Imagine: A world without passwords, it is easy if you try

Who am I?

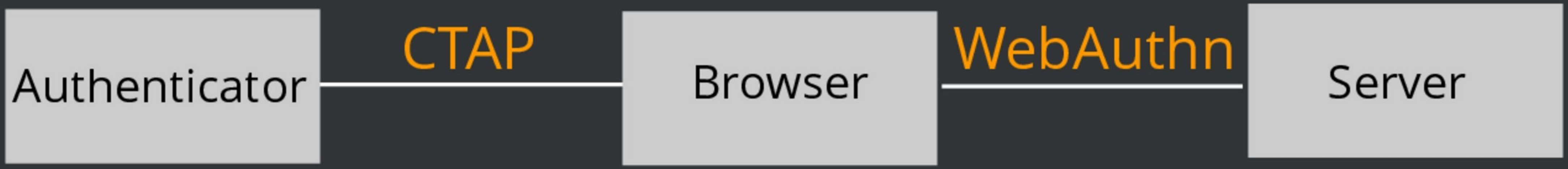
- Sigurhjörtur Snorrason
- Head of Software Development at PONE Biometrics AS
- Work with making FIDO2 Hardware Devices

Agenda

- The FIDO2 Project
- Passwords
- How FIDO2 is safer
- What is possible today

What is FIDO

- Original idea to use Biometrics to login
- Moved forward and made CTAP and WebAuthn
- Officially a standard since December 2018
- CTAP the real magic for servers and authenticators
- WebAuthn frontend API to make CTAP easy



Passwords are great...

- Passwords are great
- Simple
- Easy to use

...but not very secure

- Symmetric
- Easy to guess
- Hard to remember

Passwords

Bangladesh Bank robbery

Bangladesh Bank Robbery

- Cyber-heist in February 2016
- Almost stole $951 million
- In the end stole about $80 million

Bangladesh Bank Robbery

- Started with spear phishing
- Tracked down passwords silently
- Got access to SWIFT system
- Most transactions got blocked by other banks

So how does it work?

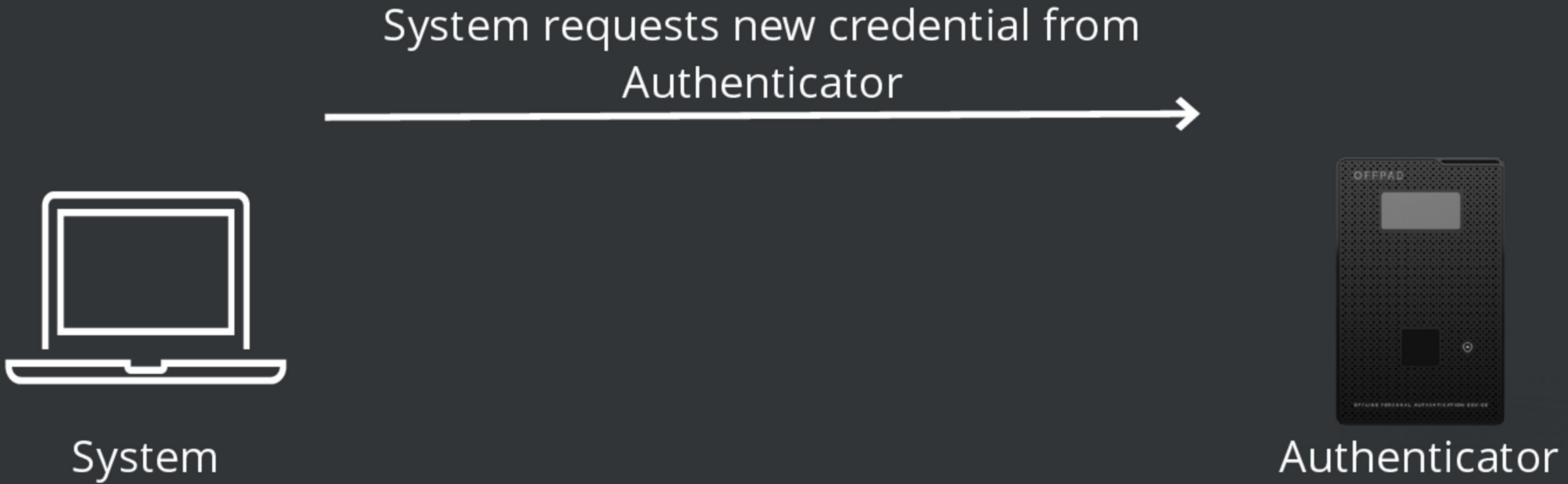
Creating a credential

Creating new credential

System

Authenticator

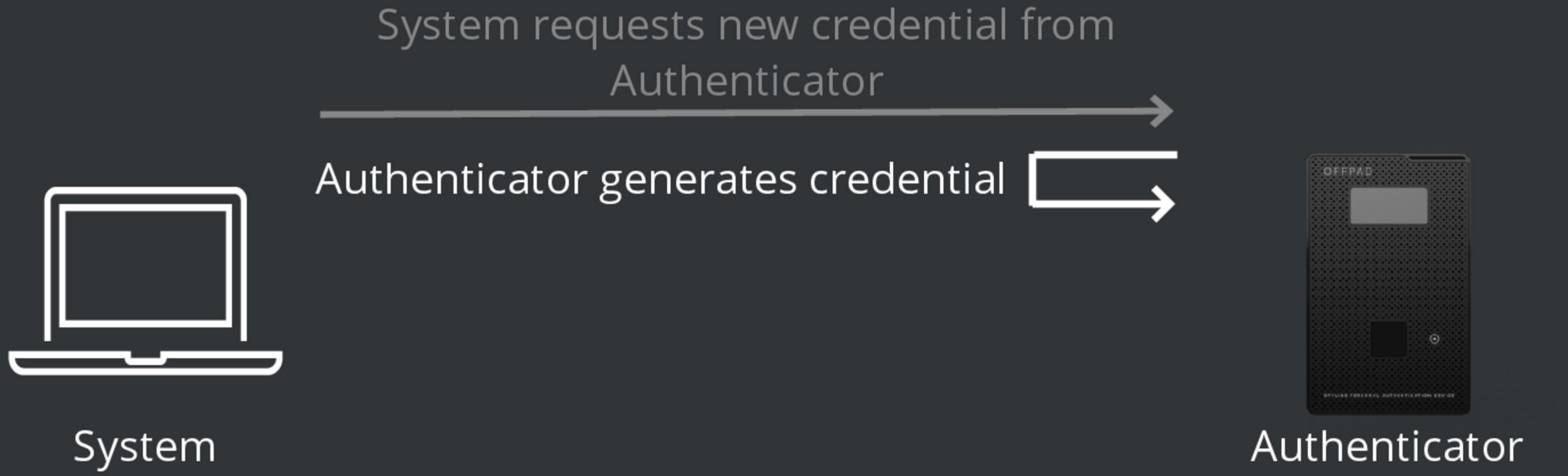
Creating new credential


System requests new credential from Authenticator

System

Authenticator

Creating new credential



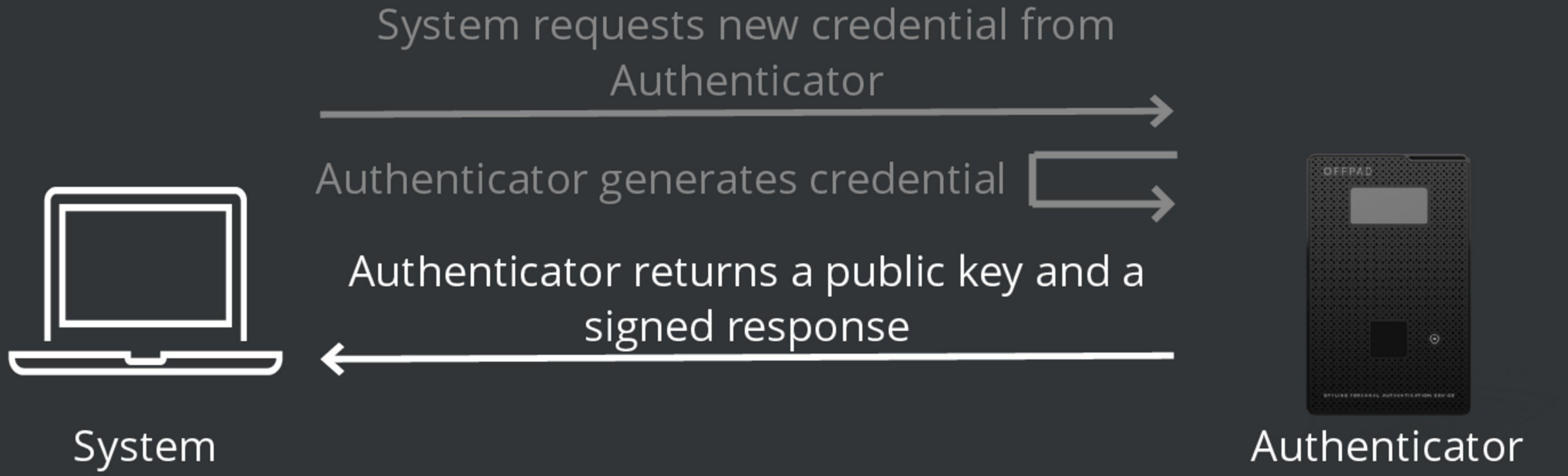
System requests new credential from Authenticator

Authenticator generates credential

System

Authenticator

Creating new credential



System requests new credential from Authenticator

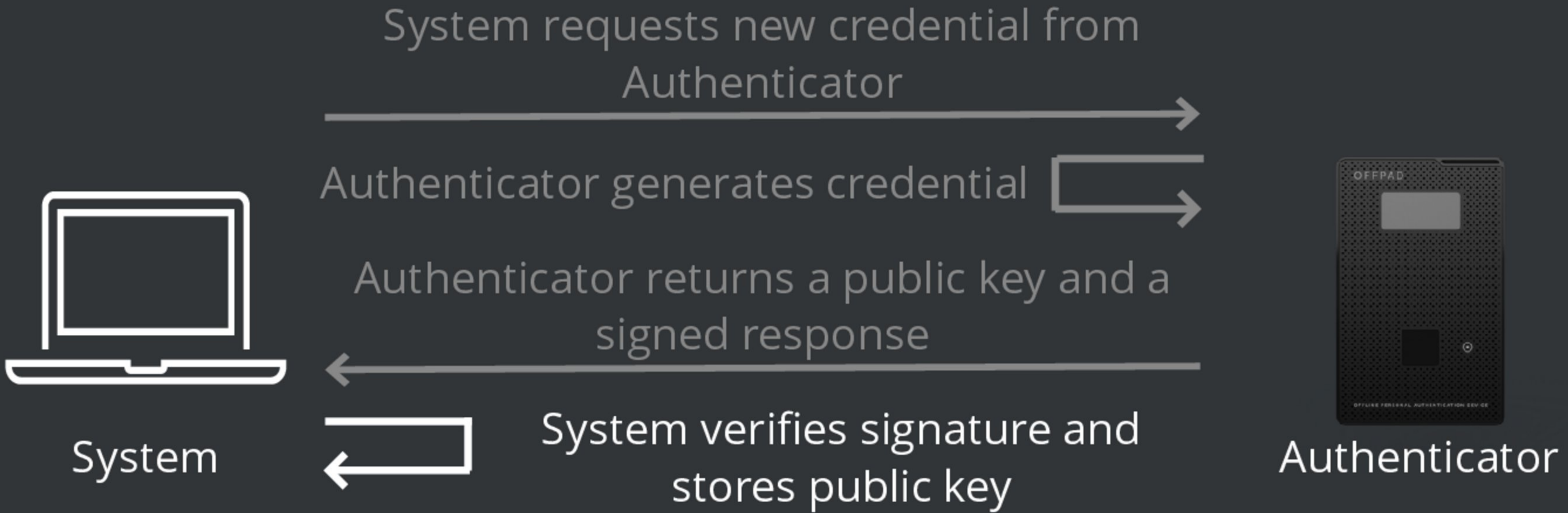
Authenticator generates credential

Authenticator returns a public key and a signed response

System

Authenticator

Creating new credential



System requests new credential from Authenticator

Authenticator generates credential

Authenticator returns a public key and a signed response

System verifies signature and stores public key

System

Authenticator

So how does it work?

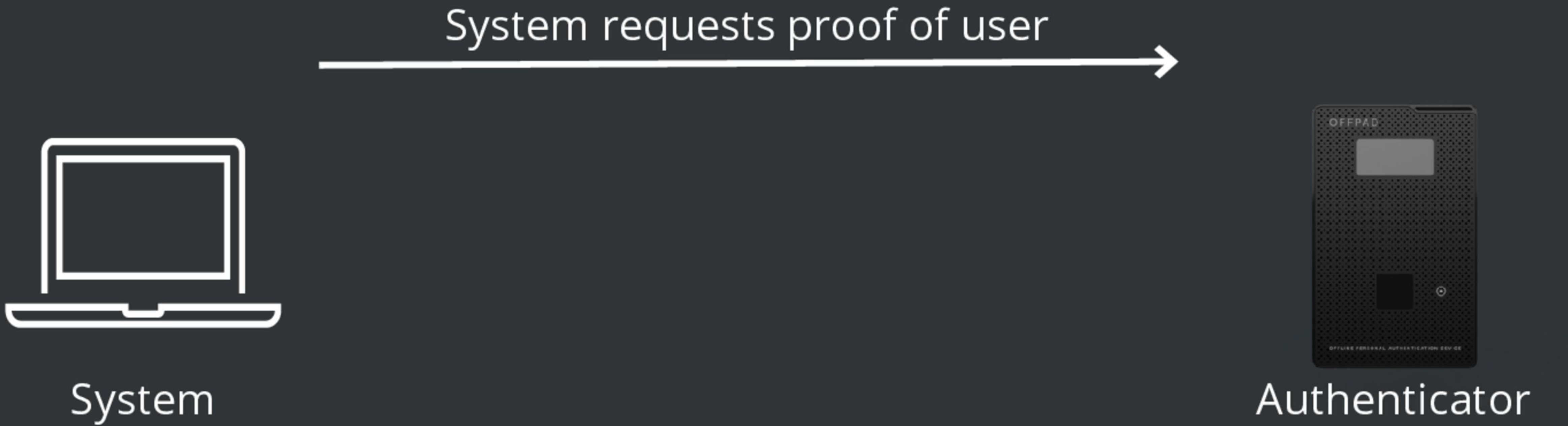
Verifying a user

Verifying user

System

Authenticator

Verifying user

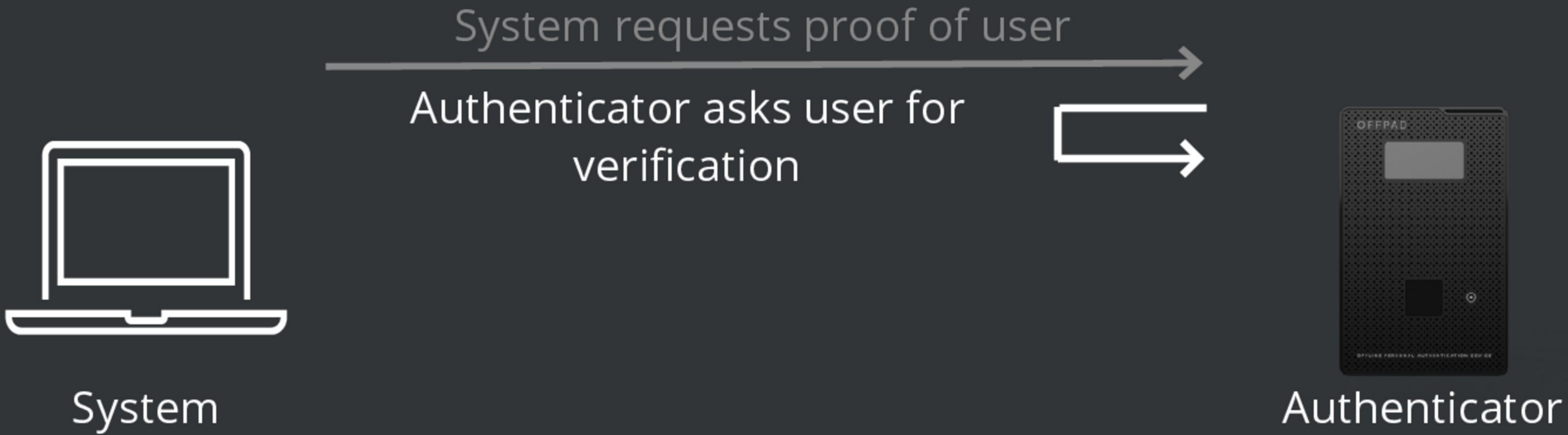


System requests proof of user

System

Authenticator

Verifying user



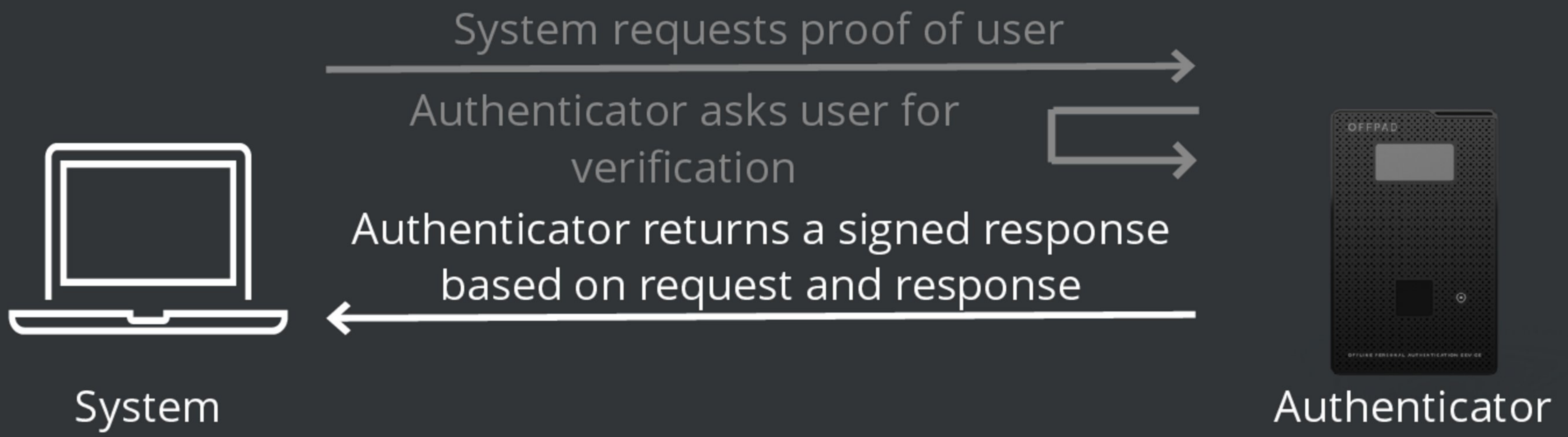
System requests proof of user

Authenticator asks user for verification

System

Authenticator

Verifying user



System requests proof of user

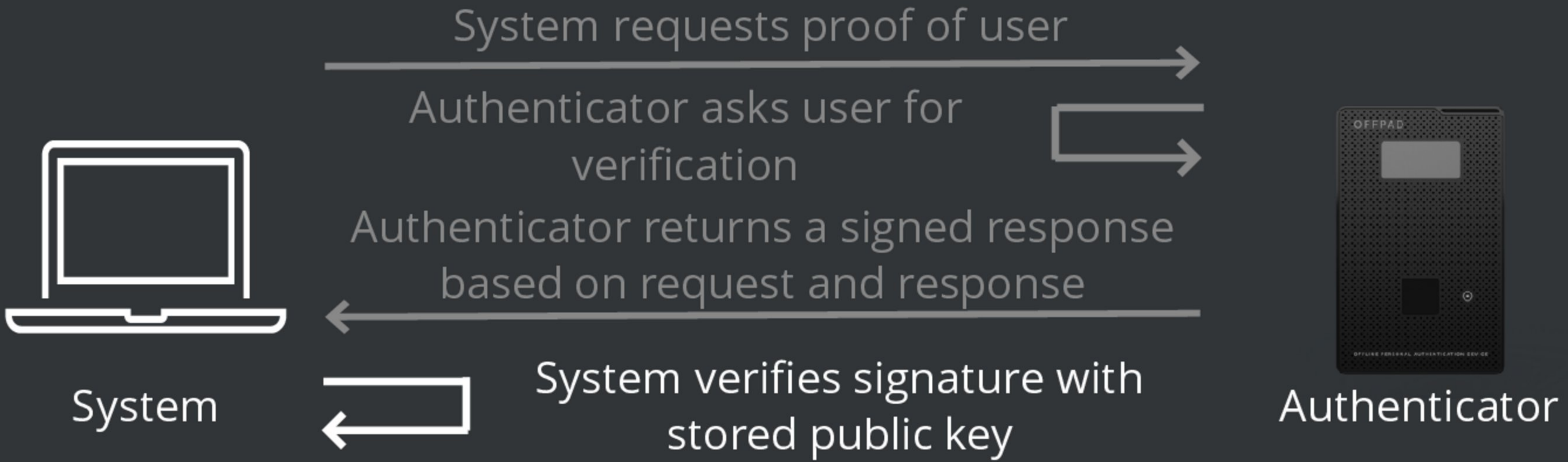
Authenticator asks user for verification

Authenticator returns a signed response based on request and response

System

Authenticator

Verifying user



System requests proof of user

Authenticator asks user for verification

Authenticator returns a signed response based on request and response

System verifies signature with stored public key

System

Authenticator

What happend?

- Server always sends random data with request
- Server also sends URL of request
- Authenticator always signs request and response
- Server can verify it is the same request
- No more phishing

What to do today?

- Depends on your paranoia level
- Passkeys
- Virtual Authenticators
- Platform based (Windows Hello)
- Hardware keys

Passkeys

- Available from both Apple and Google since 2023
- iOS 16 or Android 4.4
- Easy to use
- Possibility to cloud share keys across devices

Virtual Authenticators

- Provided through Password Managers mostly
- Let's you store private key in your vault
- Easy to use
- Possibility to cloud share keys across devices
- Everything is virtual, not the most secure

Platform authenticators

- Mostly applies to Windows Hello
- Available since 2019 (!)
- Even easier to use
- Locked to the machine you use

Hardware authenticators

- Multiple vendors
- Private keys stored on authenticator only
- Same hardware key towards multiple devices
- Expensive

FIDO2 Limitations

- Limited Android support, only through Apps or Passkeys
- Linux USB only
- macOS/iOS supports USB and NFC only
- Windows supports everything

Questions?