# #8 FIDO2 / WebAuthn

**Segurança Informática e nas Organizações**

**2024/2025**

# Asymmetric Cryptography Recap

Private Key

Public Key

# Asymmetric Cryptography Recap

Private Key
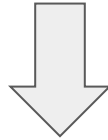
Public Key

- Sign data
- Decipher ciphered data

- Verify signed data
- Cipher data

# Fast IDentity Online 2 (FIDO2)

It is a **passwordless** authentication standard based on **asymmetric cryptography**
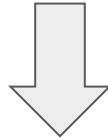
# Fast IDentity Online 2 (FIDO2)

It is a **passwordless** authentication standard based on **asymmetric cryptography**
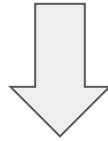
The private key is generated and maintained in a device upon registration

# Fast IDentity Online 2 (FIDO2)

It is a **passwordless** authentication standard based on **asymmetric cryptography**
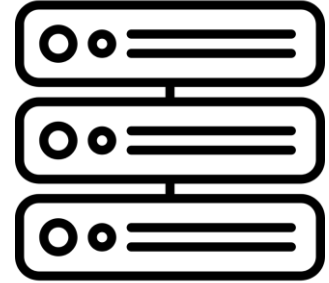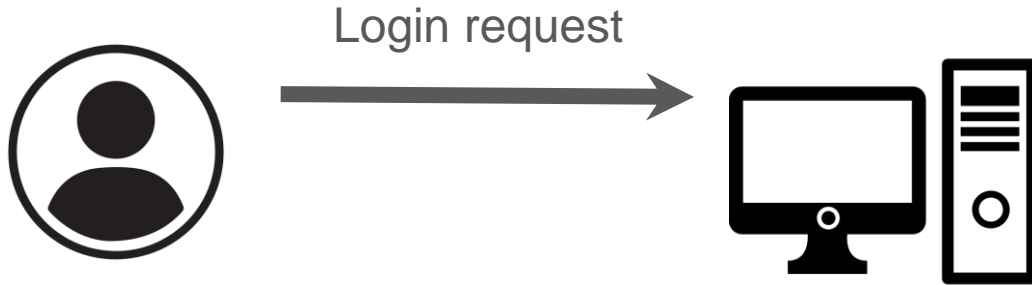
⬇

The private key is generated and maintained in a device upon registration

⬇

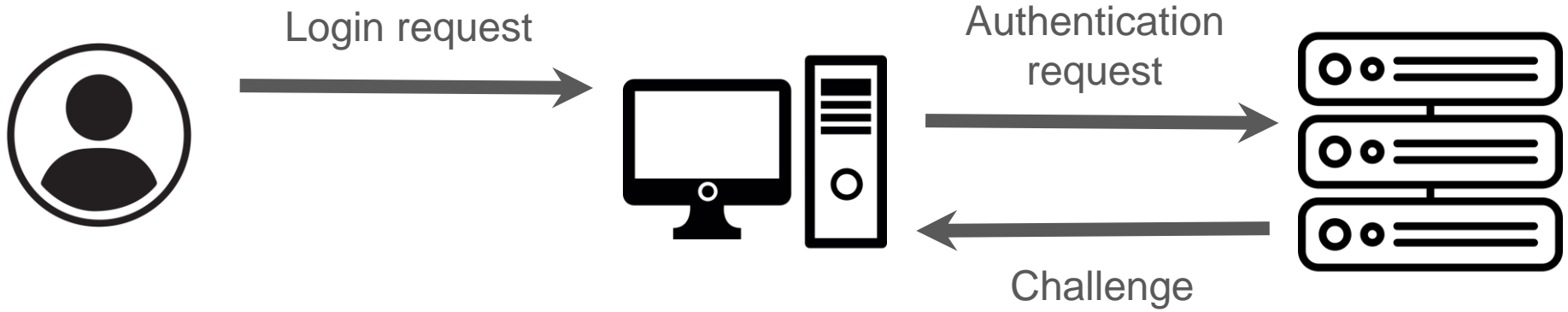It can be used later to sign data and, therefore, authenticate a user
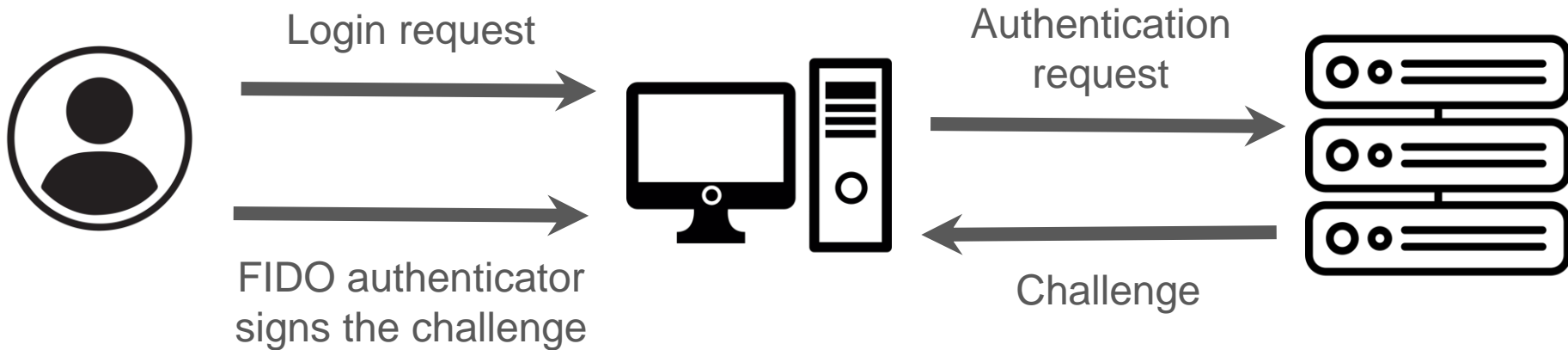
# Webpage authentication example

Login request

# Webpage authentication example

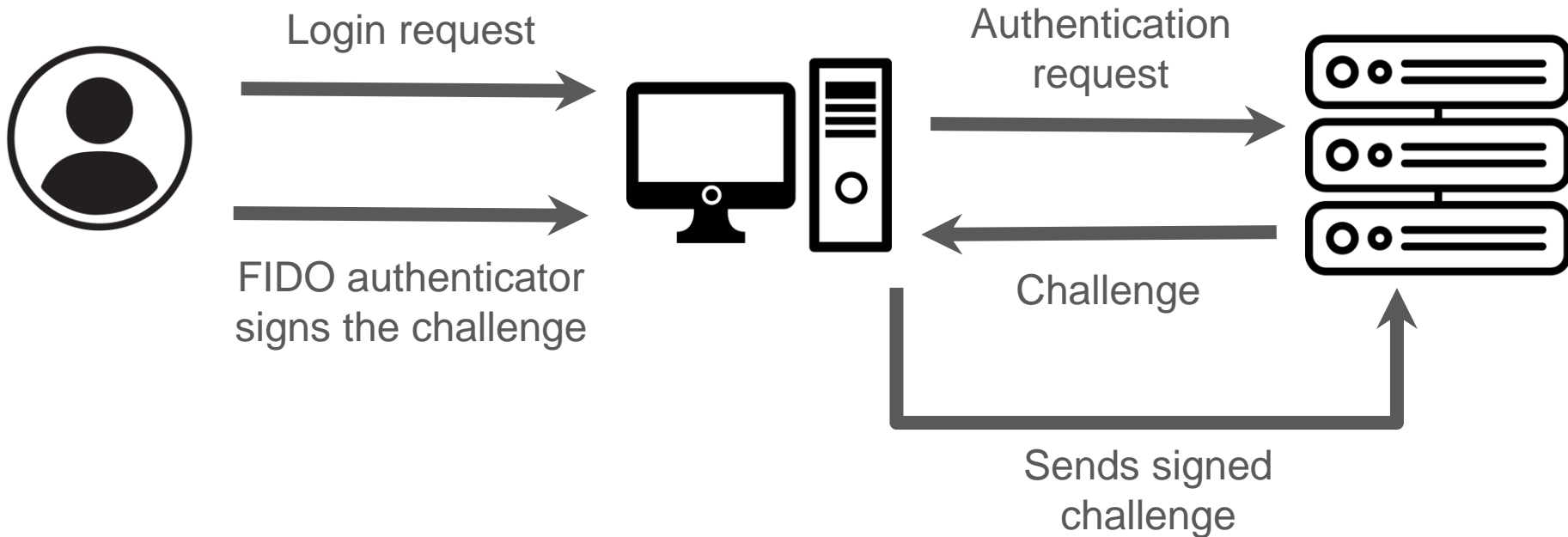Login request

Authentication request

# Webpage authentication example



Login request

Authentication request

Challenge

# Webpage authentication example



Login request

FIDO authenticator signs the challenge

Authentication request

Challenge

# Webpage authentication example



Login request

Authentication request

FIDO authenticator signs the challenge

Challenge

Sends signed challenge

# Webpage authentication example



Login request

Authentication request

FIDO authenticator signs the challenge

Challenge

Successful login

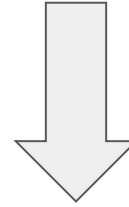Sends signed challenge

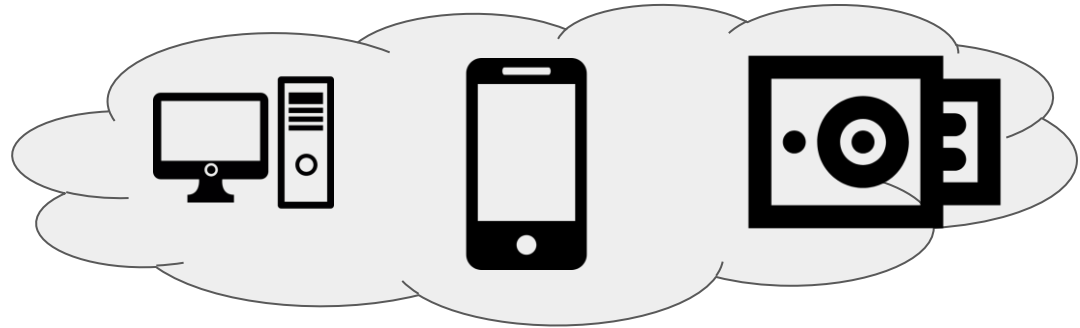Successful authentication (if signature is correct)
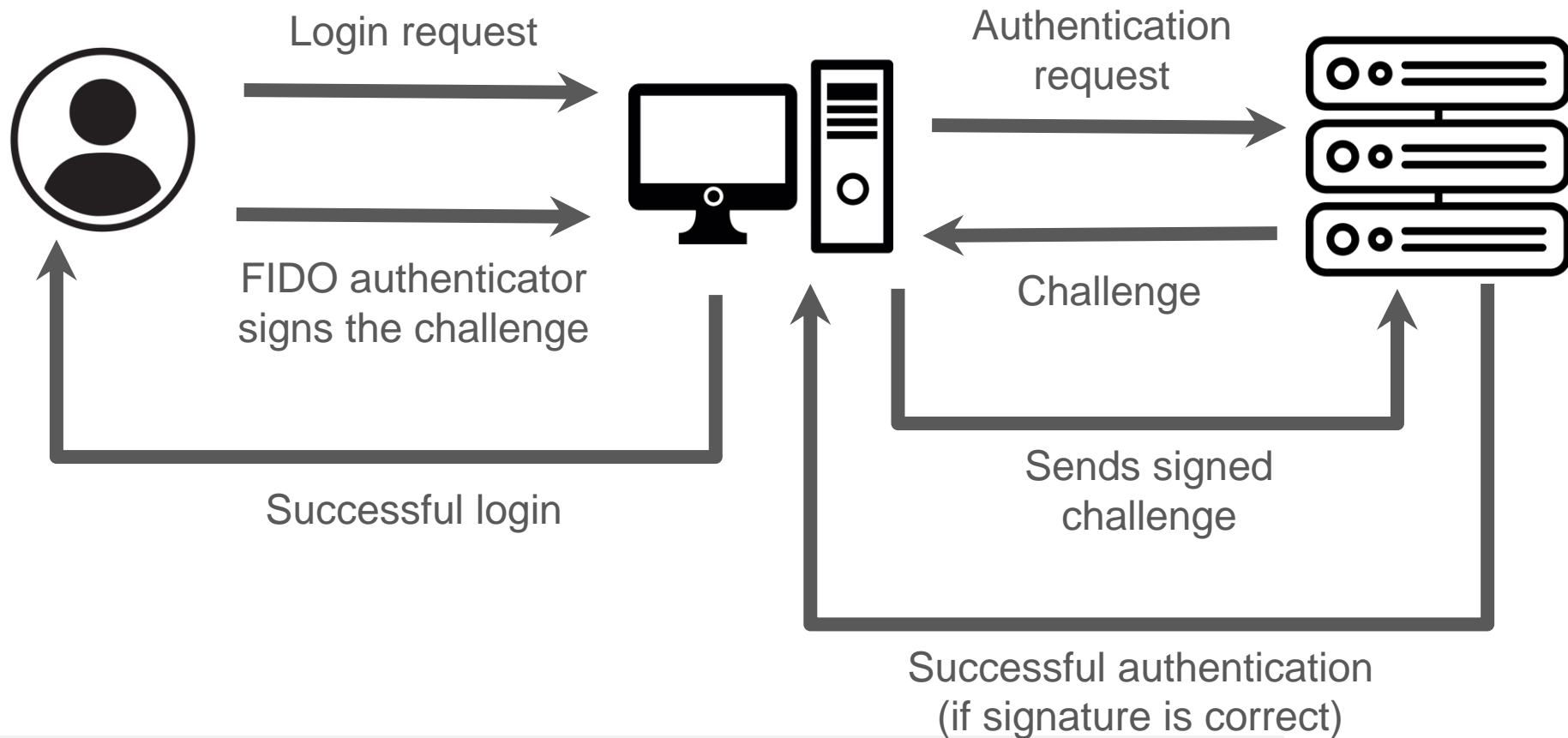
# Passkey

We call **Passkeys** to the FIDO credentials

# Passkey

We call **Passkeys** to the FIDO credentials

They can be stored in many ways
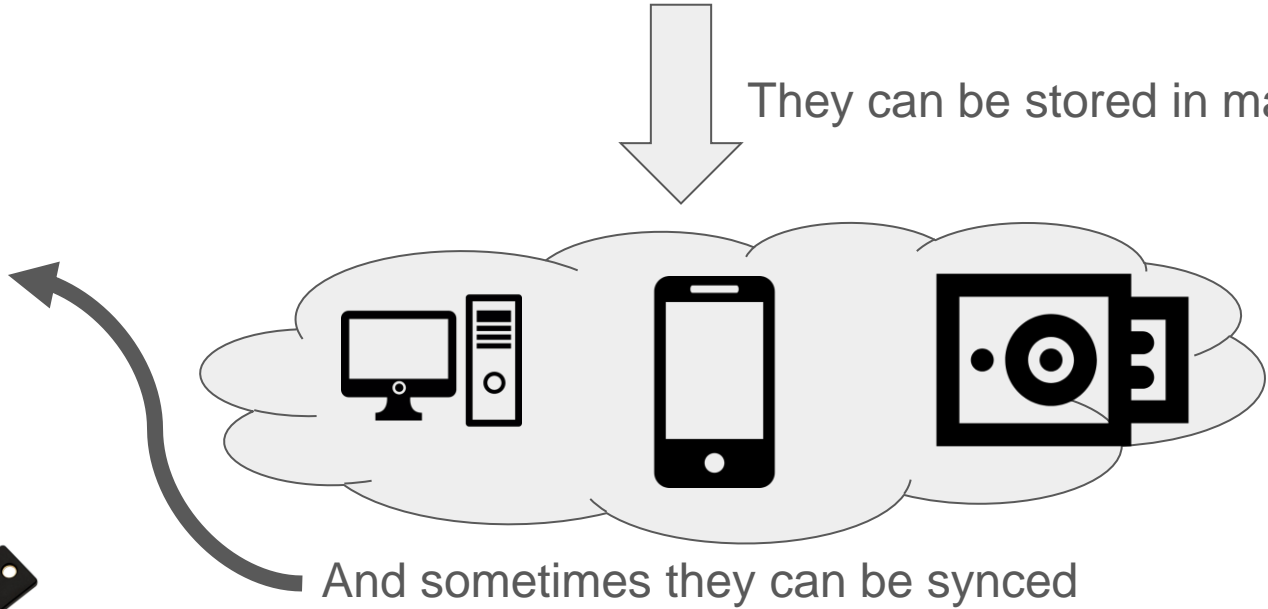
And sometimes they can be synced

# Passkey

We call **Passkeys** to the FIDO credentials

They can be stored in many ways

If not, we are in the presence of **device-bound passkeys**

Example: **Yubikeys**

And sometimes they can be synced

# Multi-Factor Authentication (MFA)



User to respond to 2 or more factors

**Something they know**

Password or PIN

**+**

**Something they have**

Smart card or push notifications

**+**

**Something they are**

Fingerprint or geographic location

**=**

**Access granted**

https://www.akamai.com/glossary/what-is-multifactor-authentication