Secure Authentication with FIDO, Biometrics and Security Keys

Tjerand Silde & Trond Peder Hagen

PONE BIOMETRICS

About Us

Tjerand Silde is a Security and Cryptography Expert at Pone Biometrics and an Associate Professor in Cryptology at NTNU

Trond Peder Hagen is the Chief Technology Officer at Pone Biometrics

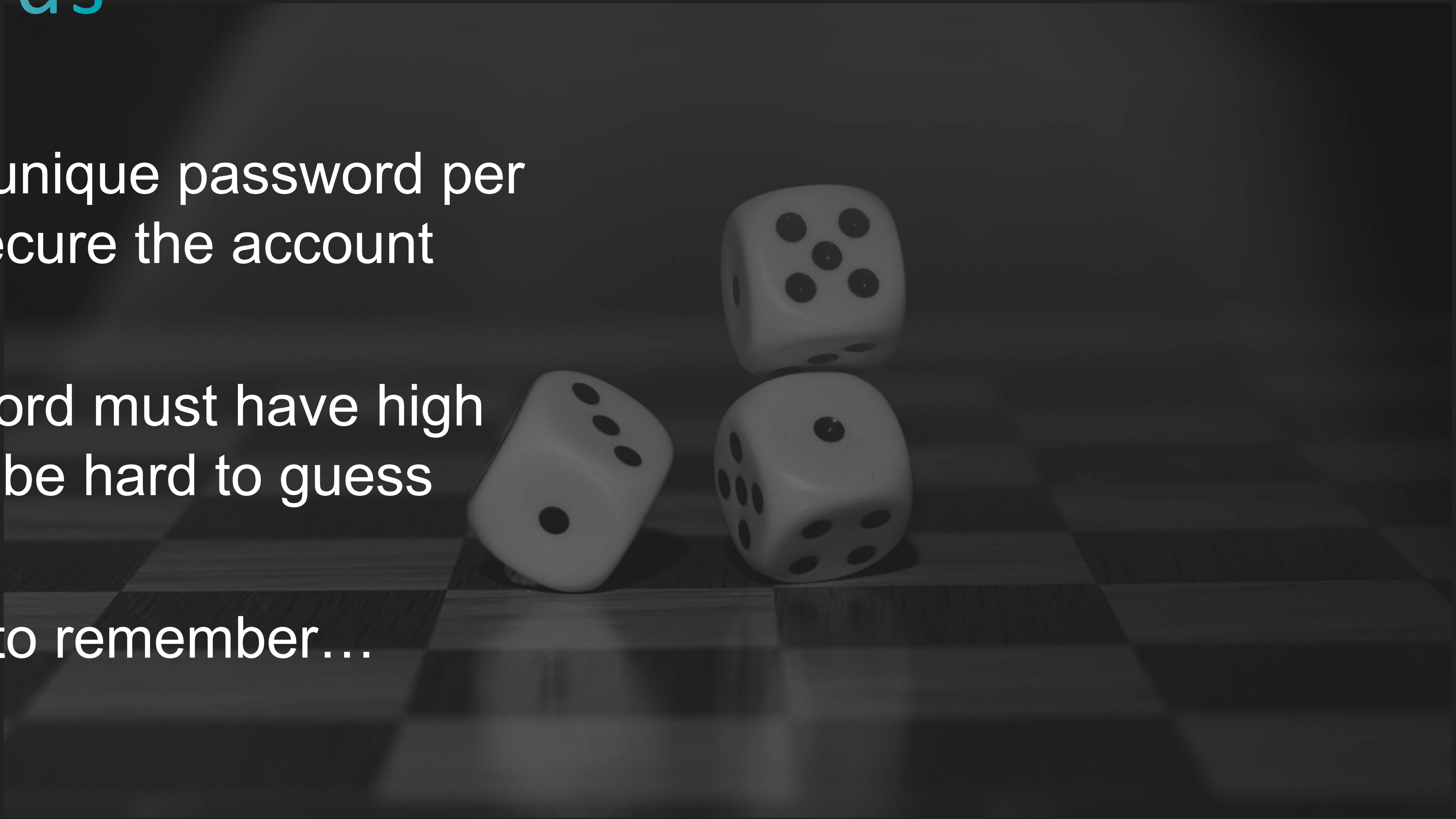
Authentication

All services need to securely authenticate their users

Authentication must be user-friendly for it to be used

Most users nowadays have approximately 100 accounts

Passwords

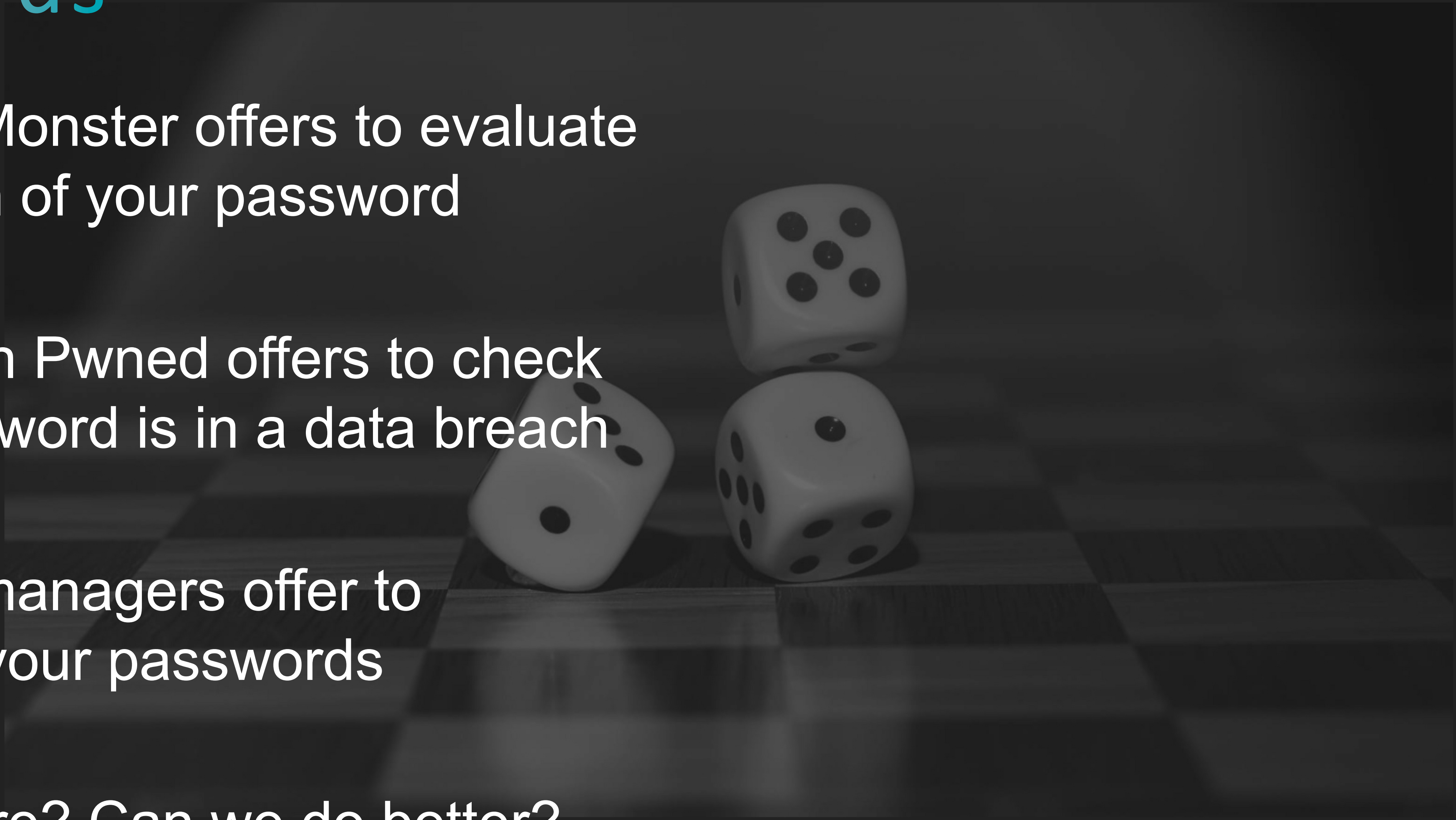


You need a unique password per service to secure the account

Each password must have high entropy and be hard to guess

This is a lot to remember…

Passwords



Password Monster offers to evaluate the strength of your password

Have I Been Pwned offers to check if your password is in a data breach

Password managers offer to remember your passwords

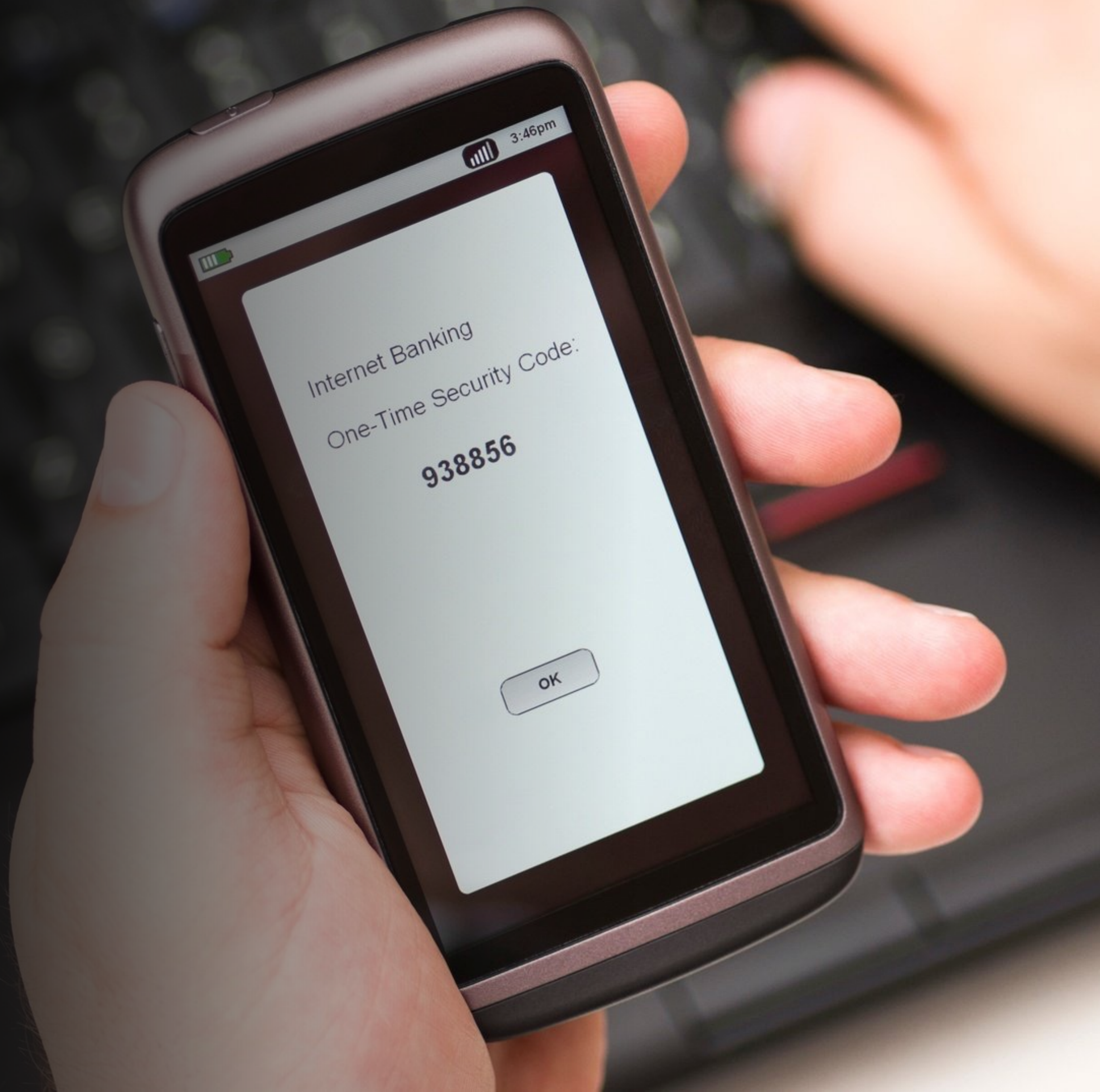
Is this secure? Can we do better?

One-Time Passwords (OTP)

We have several ways to provide extra security with one-time passwords:

- OTPs on SMS
- OTPs via app
- OTPs as push

Is this fully secure?



Challenges with OTP

Someone can steal your SIM card (SIM-swapping)

People get tired of notifications (MFA-fatigue)

It does not protect against phishing and false websites

Issues with backing up password generators

Biometrics

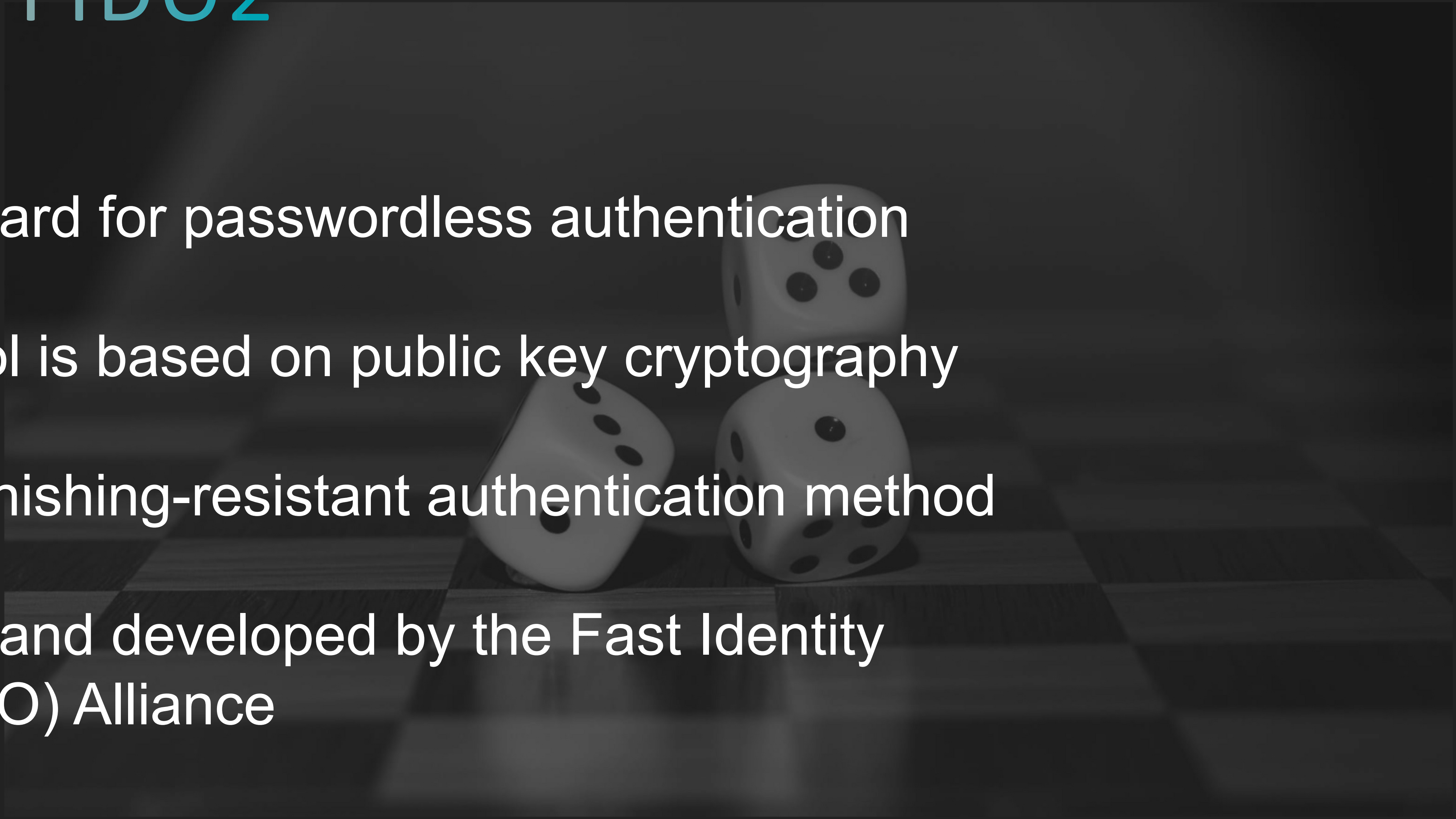
Offers higher entropy than (rememberable) passwords

Ties the user tightly to their identity and role

Strong but not secret authentication (username)

Biometric sensors and algorithms improves yearly

What is FIDO2



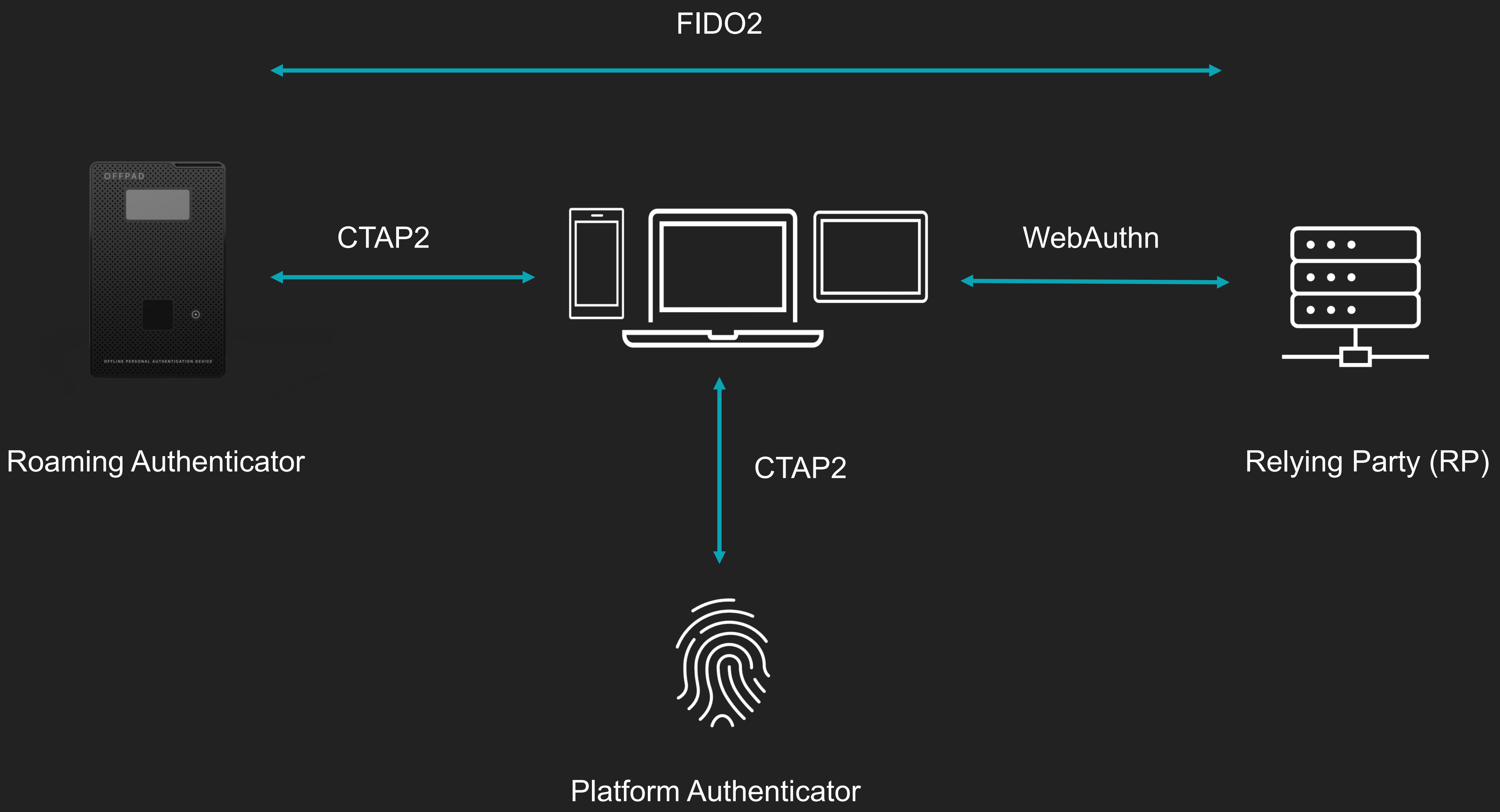
Open standard for passwordless authentication

The protocol is based on public key cryptography

It offers a phishing-resistant authentication method

Maintained and developed by the Fast Identity Online (FIDO) Alliance

FIDO2 Ecosystem



FIDO2

CTAP2

WebAuthn

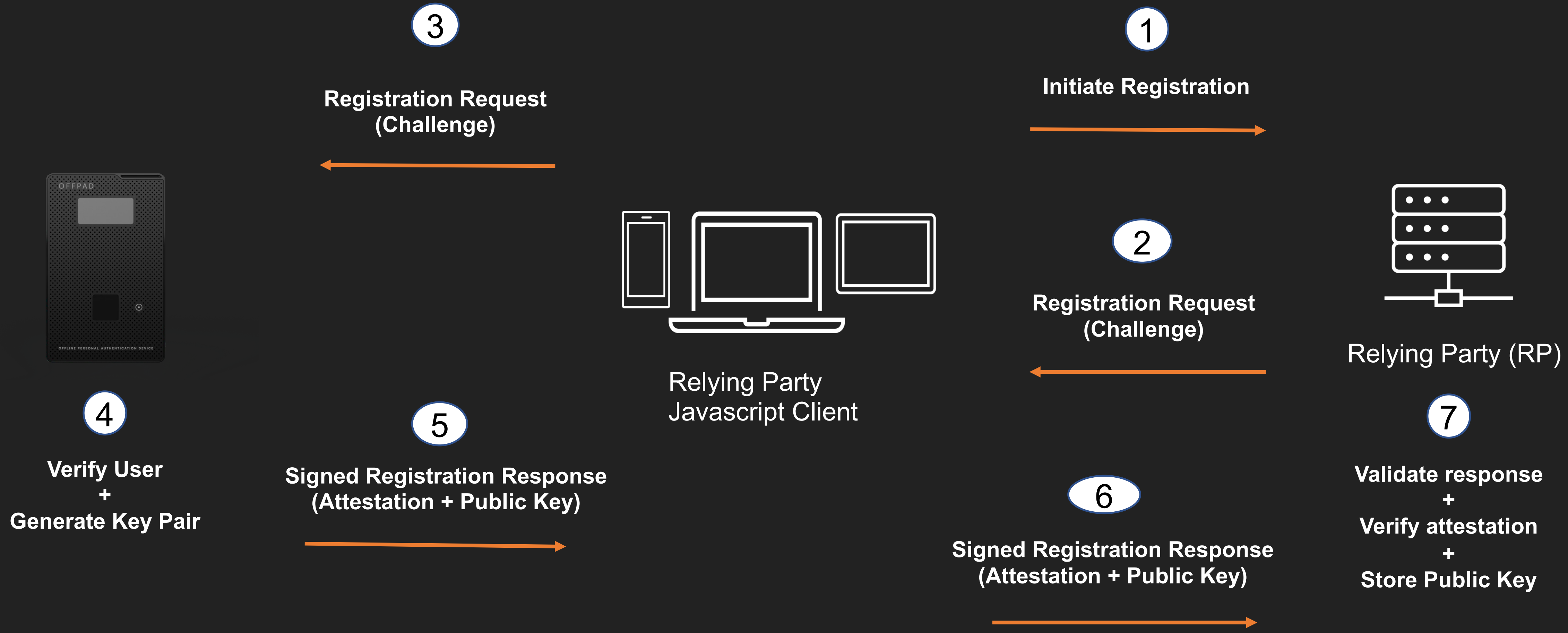
Roaming Authenticator

CTAP2

Relying Party (RP)

Platform Authenticator

FIDO2 Registration



1 Initiate Registration

2 Registration Request (Challenge)

3 Registration Request (Challenge)

4 Verify User + Generate Key Pair

5 Signed Registration Response (Attestation + Public Key)

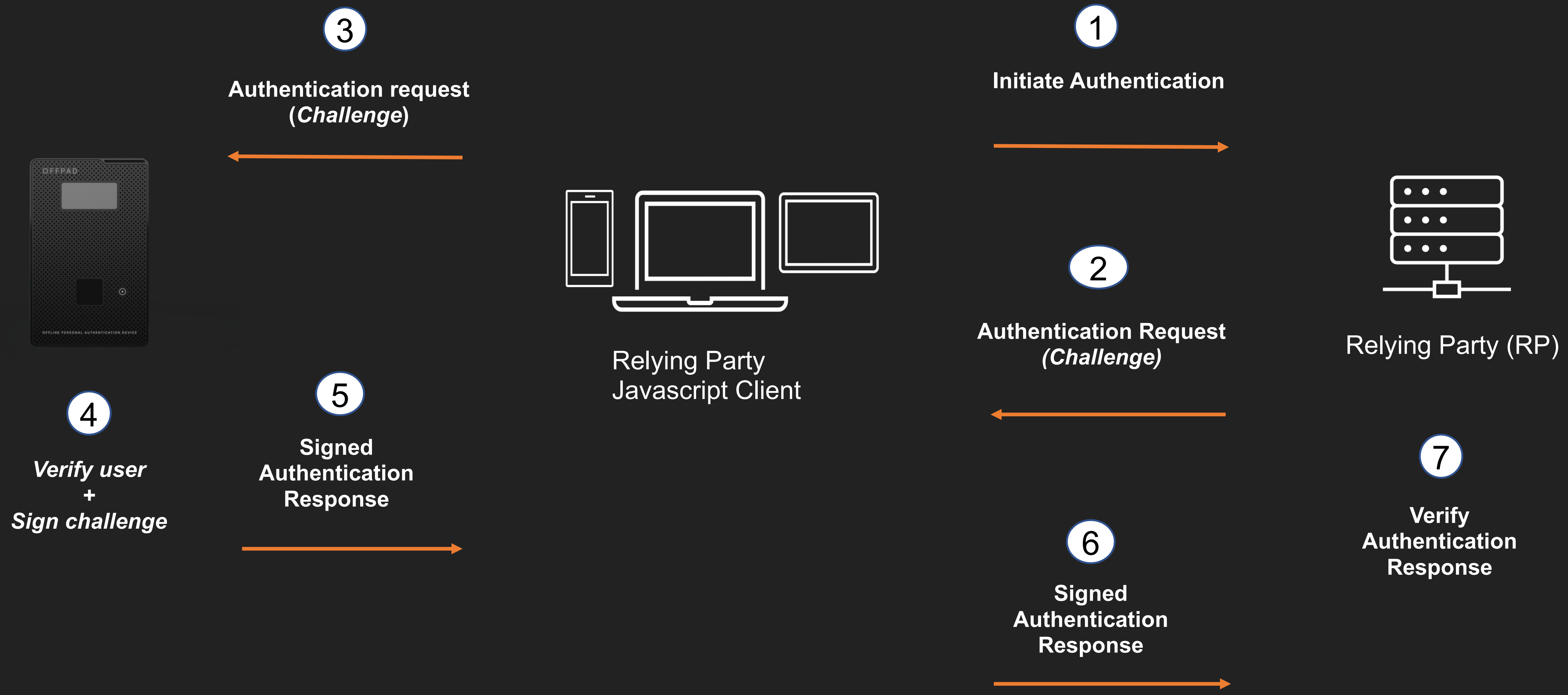
6 Signed Registration Response (Attestation + Public Key)

7 Validate response + Verify attestation + Store Public Key

Relying Party Javascript Client

Relying Party (RP)

FIDO2 Authentication



Relying Party Javascript Client

Relying Party (RP)

1 **Initiate Authentication**

2 **Authentication Request *(Challenge)***

3 **Authentication request (*Challenge*)**

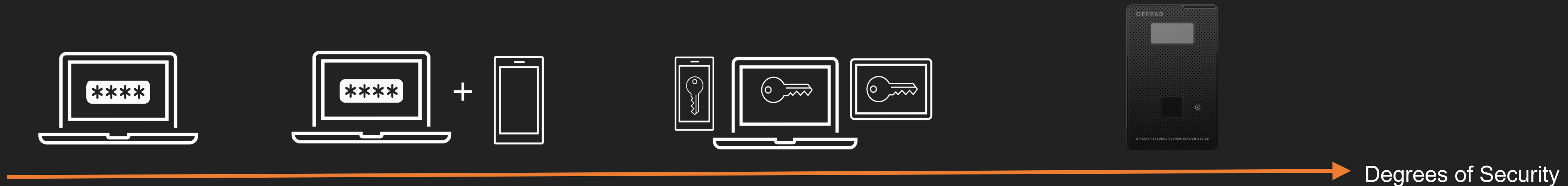
4 ***Verify user*** **+** ***Sign challenge***

5 **Signed Authentication Response**

6 **Signed Authentication Response**

7 **Verify Authentication Response**

Security Spectrum



Degrees of Security

Password

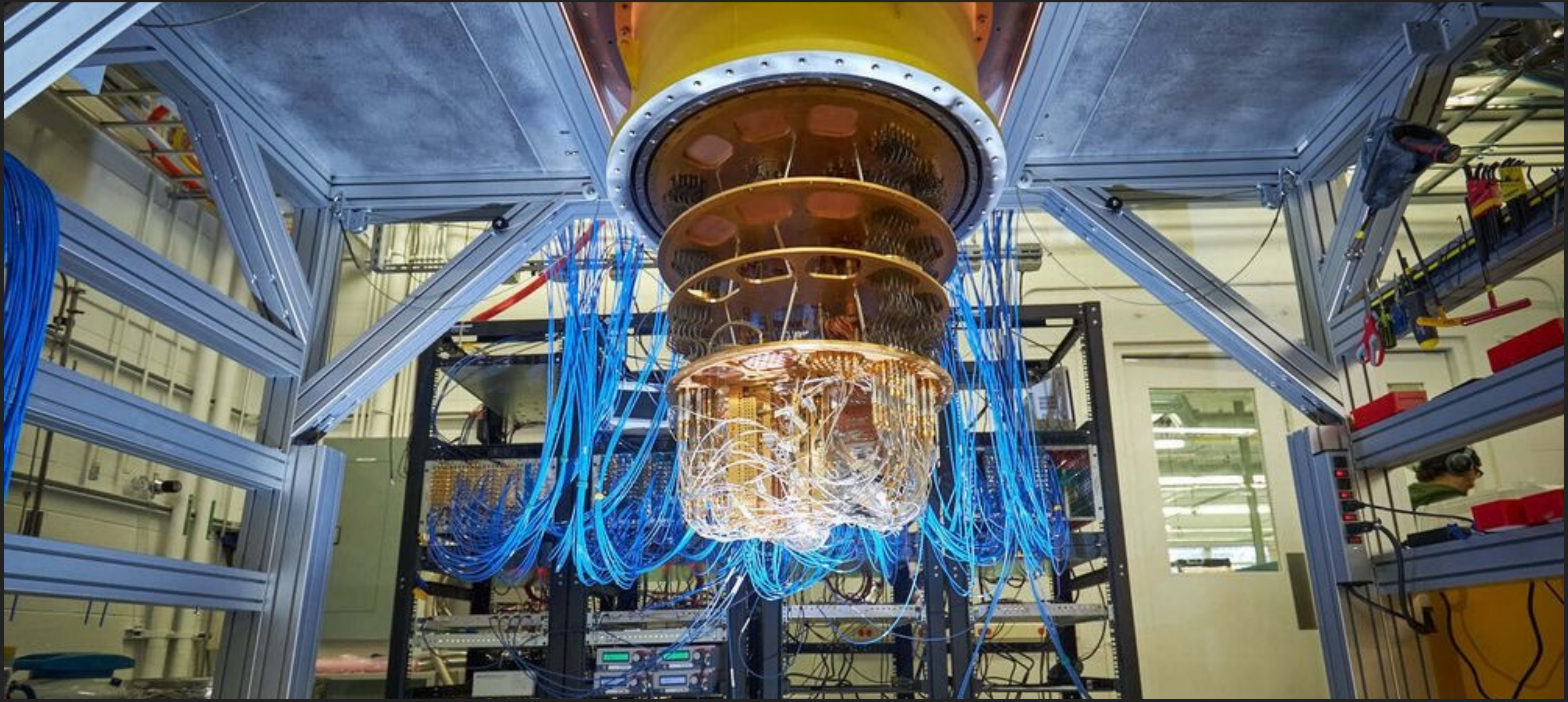
Password + OTP

Synced Passkeys

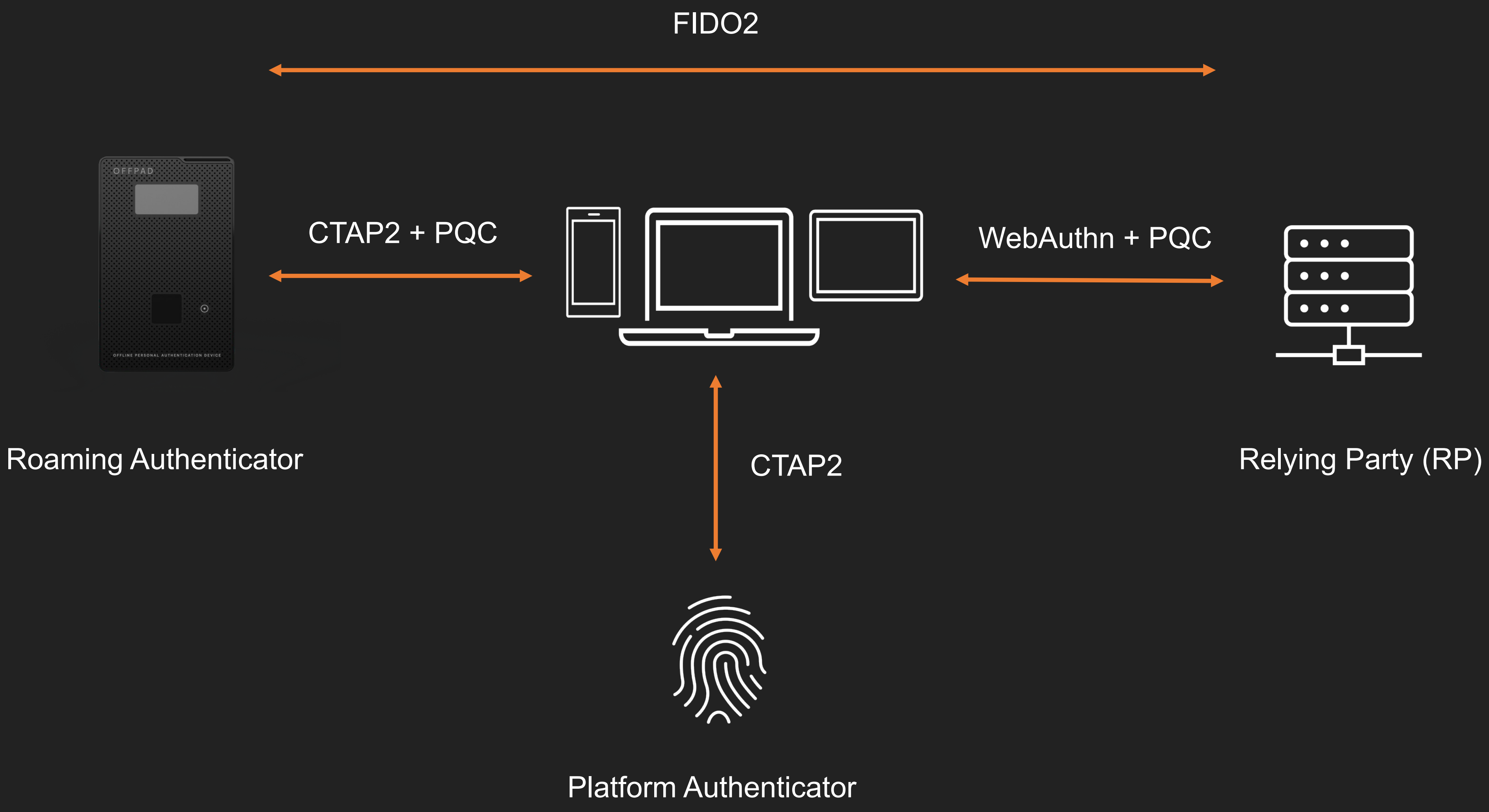
Device-Bound Passkeys

Thank you!
Questions?

Tomorrow: Quantum Computers



FIDO2 and PQC (Dilithium) Signatures



FIDO2

CTAP2 + PQC

WebAuthn + PQC

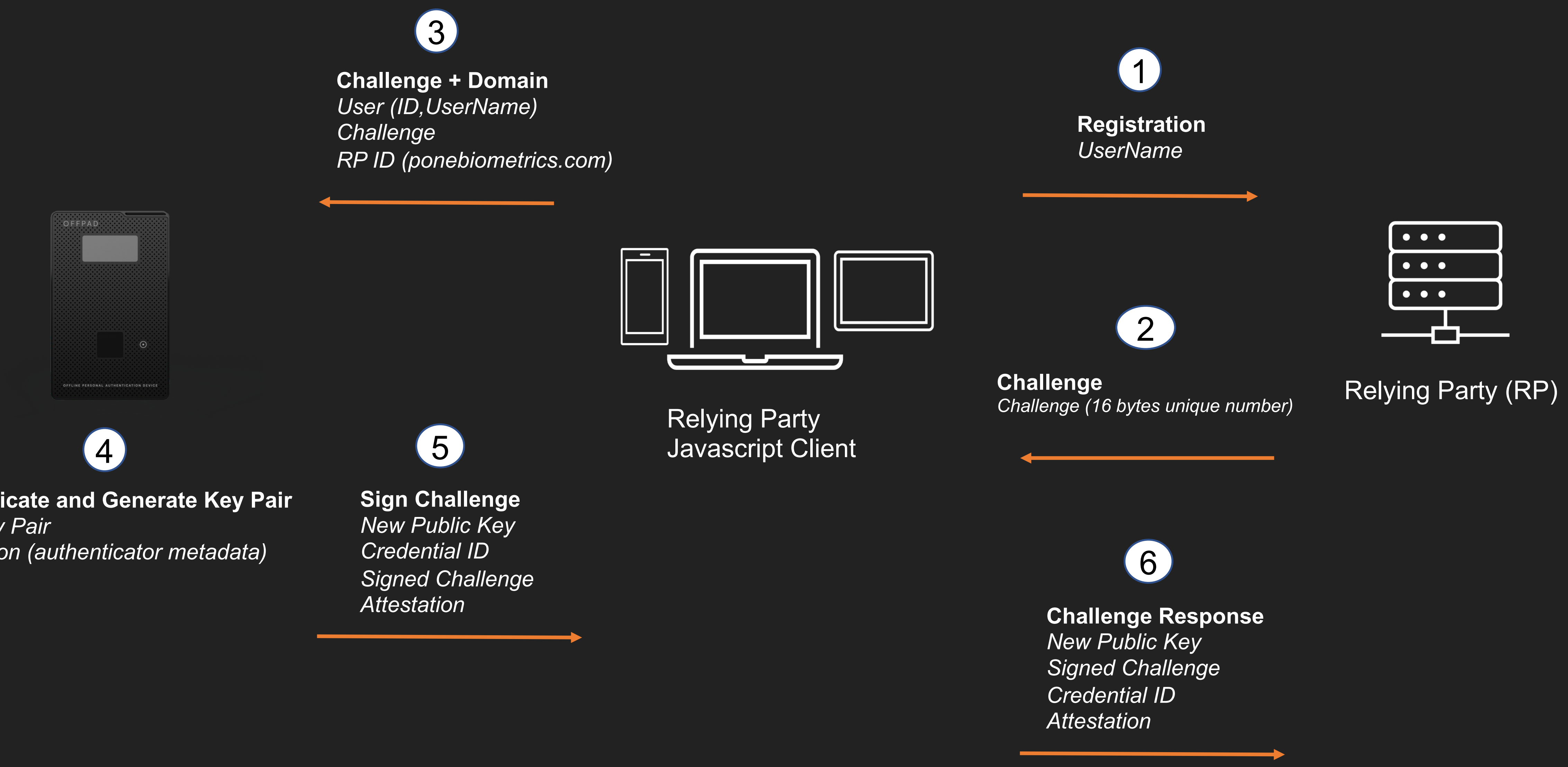
CTAP2

Roaming Authenticator

Relying Party (RP)

Platform Authenticator

FIDO2 Registration



1

Registration
UserName

2

Challenge
Challenge (16 bytes unique number)

3

Challenge + Domain
User (ID,UserName)
Challenge
RP ID (ponebiometrics.com)

4

Authenticate and Generate Key Pair
New Key Pair
Attestation (authenticator metadata)

5

Sign Challenge
New Public Key
Credential ID
Signed Challenge
Attestation

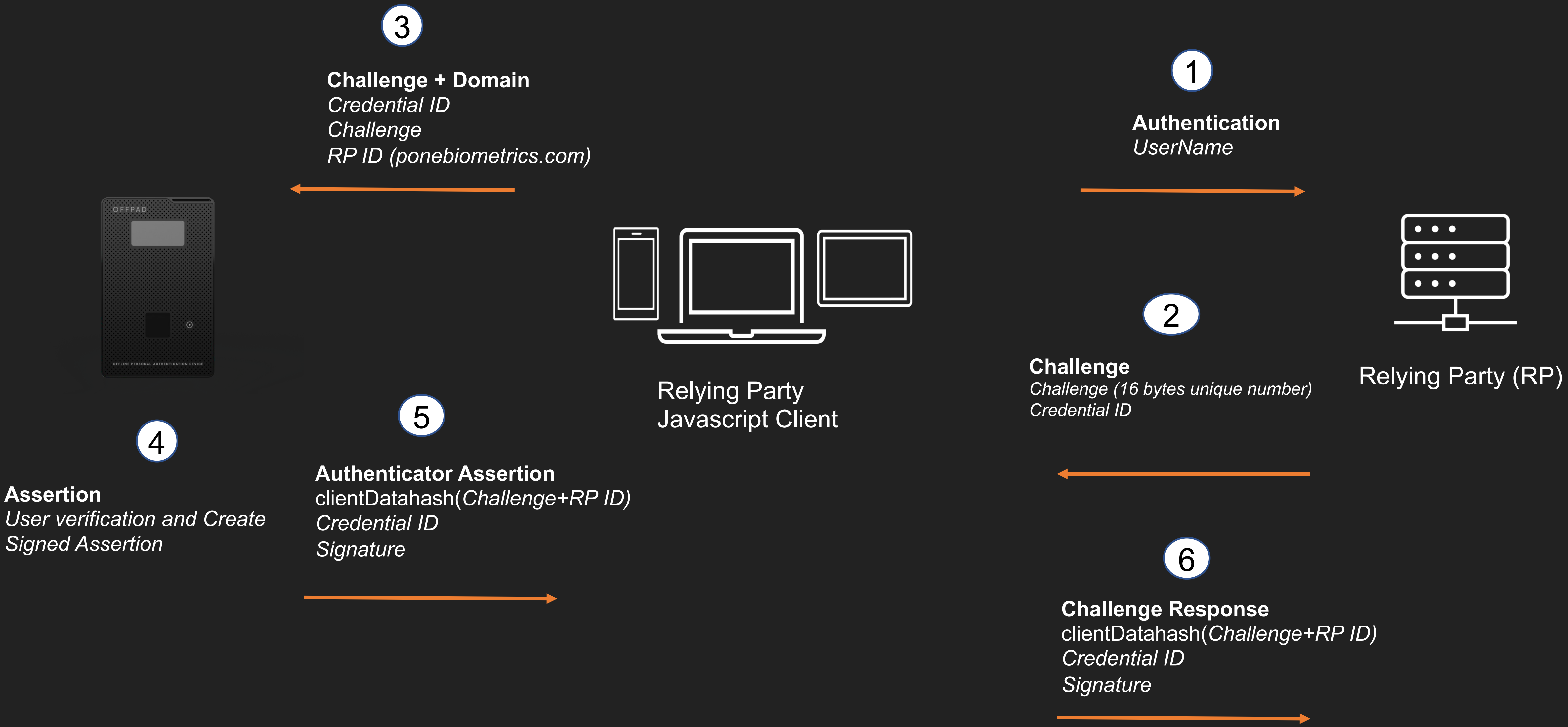
6

Challenge Response
New Public Key
Signed Challenge
Credential ID
Attestation

Relying Party
Javascript Client

Relying Party (RP)

FIDO2 Authentication



1

Authentication
UserName

2

Challenge
Challenge (16 bytes unique number)
Credential ID

3

Challenge + Domain
Credential ID
Challenge
RP ID (ponebiometrics.com)

4

Assertion
User verification and Create
Signed Assertion

5

Authenticator Assertion
clientDatahash(*Challenge+RP ID)*
Credential ID
Signature

6

Challenge Response
clientDatahash(*Challenge+RP ID)*
Credential ID
Signature

Relying Party
Javascript Client

Relying Party (RP)