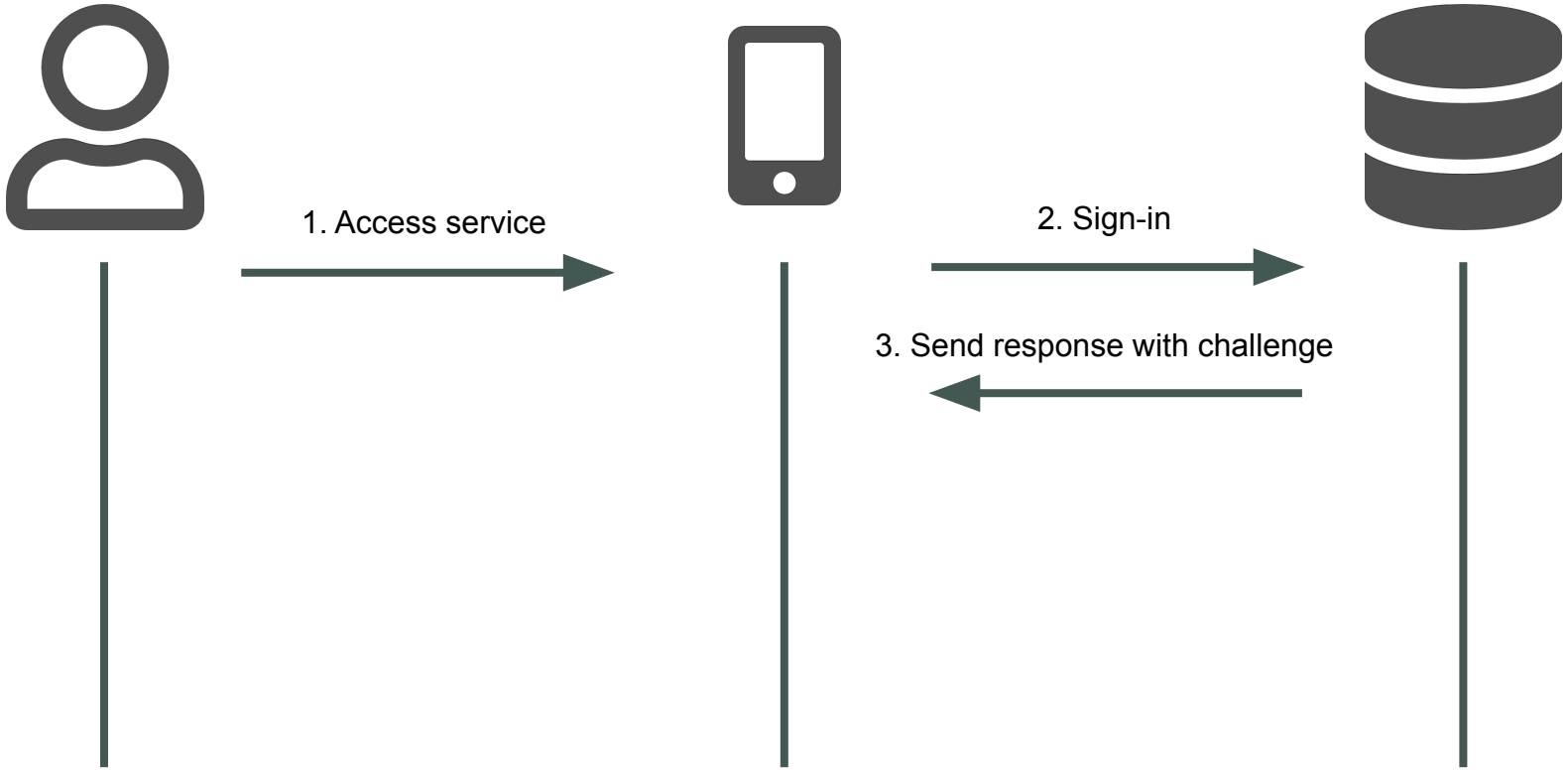
Passkeys - Registering a new passkey



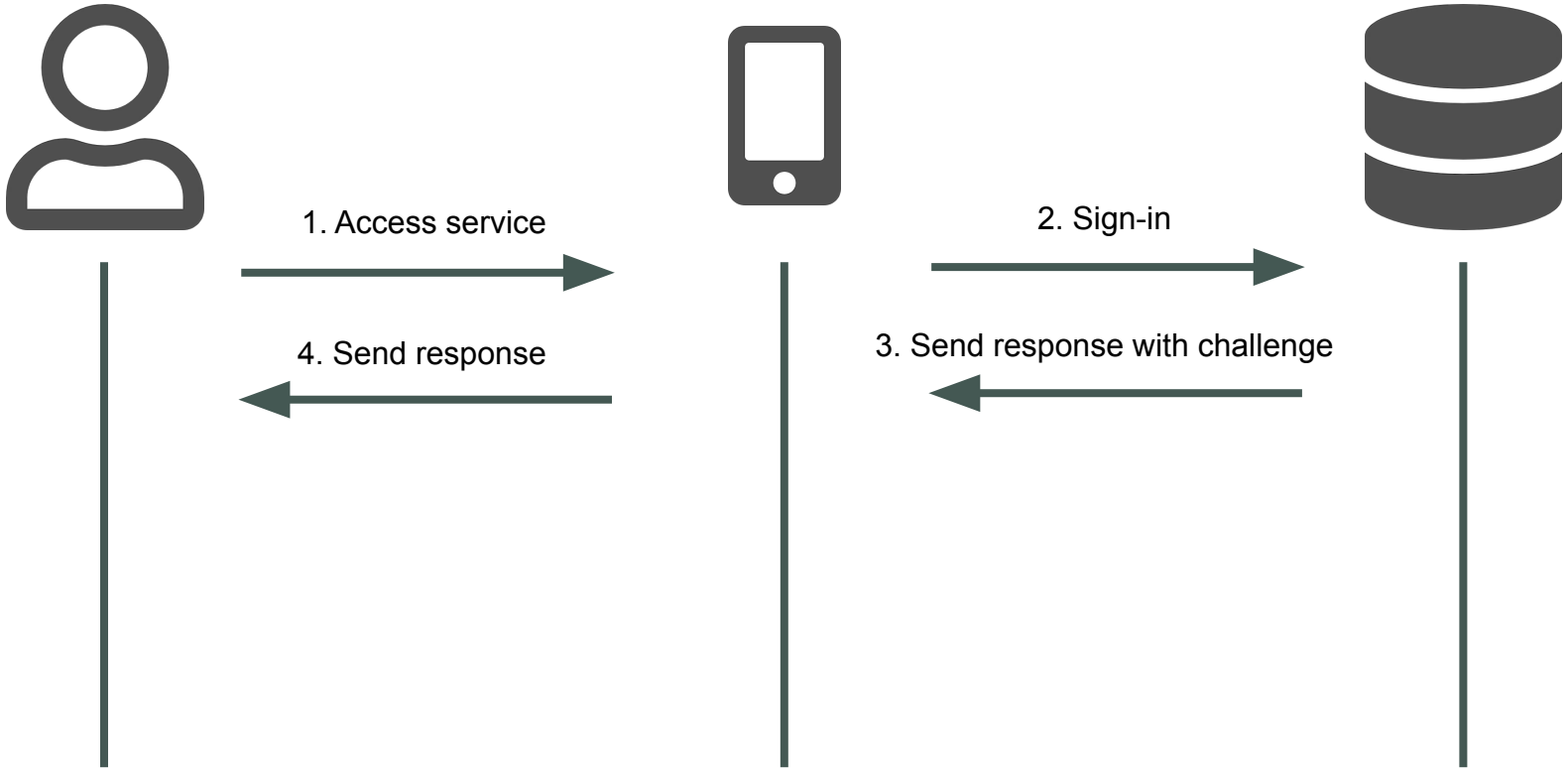
Passkeys - Registering a new passkey



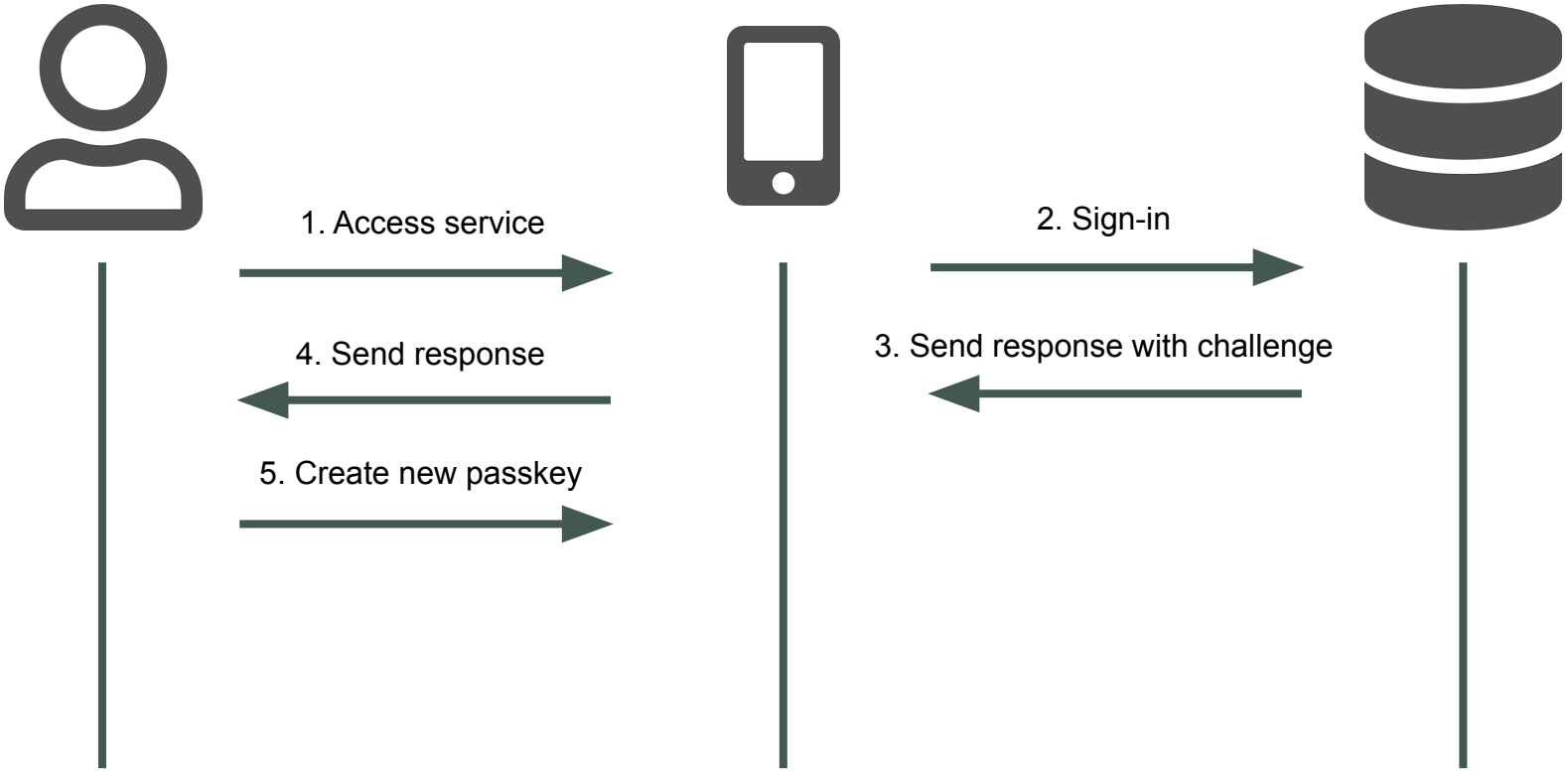
Passkeys - Registering a new passkey



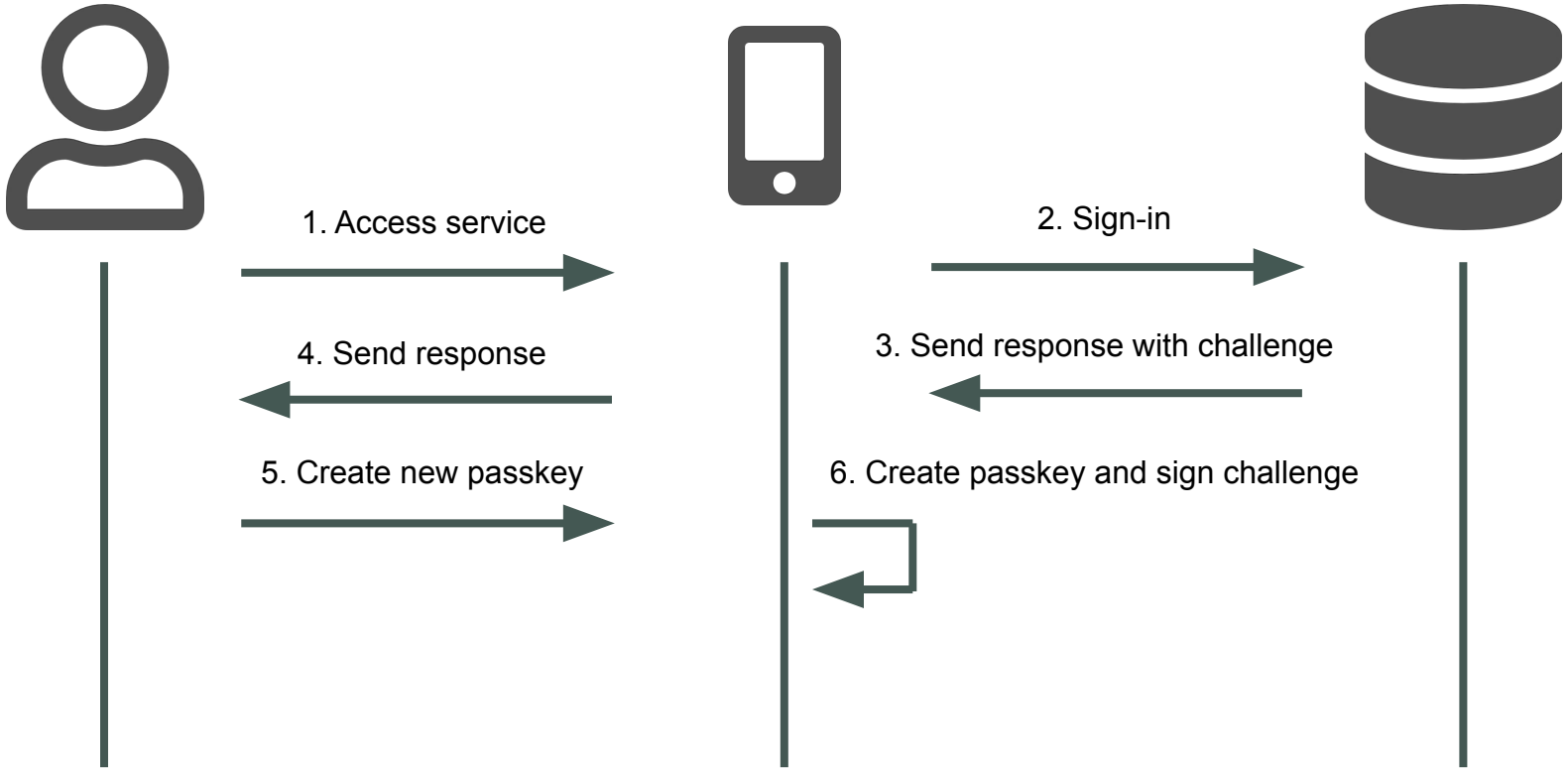
Passkeys - Registering a new passkey



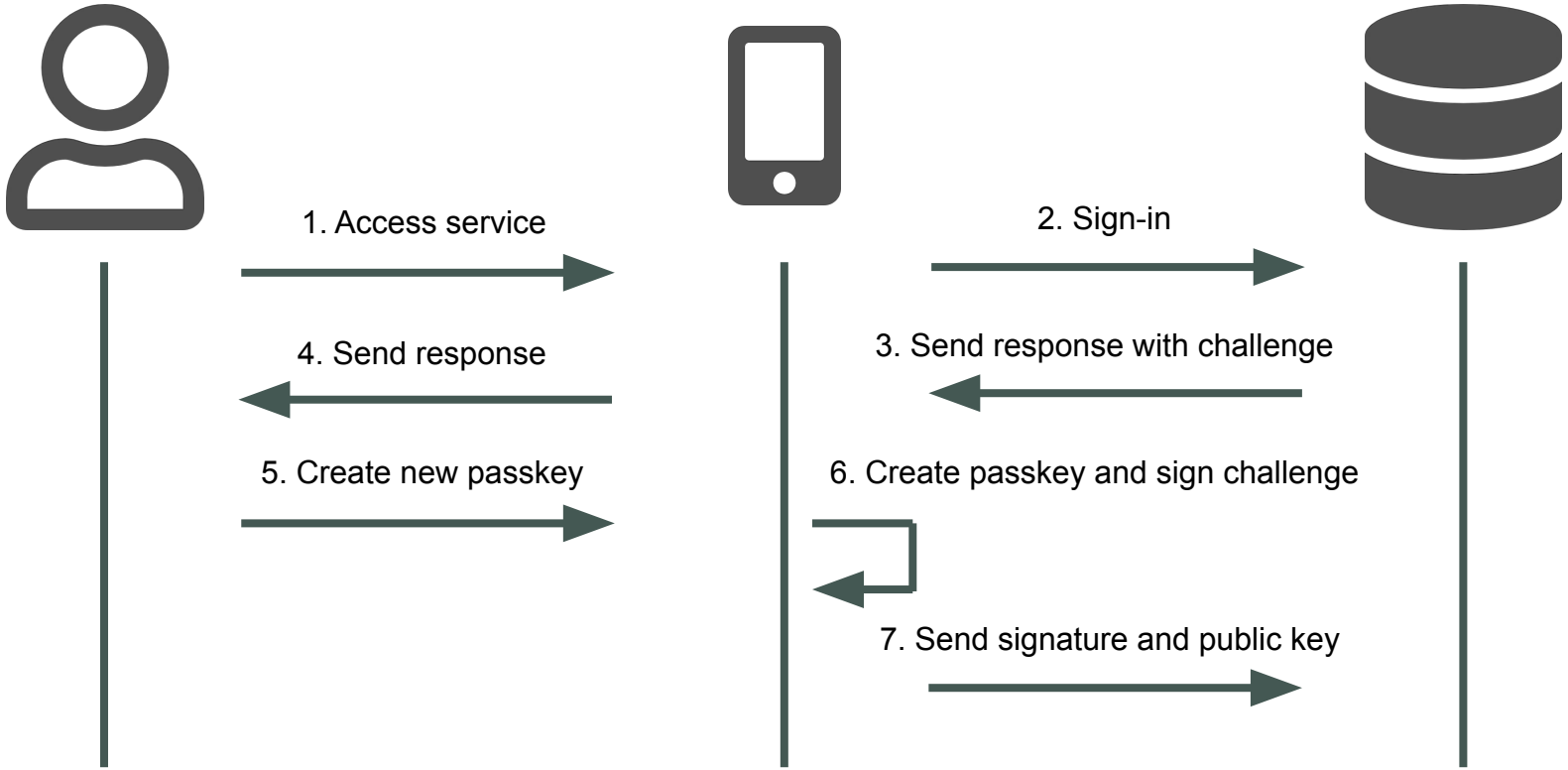
Passkeys - Registering a new passkey



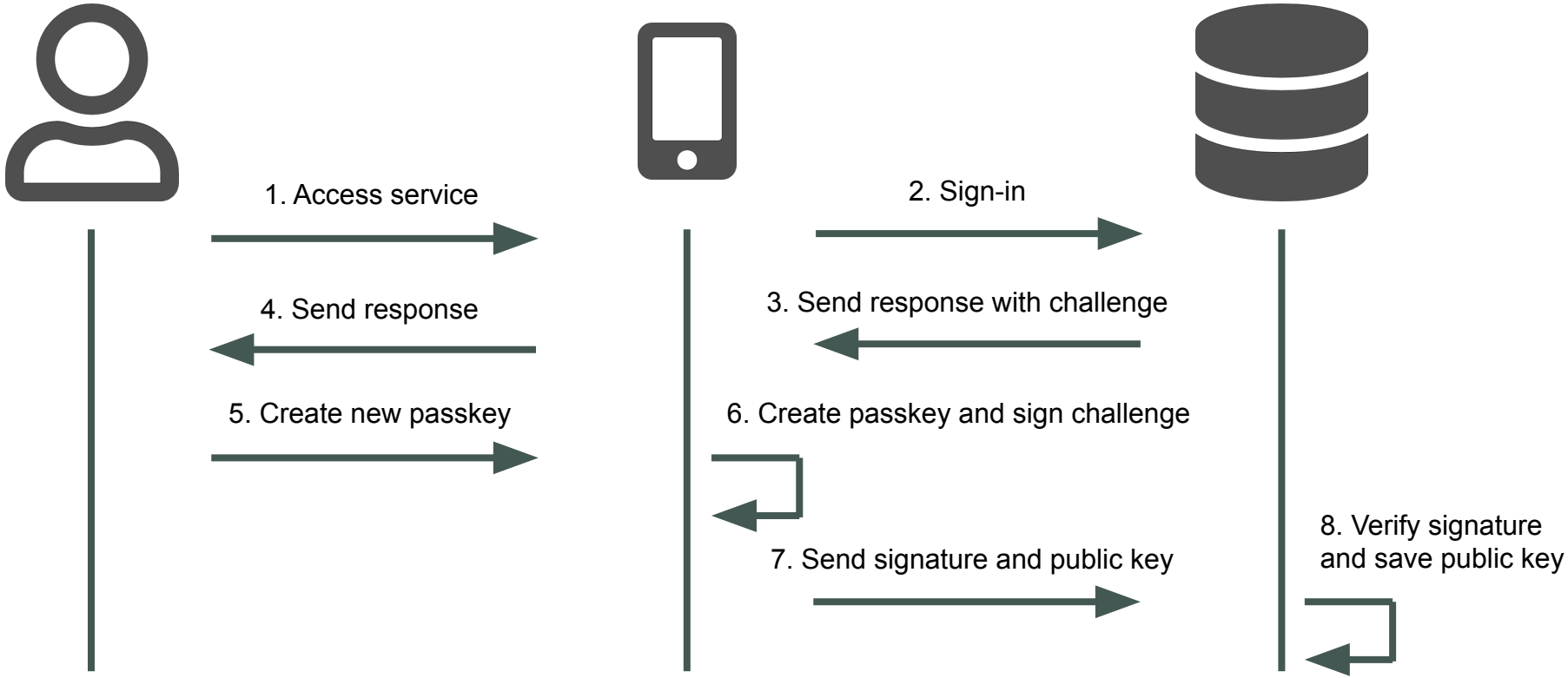
Passkeys - Registering a new passkey



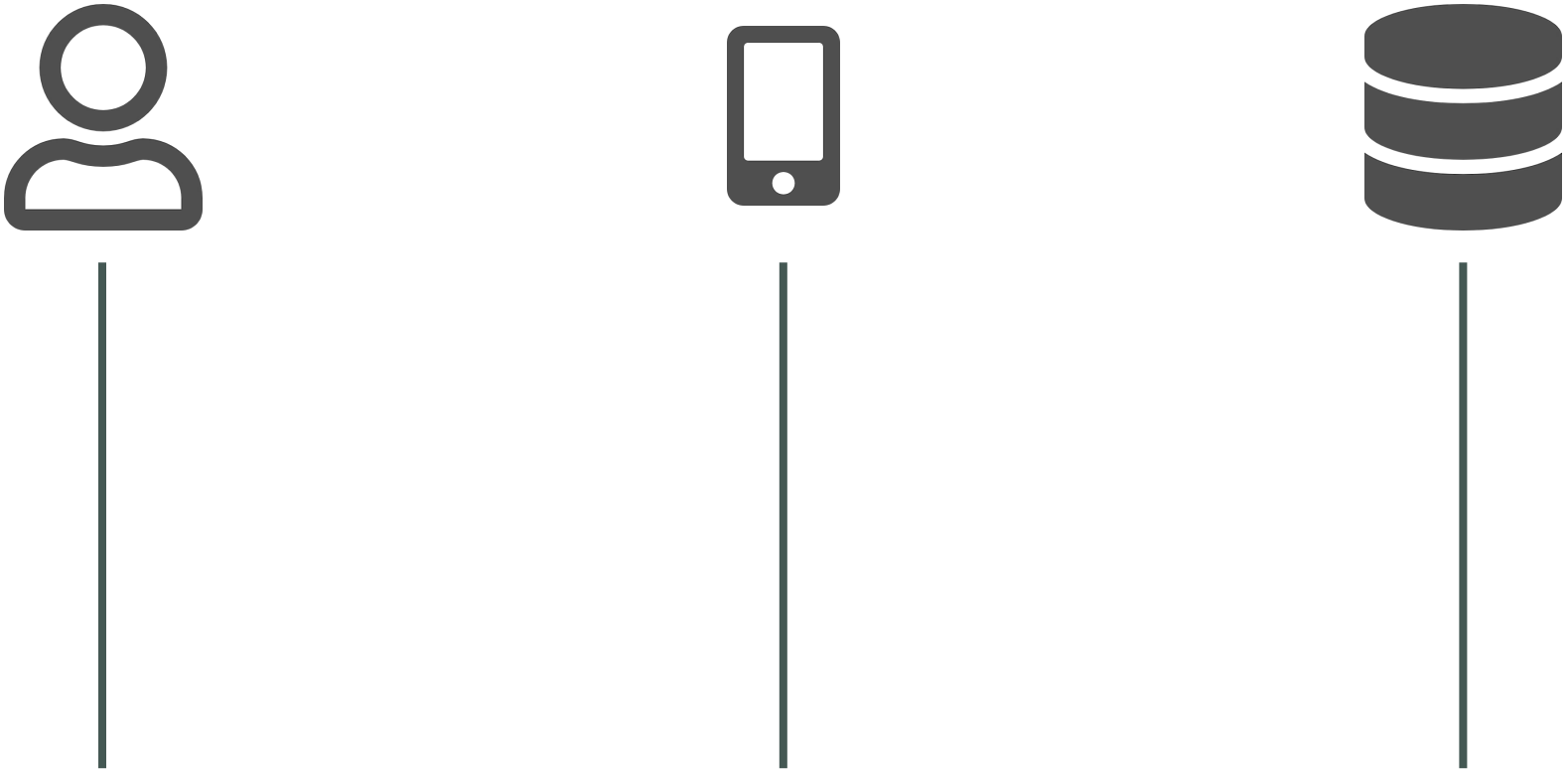
Passkeys - Registering a new passkey



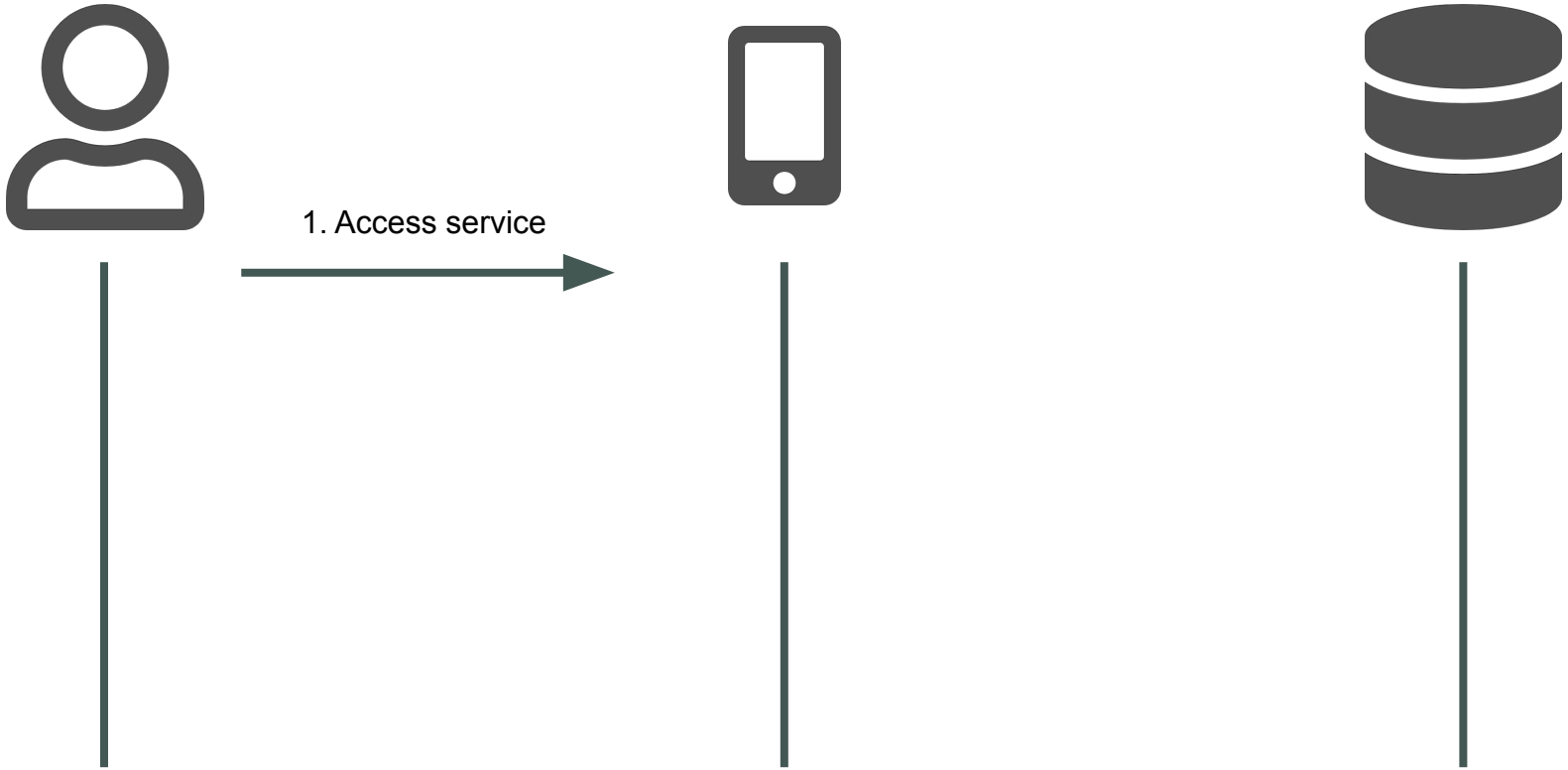
Passkeys - Registering a new passkey



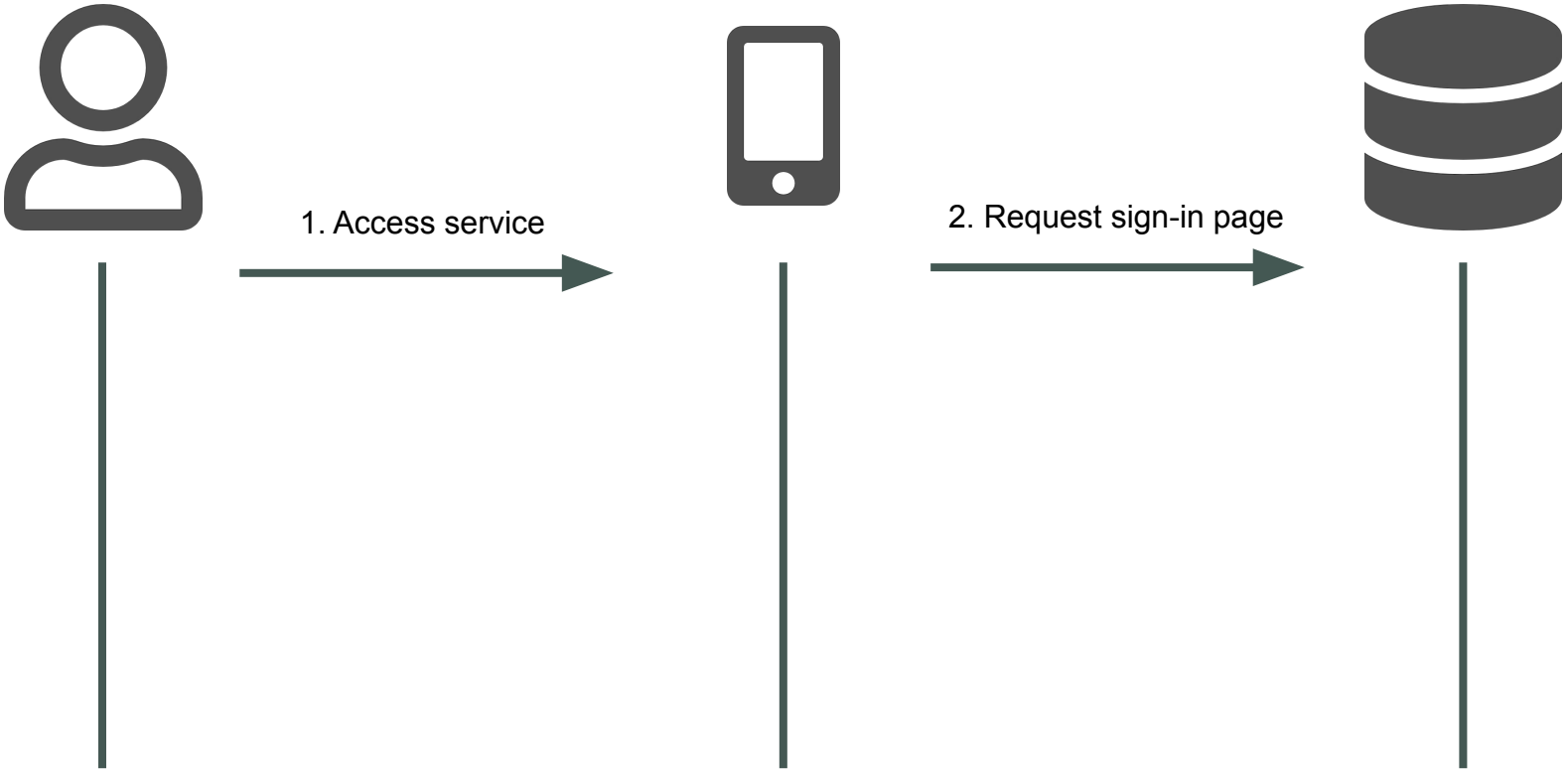
Passkeys - Sign in with a passkey



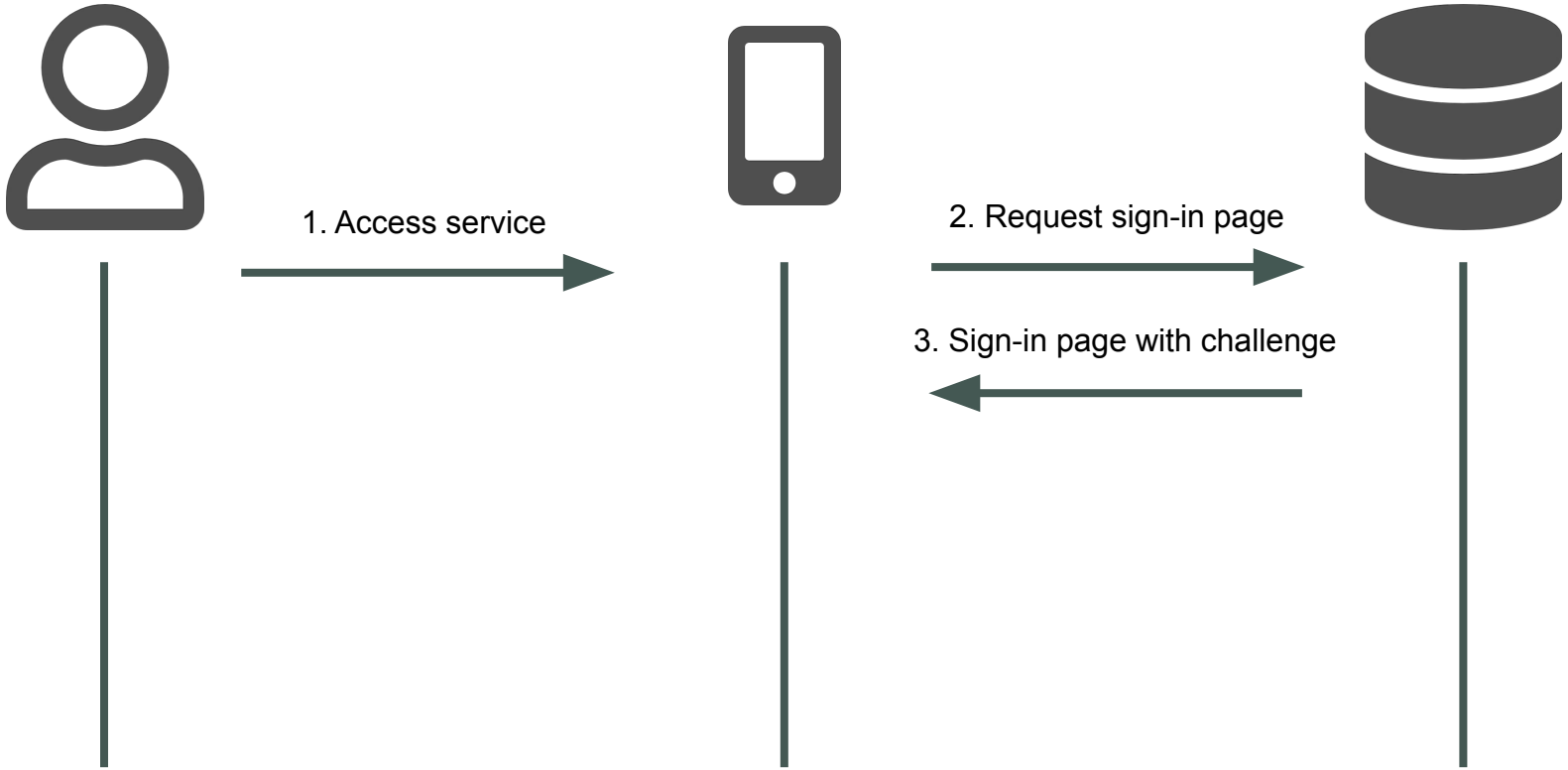
Passkeys - Sign in with a passkey



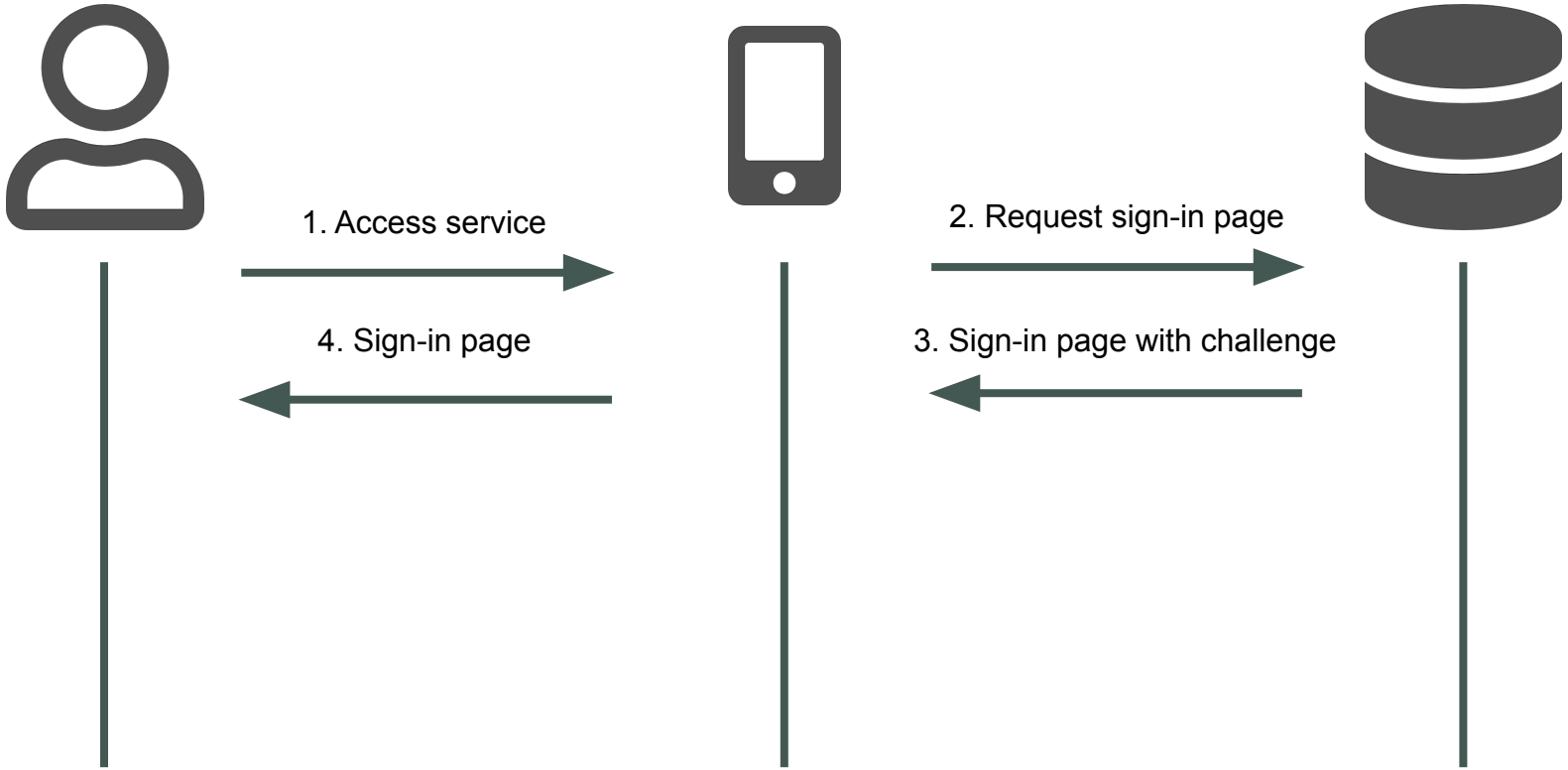
Passkeys - Sign in with a passkey



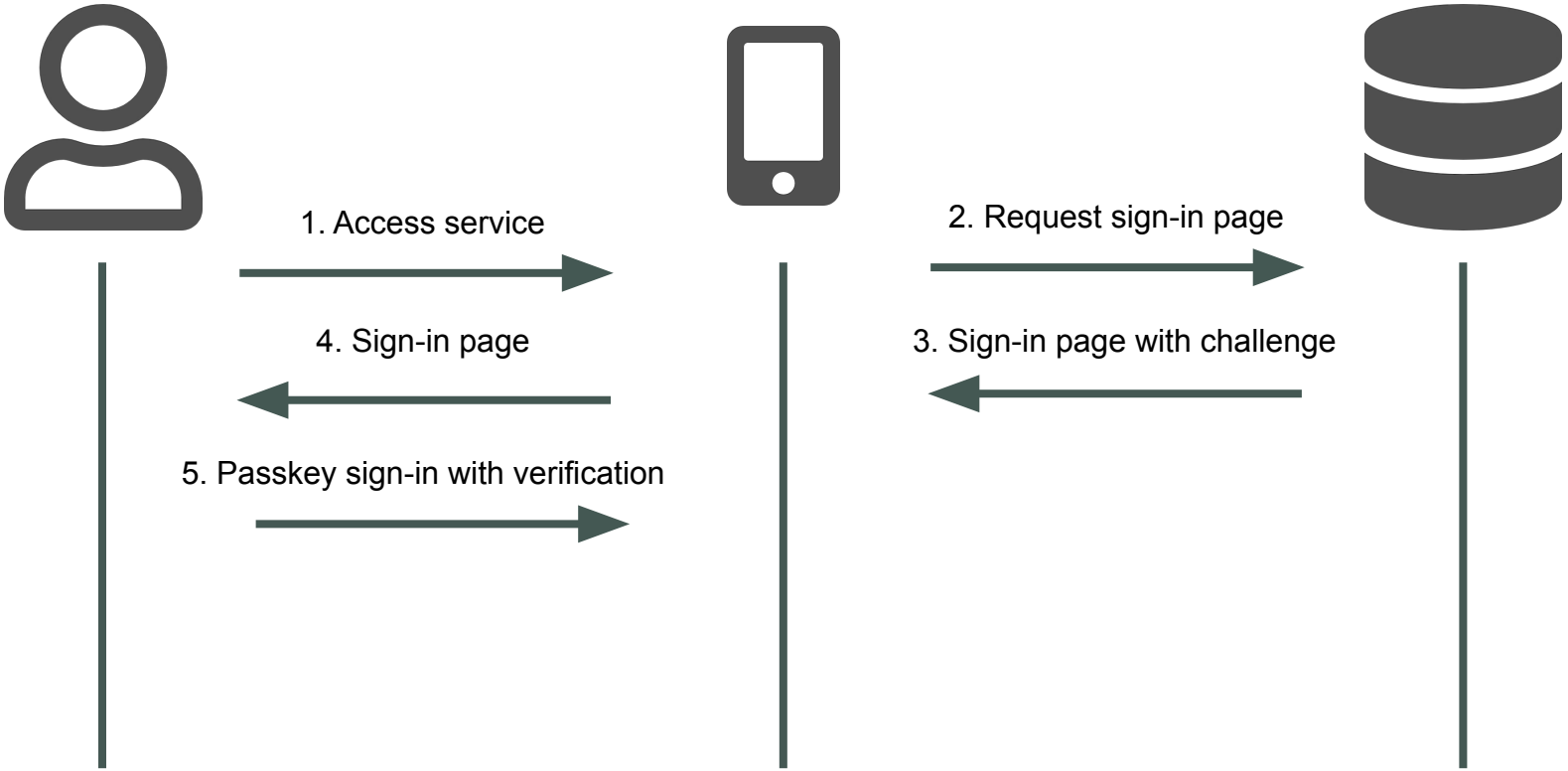
Passkeys - Sign in with a passkey



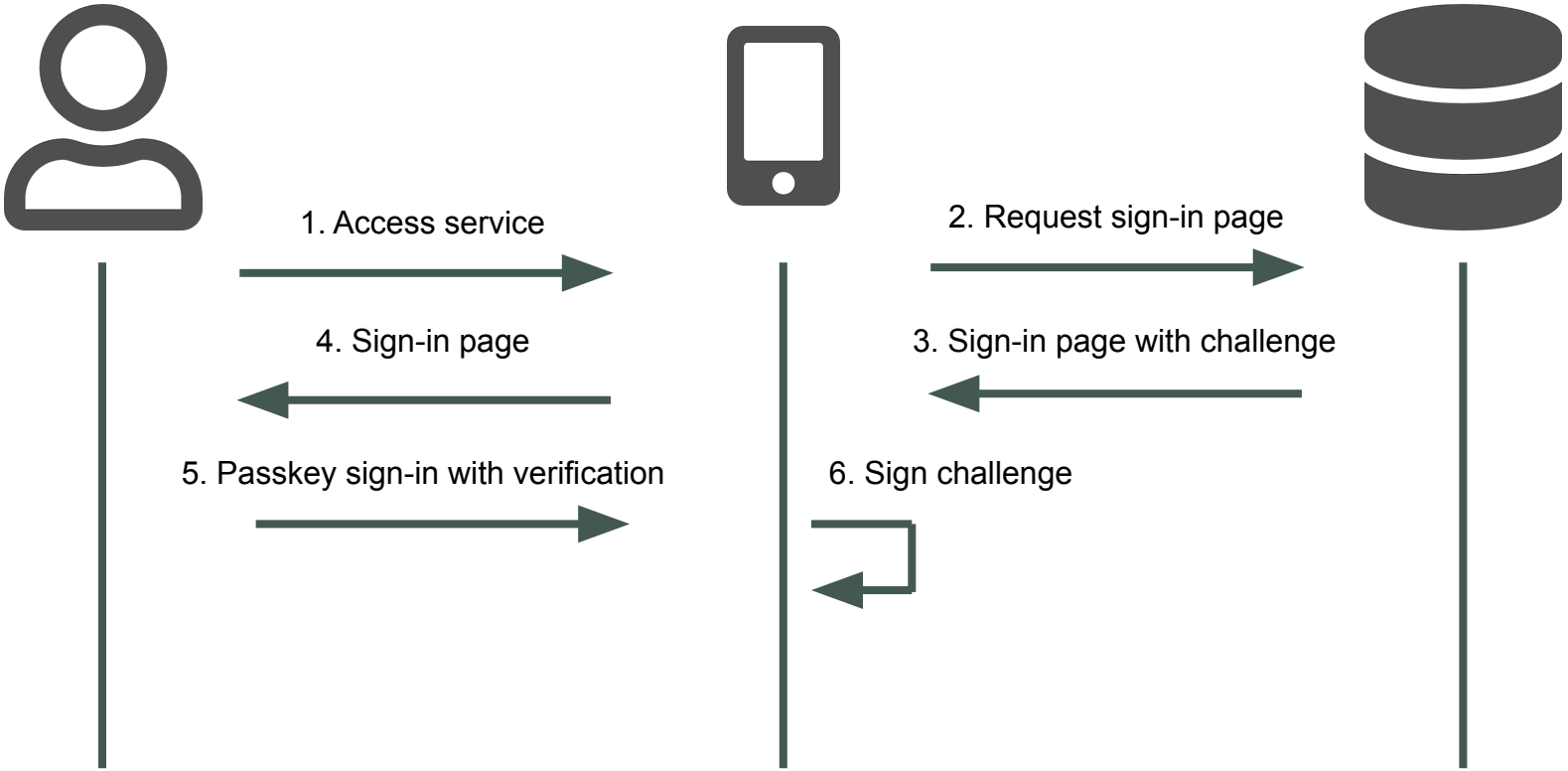
Passkeys - Sign in with a passkey



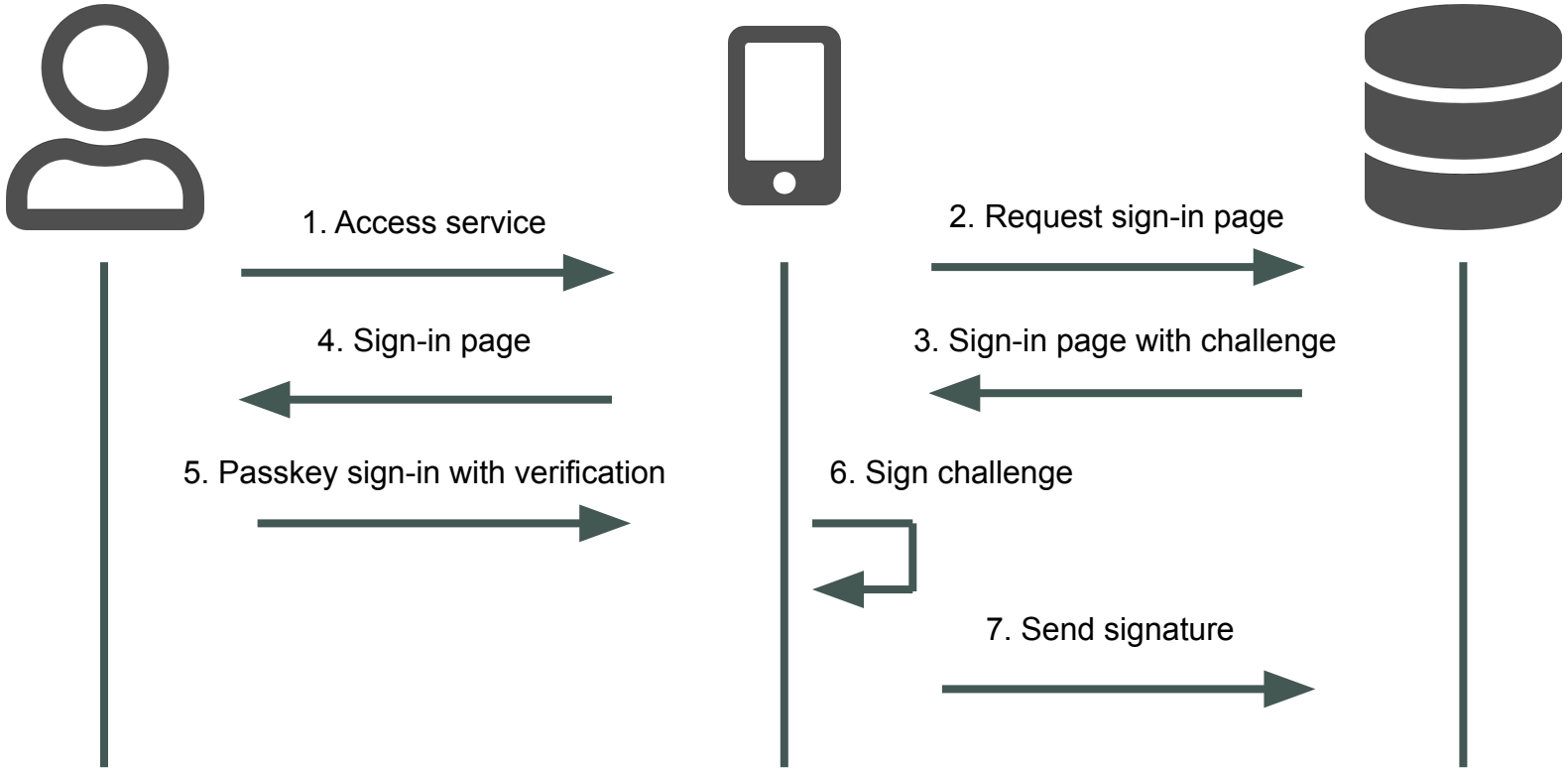
Passkeys - Sign in with a passkey



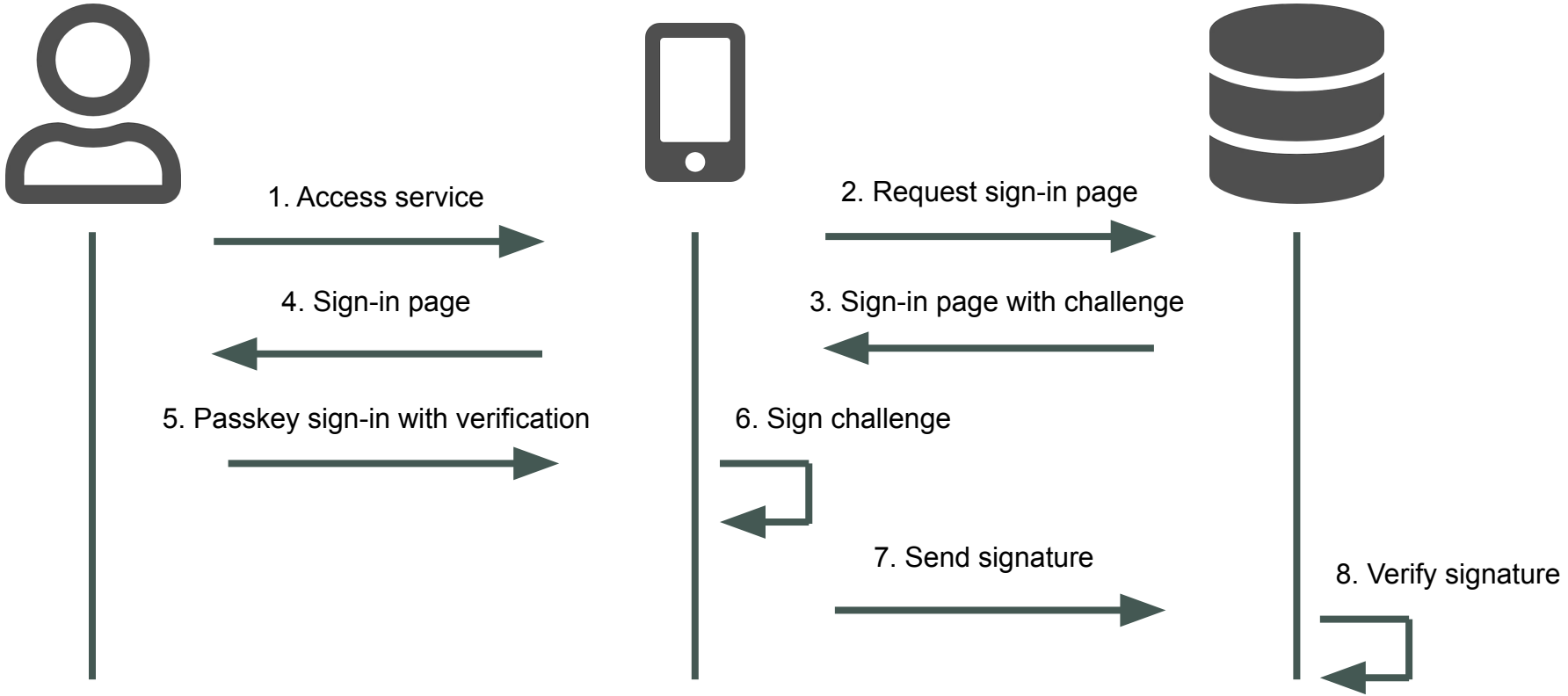
Passkeys - Sign in with a passkey



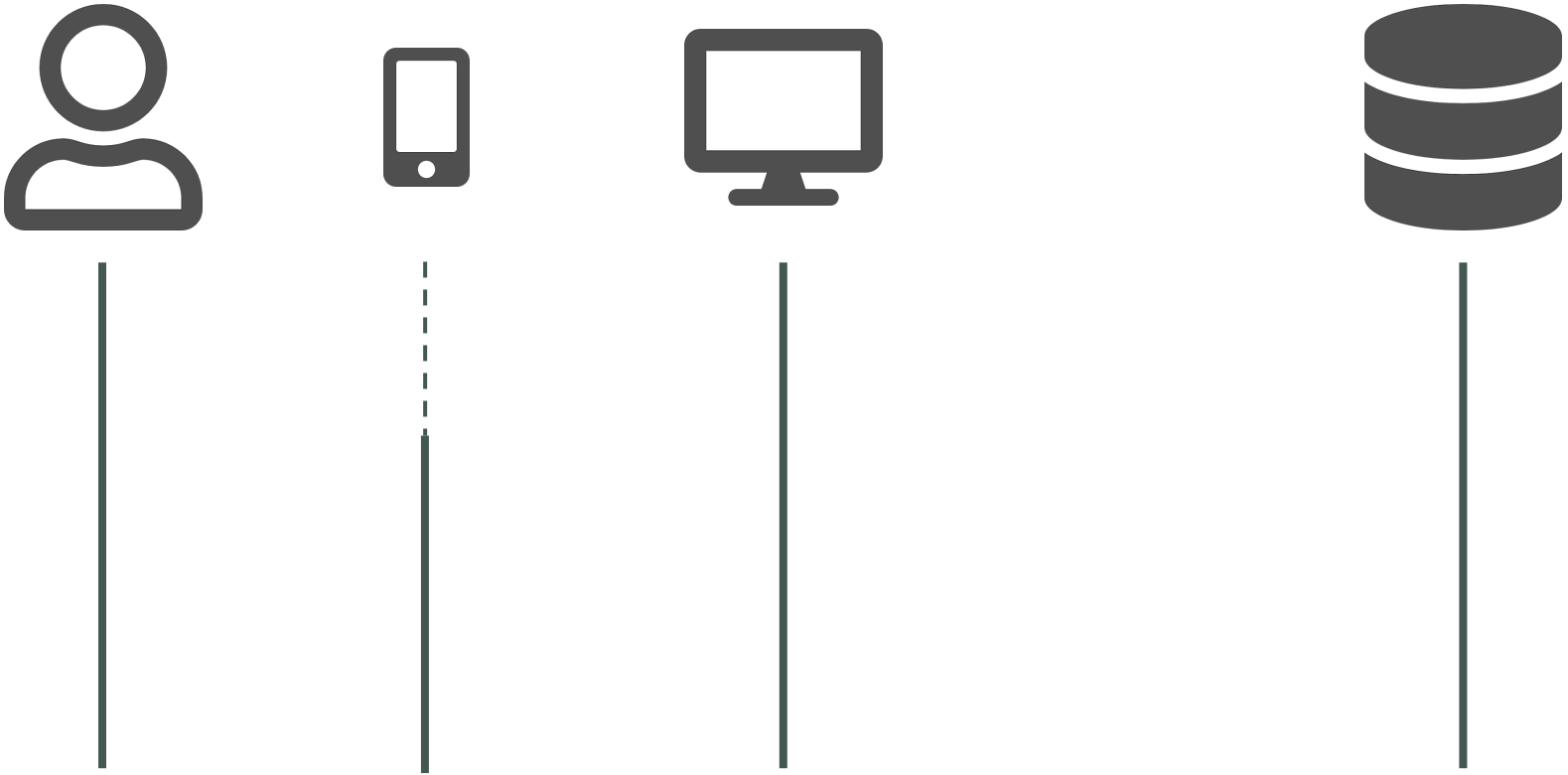
Passkeys - Sign in with a passkey



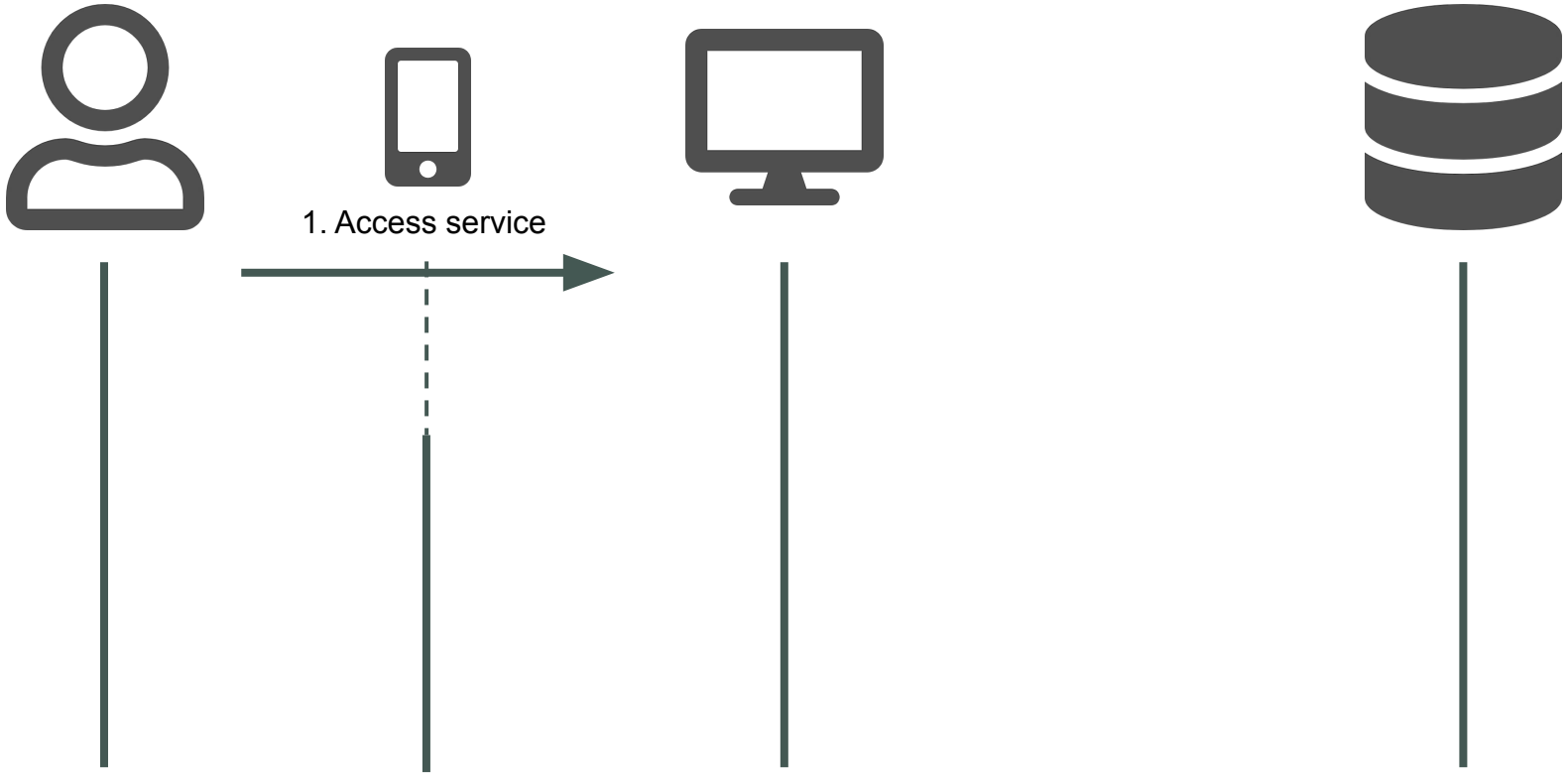
Passkeys - Sign in with a passkey



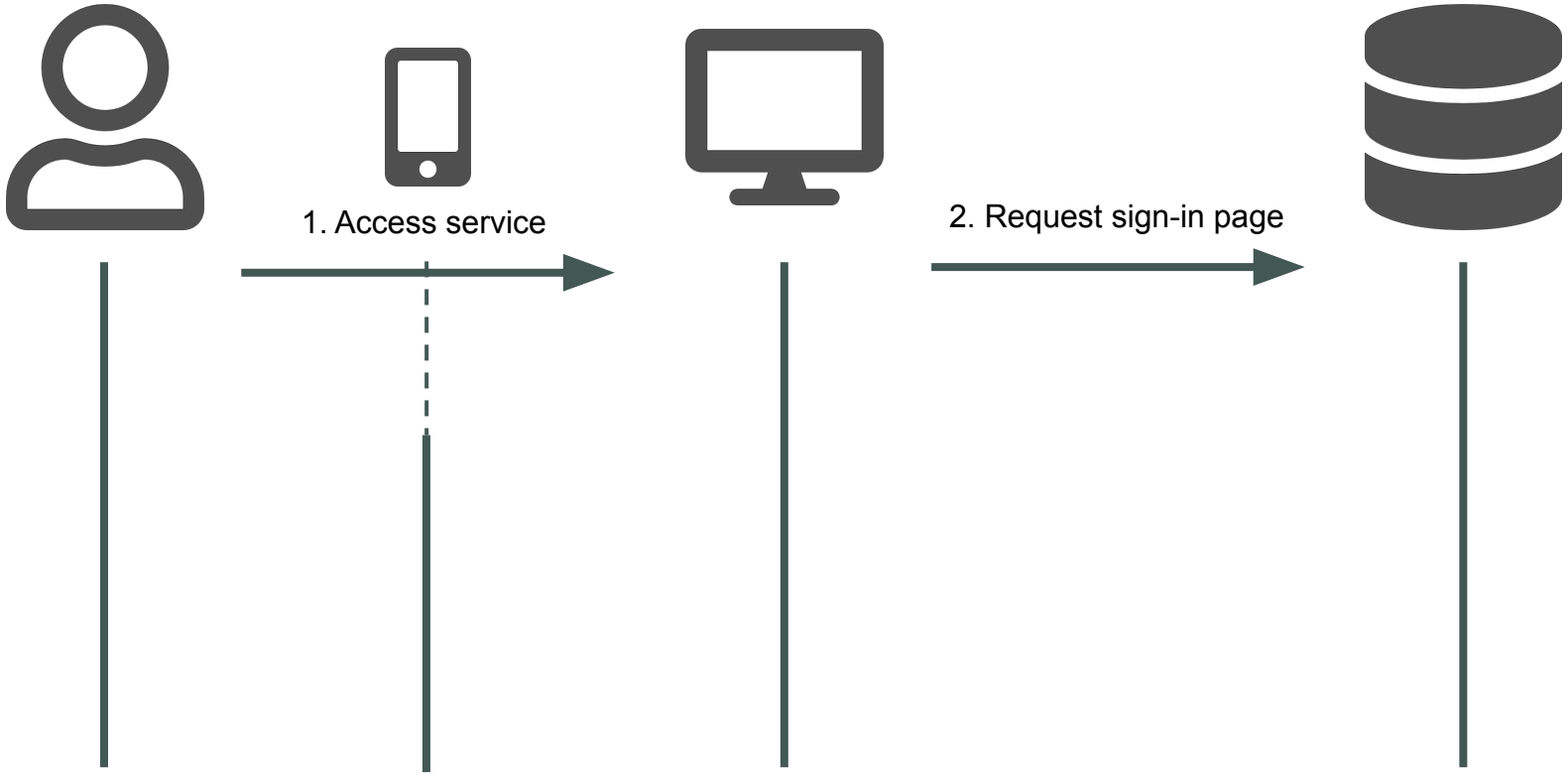
Passkeys - Sign in with a passkey on other device



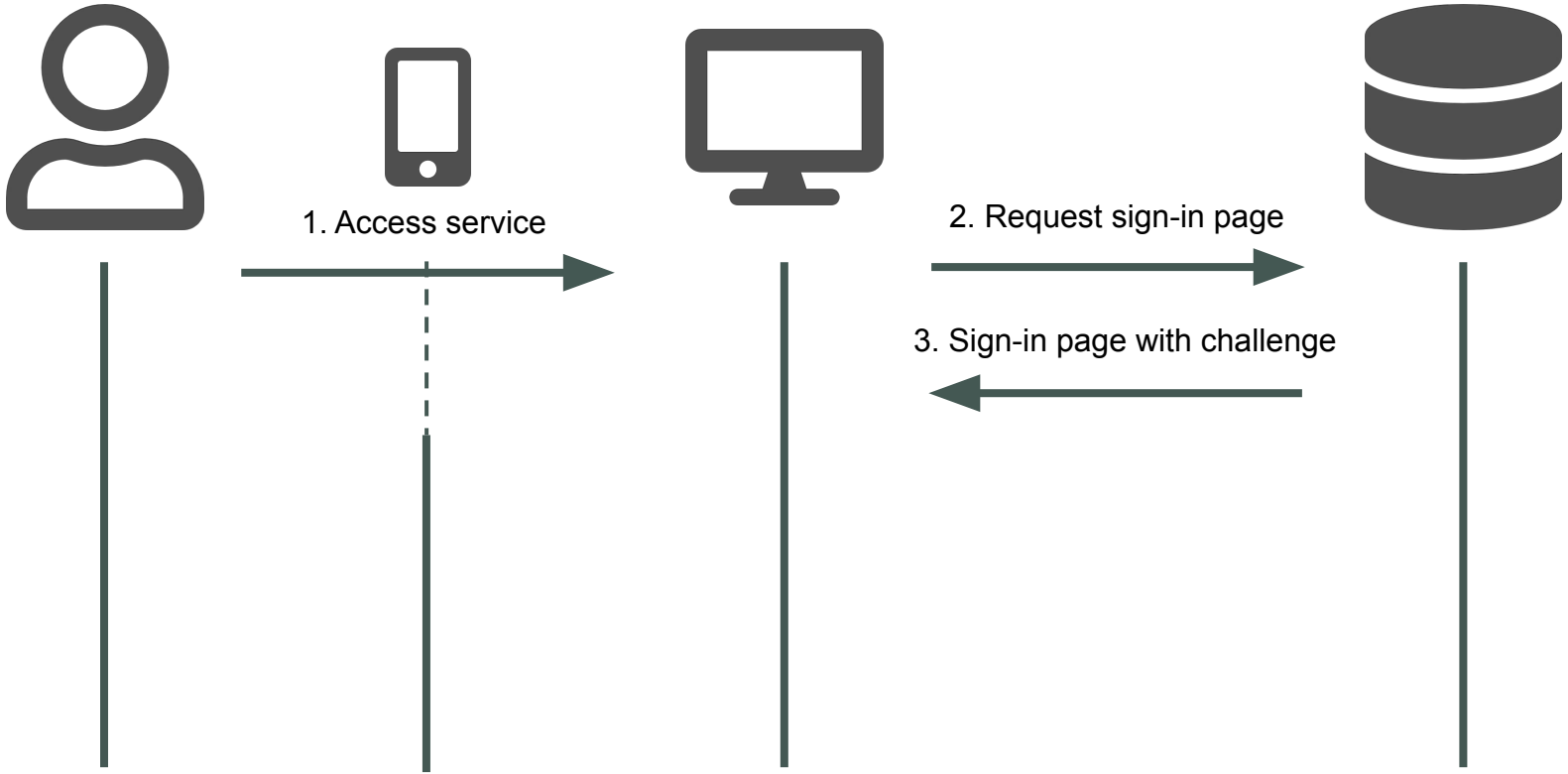
Passkeys - Sign in with a passkey on other device



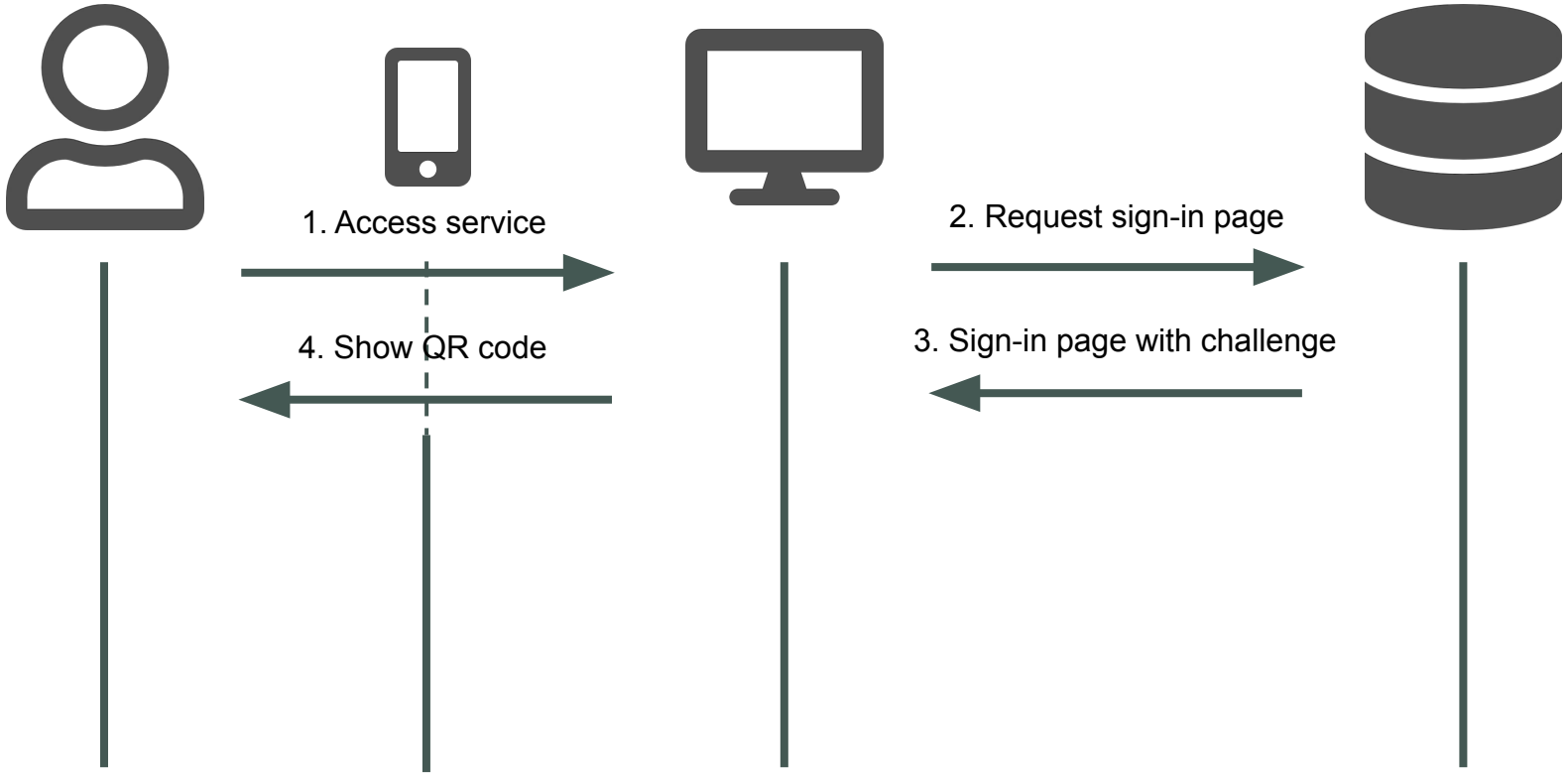
Passkeys - Sign in with a passkey on other device



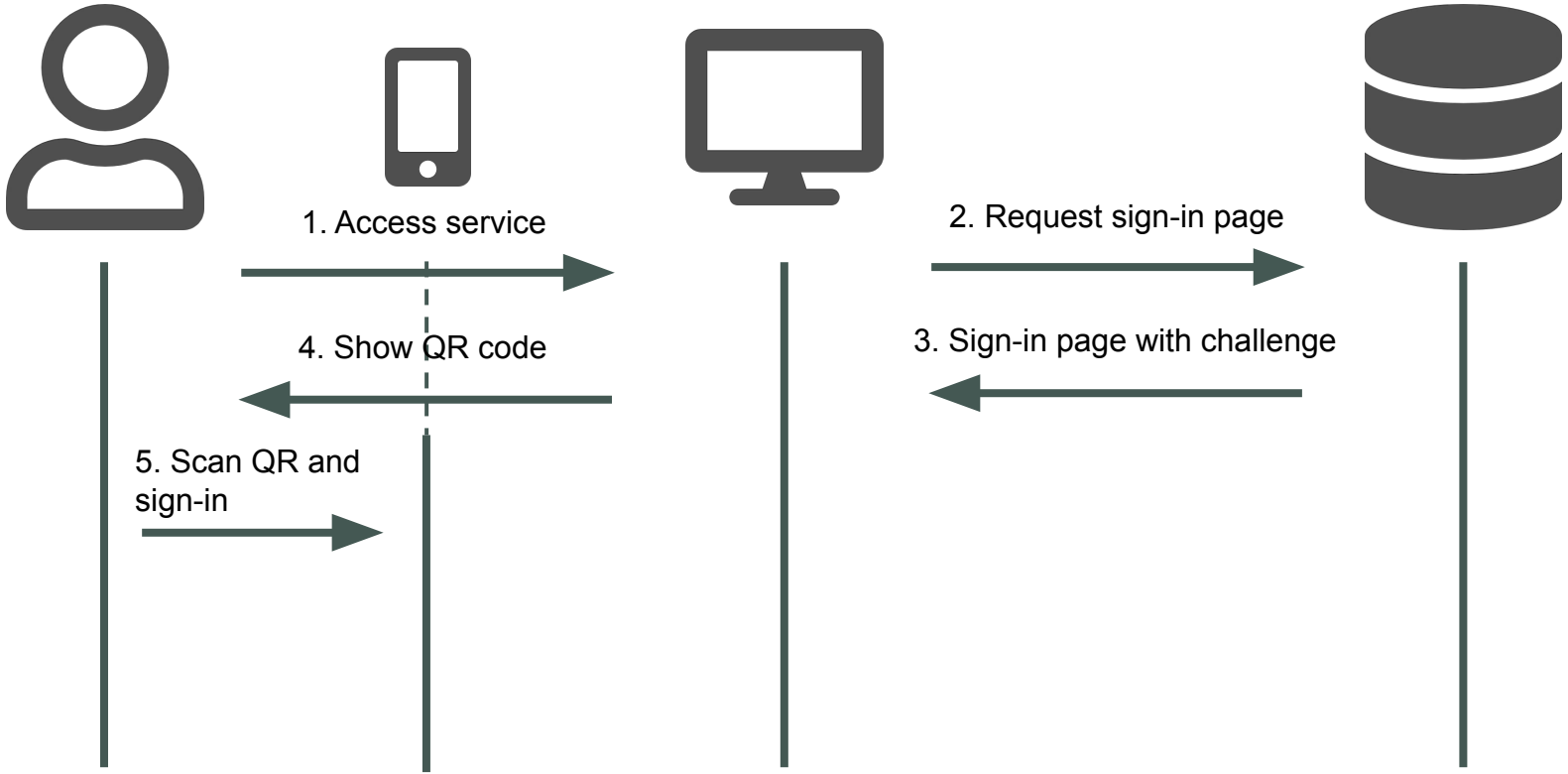
Passkeys - Sign in with a passkey on other device



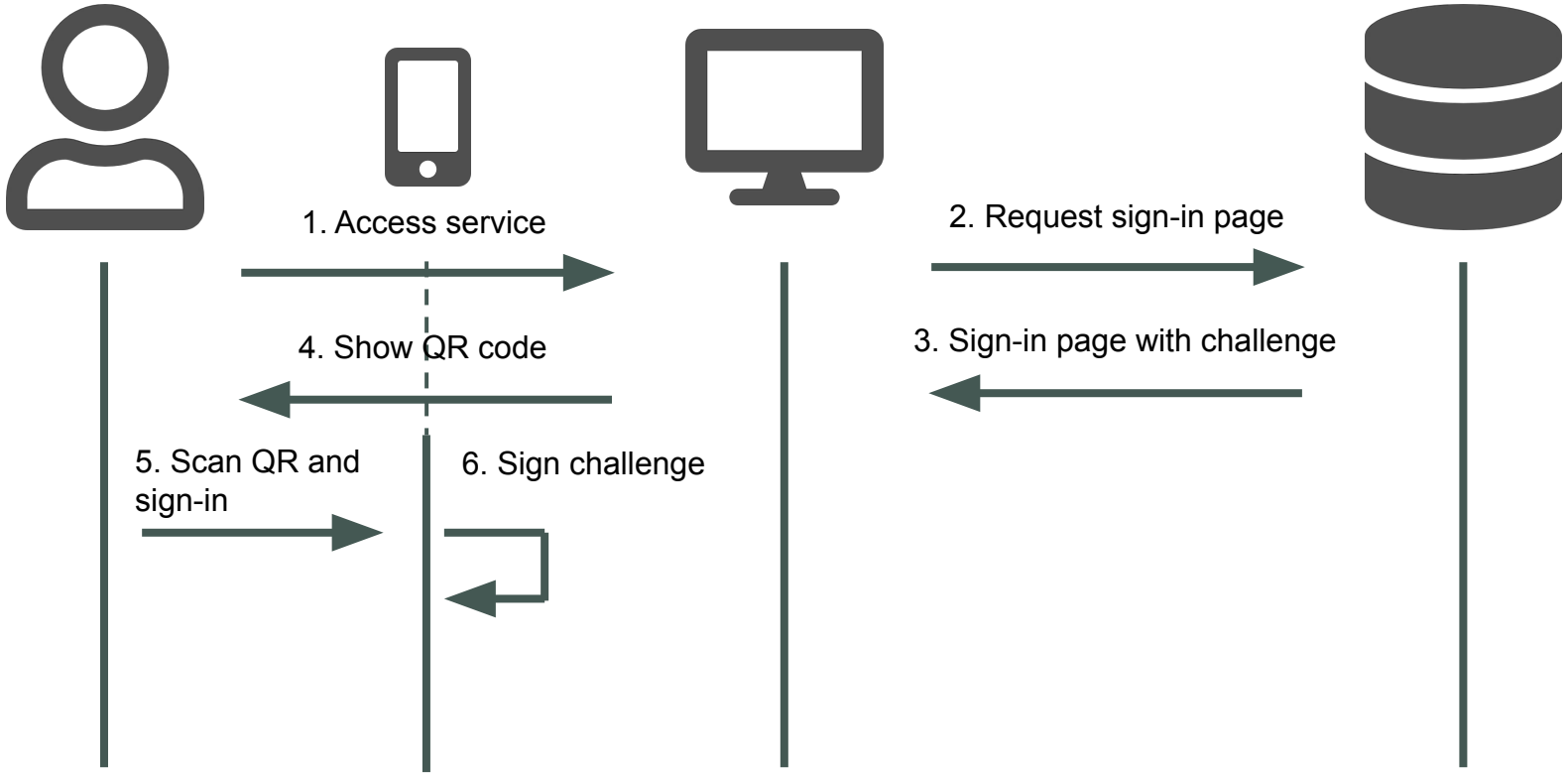
Passkeys - Sign in with a passkey on other device



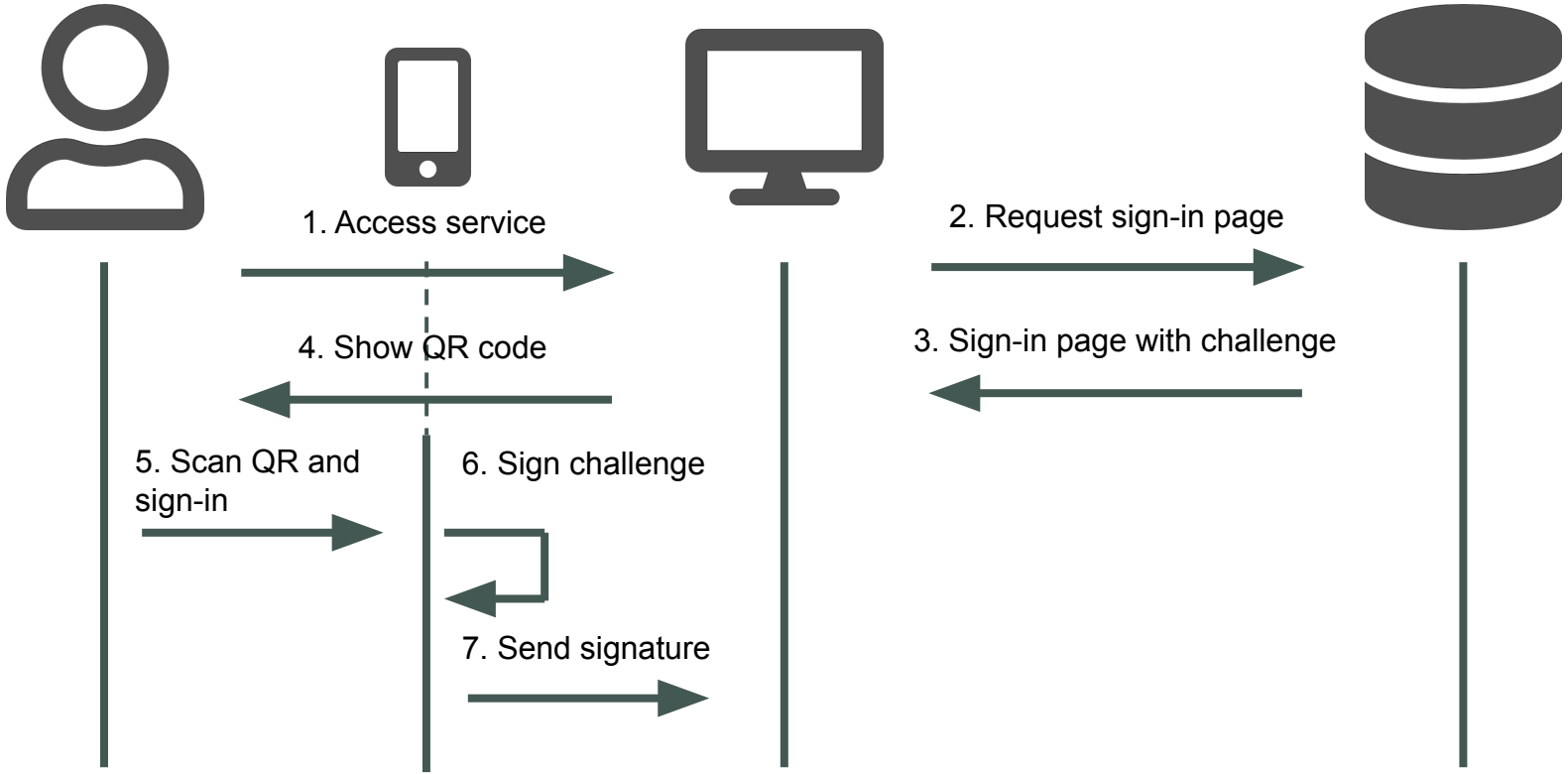
Passkeys - Sign in with a passkey on other device



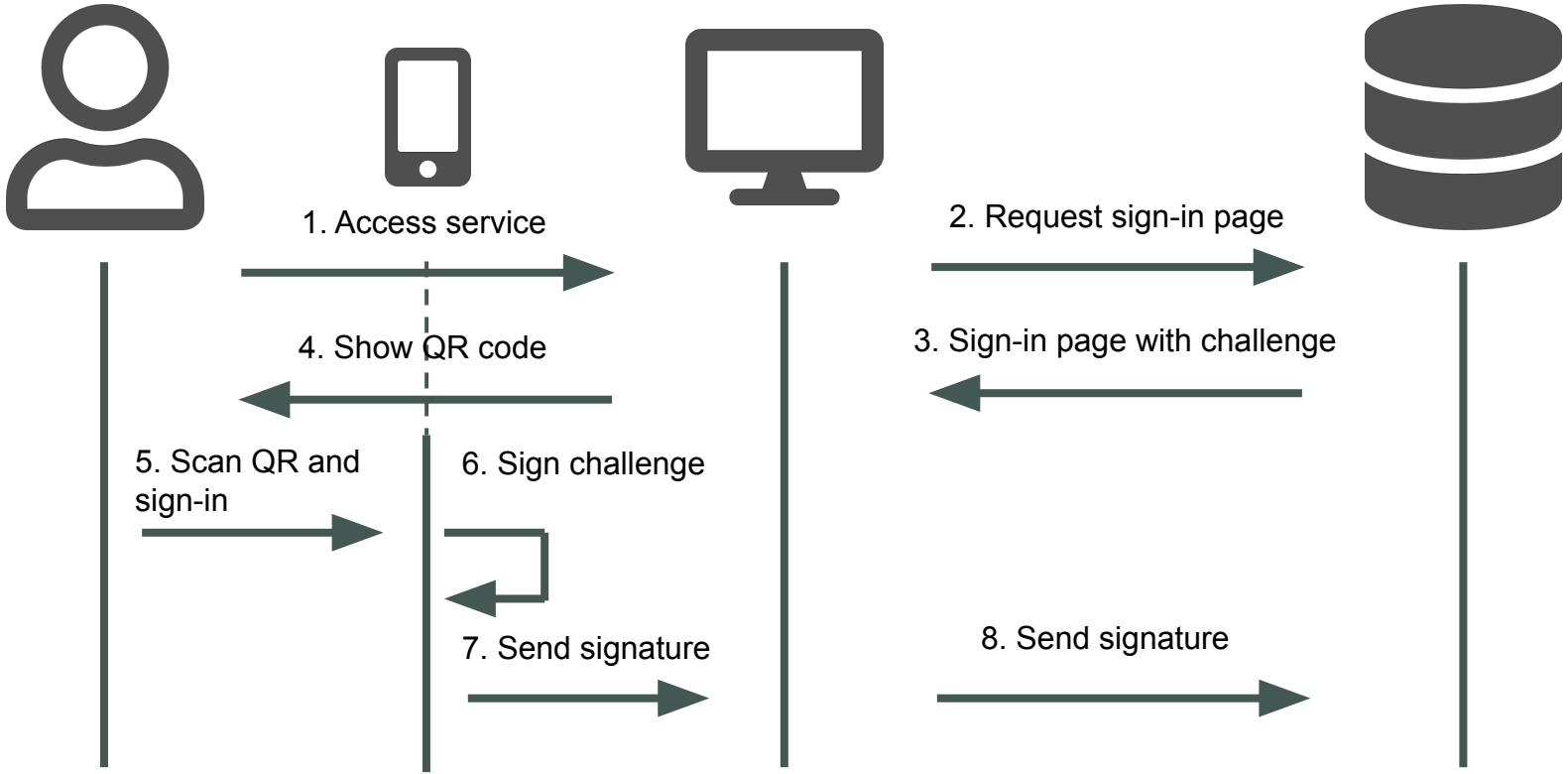
Passkeys - Sign in with a passkey on other device



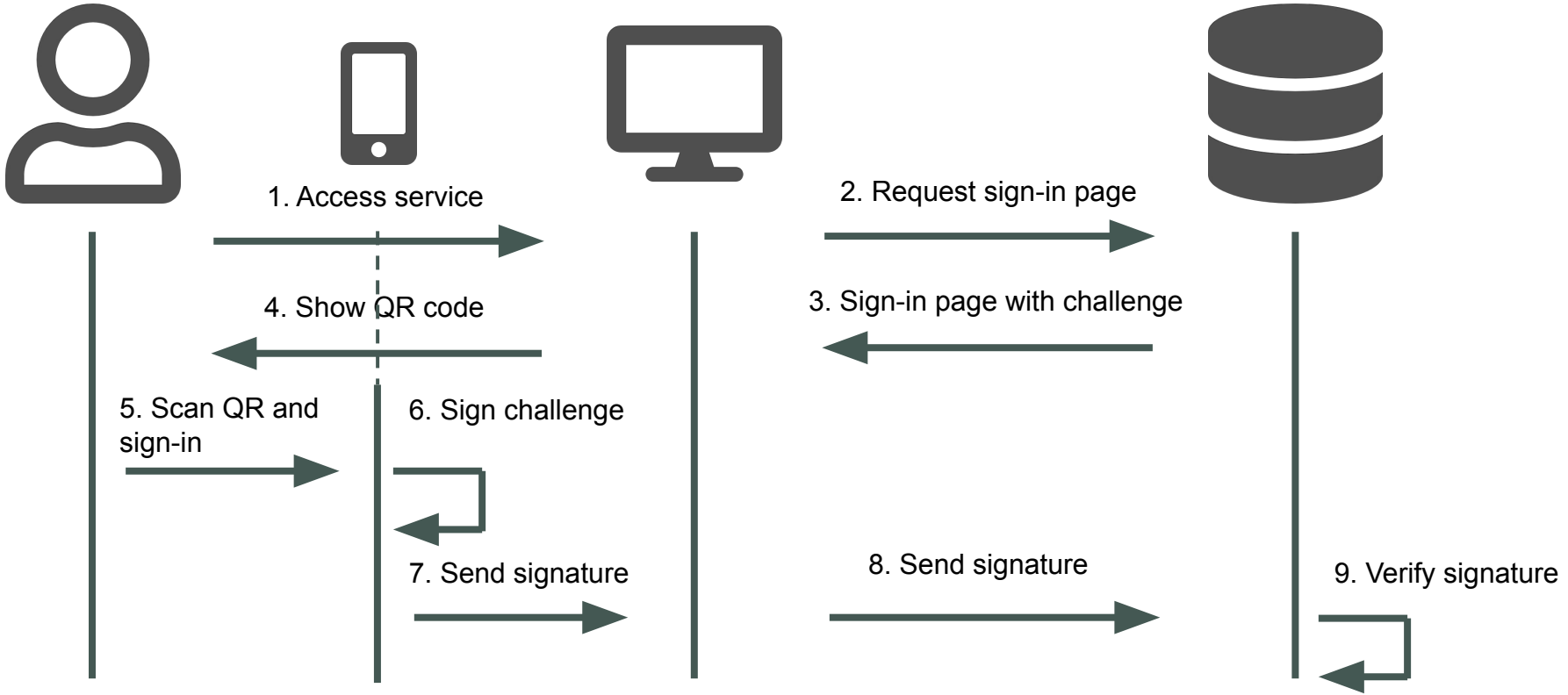
Passkeys - Sign in with a passkey on other device



Passkeys - Sign in with a passkey on other device



Passkeys - Sign in with a passkey on other device



Passkeys - Situation on the market

- Many commercial vendors **support** passkeys
- SimpleSAMLphp **supports** passkeys
- Shibboleth does **not support** passkeys (in progress)
- Keycloak **supports** passkeys
- PrivacyIDEA does **not fully support** passkeys yet

Passkeys - Our approach

- Aim to build it on top of our MFA solution
- Need to replace some underlying components first
- Need to solve the UX part before implementation

Passkeys - How to do the transition?

- Change our authentication gateway
- Need to support both approaches
- Passkeys through a button or autofill
- Need to educate users

Perun

Which multi-factor authentication solution is right for me?

We know that it can be difficult to understand all the options for multi-factor authentication. It can be challenging to decide which method, device or software to use.

However, this guide can help you with that. Come and give it a try!

Start

Passkeys - How to do the recovery and onboarding?

- What if users lost their passkey?
- How to onboard new users?
- Password as a backup?

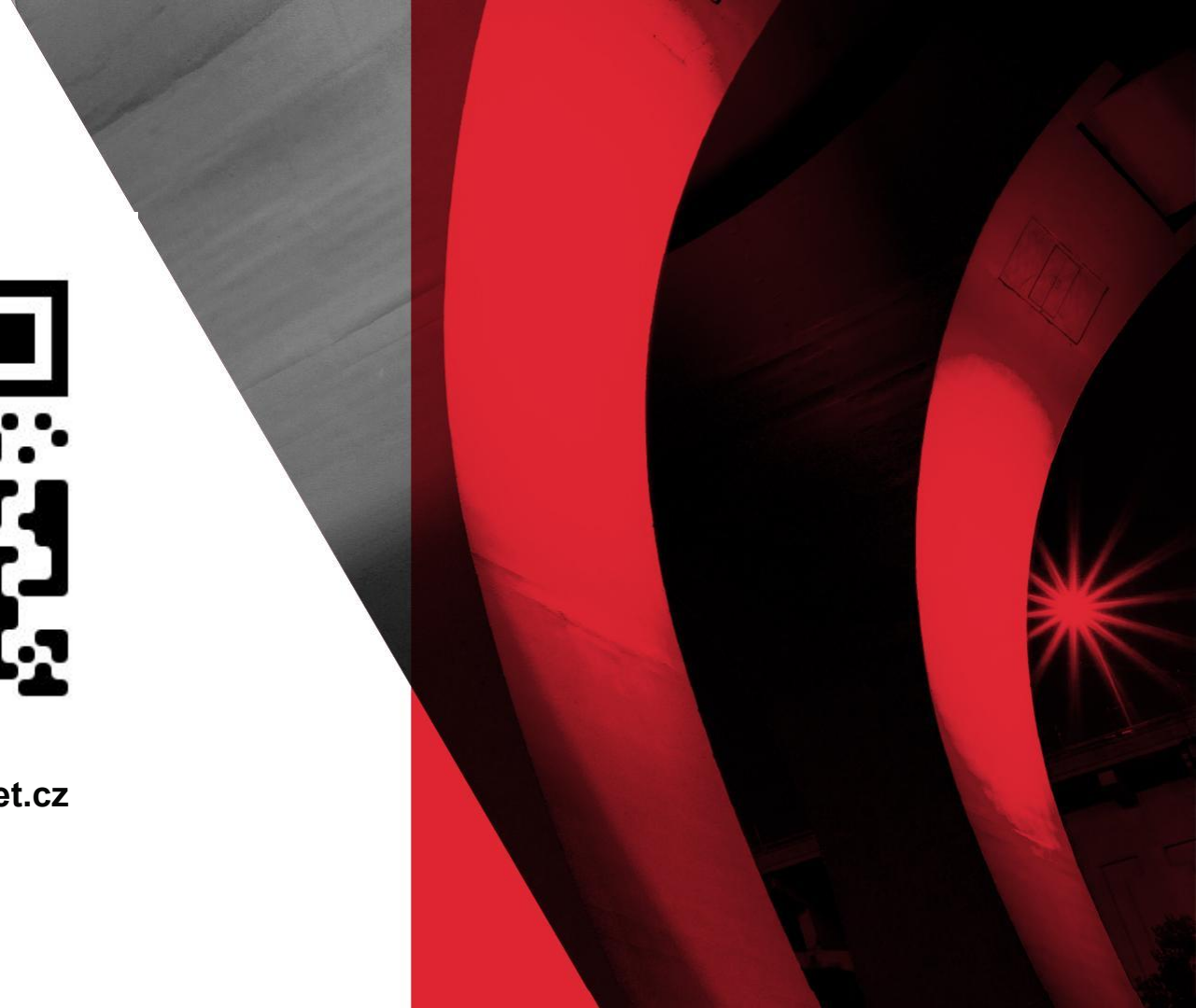
Passkeys - What if passkeys are not enough?

- What if some community requires another factor?
- We need to know which passkey was used as a first factor
- Doable at one IdP
- Difficult when interconnecting separate AAIs

Passkeys - What if an IdP does not support passkeys?

- IdP does not tell us what factor was used
- Need to handled on the AAI side
- Need to navigate users seamlessly

If not passwordless, at least use passwords less



peter.balcirak@cesnet.cz