All the Things PQ – End-to-End PQ-Secure Fido2 Protocol

Nina Bindel, Staff Researcher

Open Source Cryptography Workshop

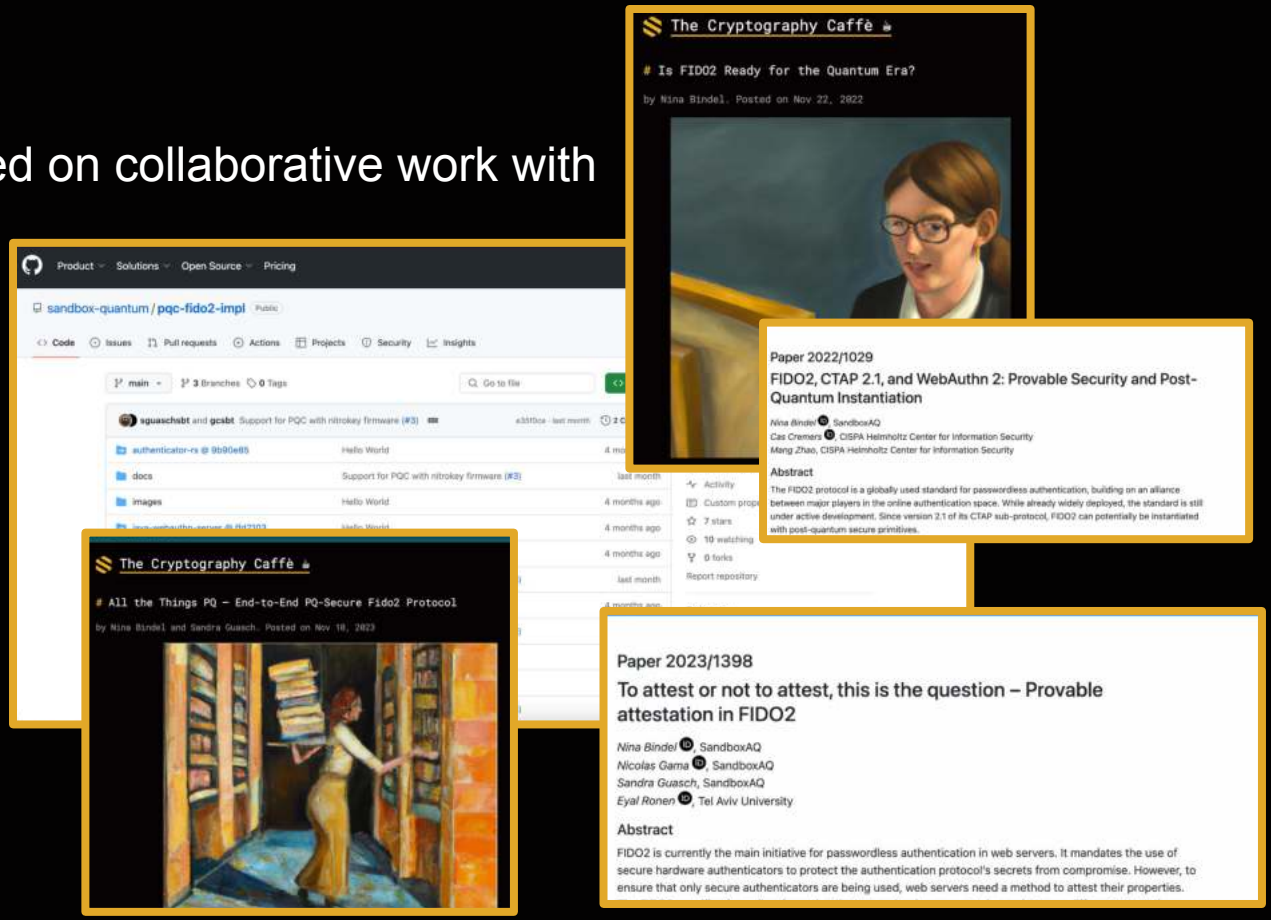
March 28, 2024

Acknowledgment

This presentation is based on collaborative work with

Gabriel Campagna
Cas Cremers
Nicolas Gama
Sandra Guasch
James Howe
Tarun Yadav
Duc Ngyuen
Eyal Ronen
Mang Zhao

All icons are from flaticon premium.



SANDBOXAQ

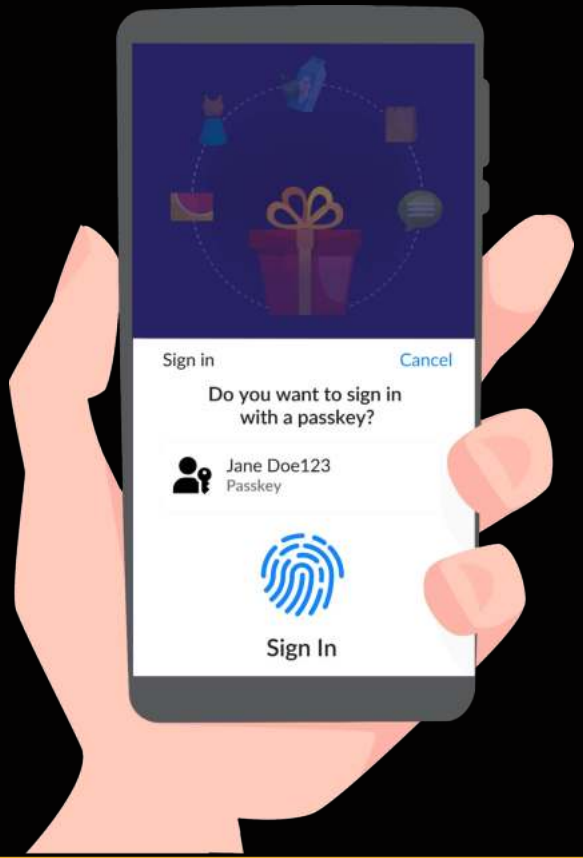
Comprised by more than **40 key companies**, including Amazon, Apple, Google, Intel, Microsoft, RSA, VISA, and Yubico

Defined de facto standard for passwordless authentication: **FIDO2 protocol**

What is FIDO2?

Advantages

- No need to remember passwords
- Easy to use
- Resistant to phishing attacks
- Widely adopted: FIDO Alliance / W3C standards
  - Supported by all major browsers and platforms
  - Wide range of industry partners
- Constant improvements



A (very) brief history of FIDO authentication

2014

U2F

2nd factor authentication

2019

FIDO2 = CTAP (FIDO) + WebAuthn (W3C)

Security tokens are generate credentials which are registered and used to authenticate

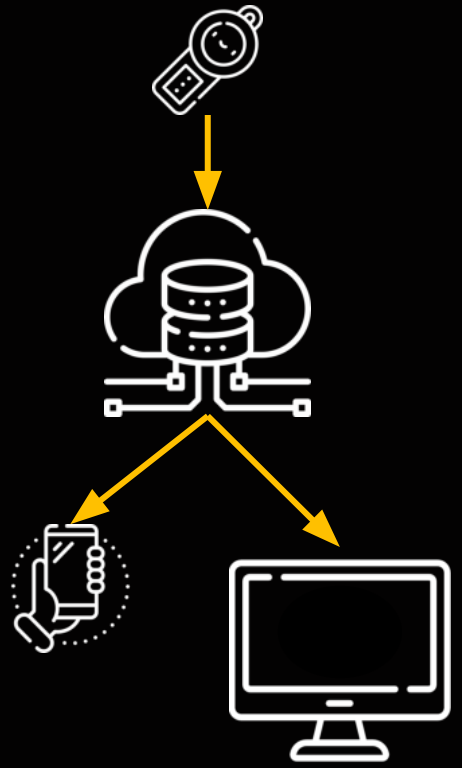
2022

Passkeys

Passkeys = FIDO2 with the option of synchronization of credentials such that synced devices can be used to authenticate

Passkeys

- Credential synchronisation among different devices
- Credentials are encrypted E2E
- Device-bound credentials can still be enforced for critical applications
- Attestation becomes crucial to understand how a credential is managed



A (very) brief history of FIDO authentication

2014

U2F

2nd factor authentication

2019

FIDO2 = CTAP (FIDO) + WebAuthn (W3C)

Security tokens are generate credentials which are registered and used to authenticate

2022

Passkeys

Passkeys = FIDO2 with the option of synchronization of credentials such that synced devices can be used to authenticate

2024

White Paper: Addressing FIDO Alliance's Technologies in Post Quantum World

Acknowledging the quantum threat and need to select suitable PQC algorithms and to prepare for smooth transition

AGENDA

01 **FIDO2**
Introduction to the FIDO2 protocol

02 **PQ-readiness of FIDO2**
Analysis of WebAuthn and CTAP

03 **E2E PQ FIDO2 OSS**
Implementation details

04 **Challenges and future work**
Additional modes to be considered in the PQ migration

AGENDA

01 **FIDO2**
Introduction to the FIDO2 protocol

02 **PQ-readiness of FIDO2**
Analysis of WebAuthn and CTAP

03 **E2E PQ FIDO2 OSS**
Implementation details

04 **Challenges and future work**
Additional modes to be considered in the PQ migration

Basic FIDO2 operation flow

User

Authenticator

Client

Relying Party

Basic FIDO2 operation flow

User

Authenticator

Client

Relying Party

User verification, e.g. provision of PIN

- Generate credential key pair

Registration of authenticators credential public key at RP

- Store credential public key

© SandboxAQ

SandboxAQ Proprietary Material

Basic FIDO2 operation flow

User

Authenticator

Client

Relying Party

User verification, e.g. provision of PIN

- Generate credential key pair

Registration of authenticators credential public key at RP

- Store credential public key

- Generate signature using credential secret key

Authentication using registered credential public key

- Verify signature using public credential key

© SandboxAQ

SandboxAQ Proprietary Material

FIDO2 with token attestation

0 Generate issuer's key pair

1 Provision of issuer's public key

1

2

Certification of attestation public key

Issuer

User

Authenticator

Client

Relying Party

- Generate credential key pair
- Attest authenticator

3 Registration of authenticators credential public key at RP using attestation

- Verify attestation
- Store credential public key

User verification, e.g. provision of PIN

- Generate signature using credential secret key

4 Authentication using registered credential public key

- Verify signature using public credential key

Remote attestation in FIDO2

None

No attestation signature

Self

Registration credentials are self-signed. No token properties are claimed.

Basic

A group of devices share the same attestation keypair.

Origin of signed attestation records is indistinguishable within the group.

Privacy / Anonymity CA

Multiple attestation keys per device (i.e. one per each server to register with).

Privacy / anonymity CA certifies attestation keys after verifying the device characteristics / identity.

Remote attestation in FIDO2

None

No attestation signature

Self

Registration credentials are self-signed. No token properties are claimed.

Basic

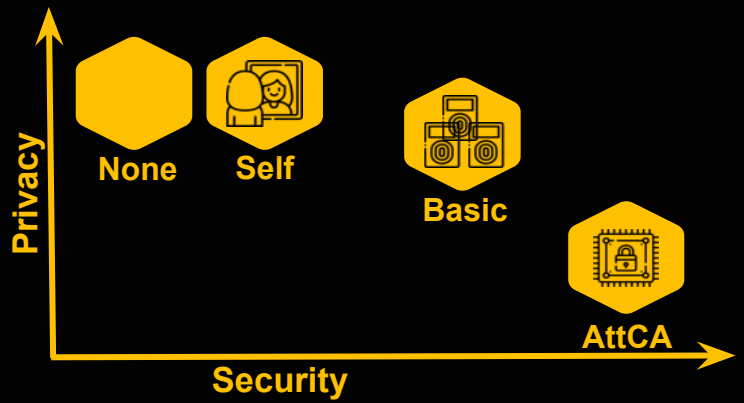
A group of devices share the same attestation keypair.

Origin of signed attestation records is indistinguishable within the group.

Privacy / Anonymity CA

Multiple attestation keys per device (i.e. one per each server to register with).

Privacy / anonymity CA certifies attestation keys after verifying the device characteristics / identity.



AGENDA

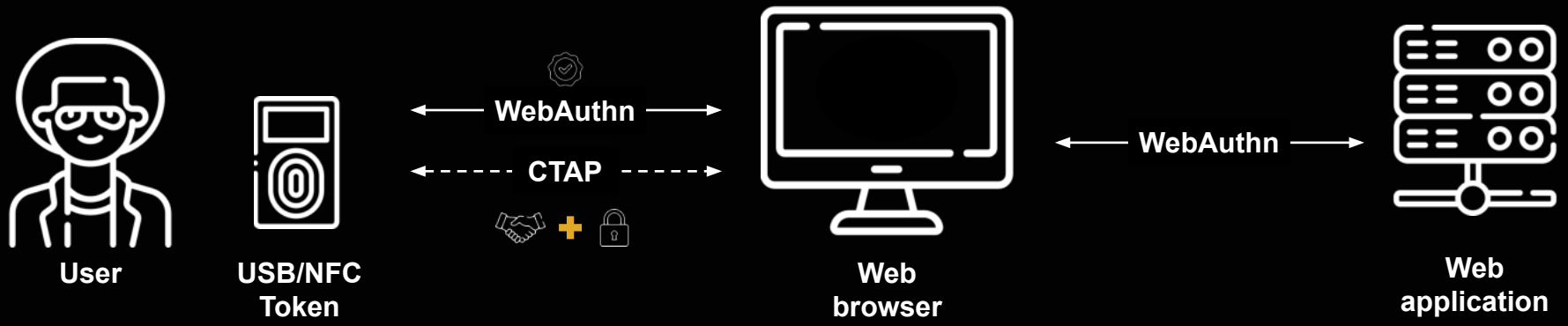
01 **FIDO2**
Introduction to the FIDO2 protocol

02 **PQ-readiness of FIDO2**
Analysis of WebAuthn and CTAP

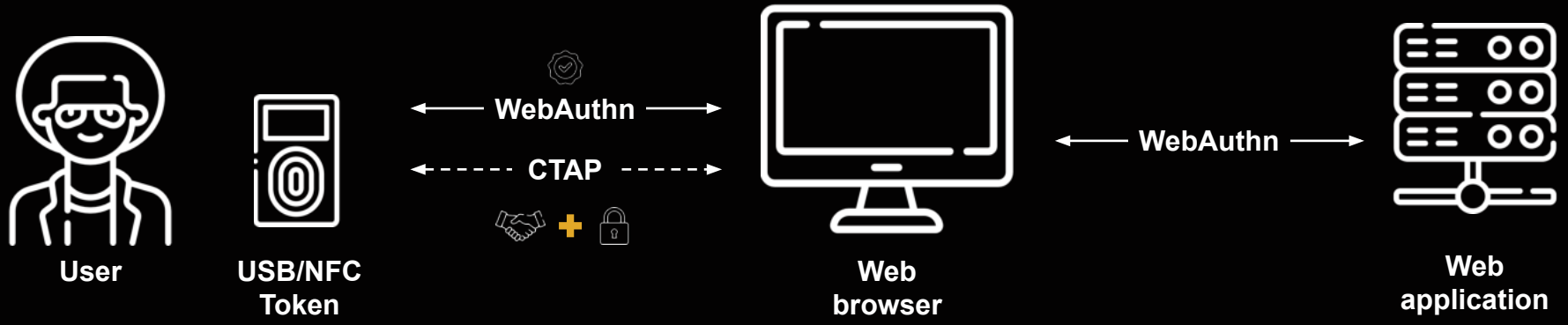
03 **E2E PQ FIDO2 OSS**
Implementation details

04 **Challenges and future work**
Additional modes to be considered in the PQ migration

FIDO2 protocol



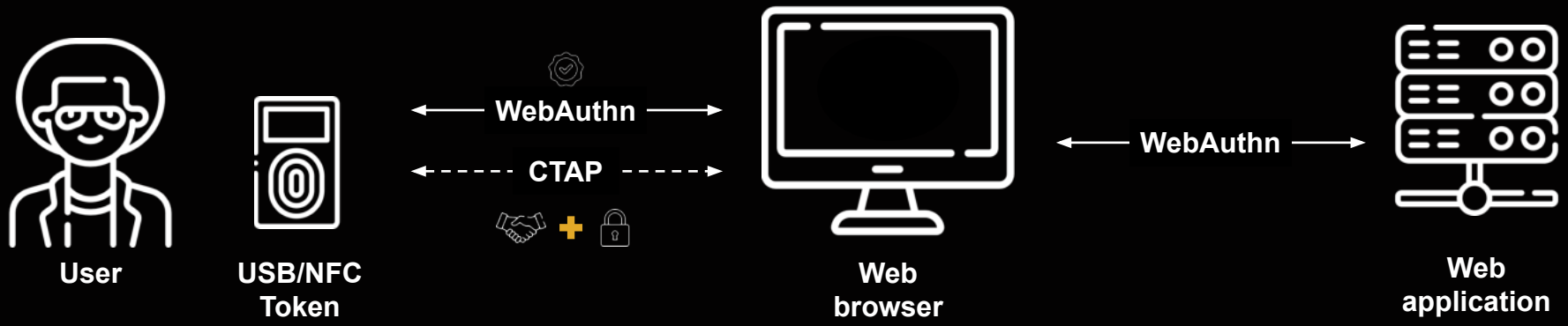
FIDO2 = WebAuthn + CTAP



WebAuthn
Sub-protocol to let the user authenticate into the web service with the hardware token

CTAP (Client To Authenticator Protocol)
Sub-protocol to make sure only a browser trusted by the user can communicate directly with the token.

Registration



- key exchange + symm. encryption
- gesture
- *(sk,vk)* generate **assertion keys**
- *att* generate attestation signature

chall, info ←

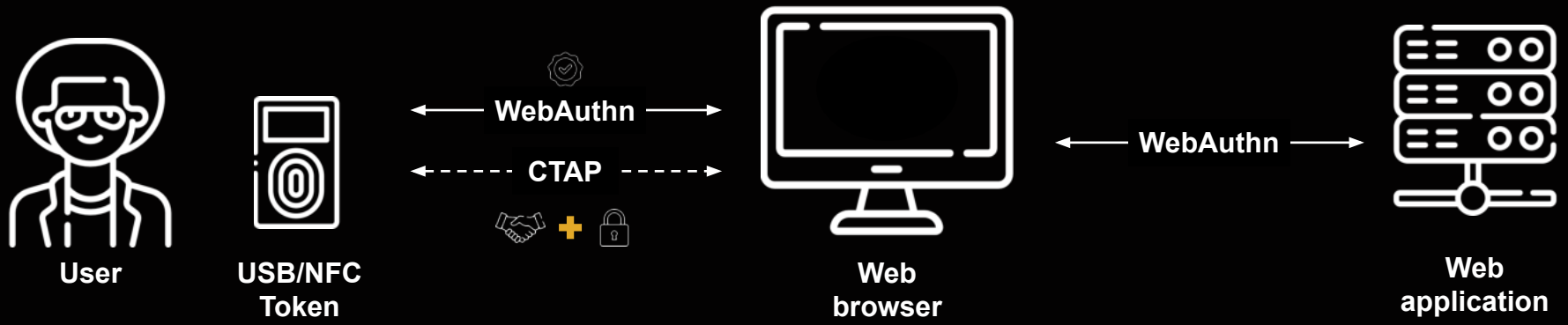
chall, info ←

vk, att, more info →

- *chall* randomly chosen
- *info* session info

- verify *info, att*
- save *vk*

Authentication



- key exchange + symm. encryption
- gesture
- ~~*(sk,vk)* generate **assertion keys**~~
- *sig* generate assertion signature

chall, info ←

chall, info ←

vk, sig, more info →

- *chall* randomly chosen
- *info* session info

- verify *info, sig*
- ~~save *vk*~~

Post-Quantum FIDO2

	WebAuthn	CTAP
PQ readiness	yes, if used signature scheme is PQ secure	yes, as DH-based CTAP subroutine can be instantiated with a KEM
PQ instantiation	• use signature algorithm negotiation of WebAuthn to include PQ/hybrid signature algorithms • use PQ signature	• use the *protocol* negotiation of CTAP 2.1 to include PQ/ hybrid KEM • use PQ KEM • increase output length hash

AGENDA

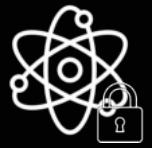
01 **FIDO2**
Introduction to the FIDO2 protocol

02 **PQ-readiness of FIDO2**
Analysis of WebAuthn and CTAP

03 **E2E PQ FIDO2 OSS**
Implementation details

04 **Challenges and future work**
Additional modes to be considered in the PQ migration

New open-source library!



Post-quantum secure, in particular using Dilithium and Kyber

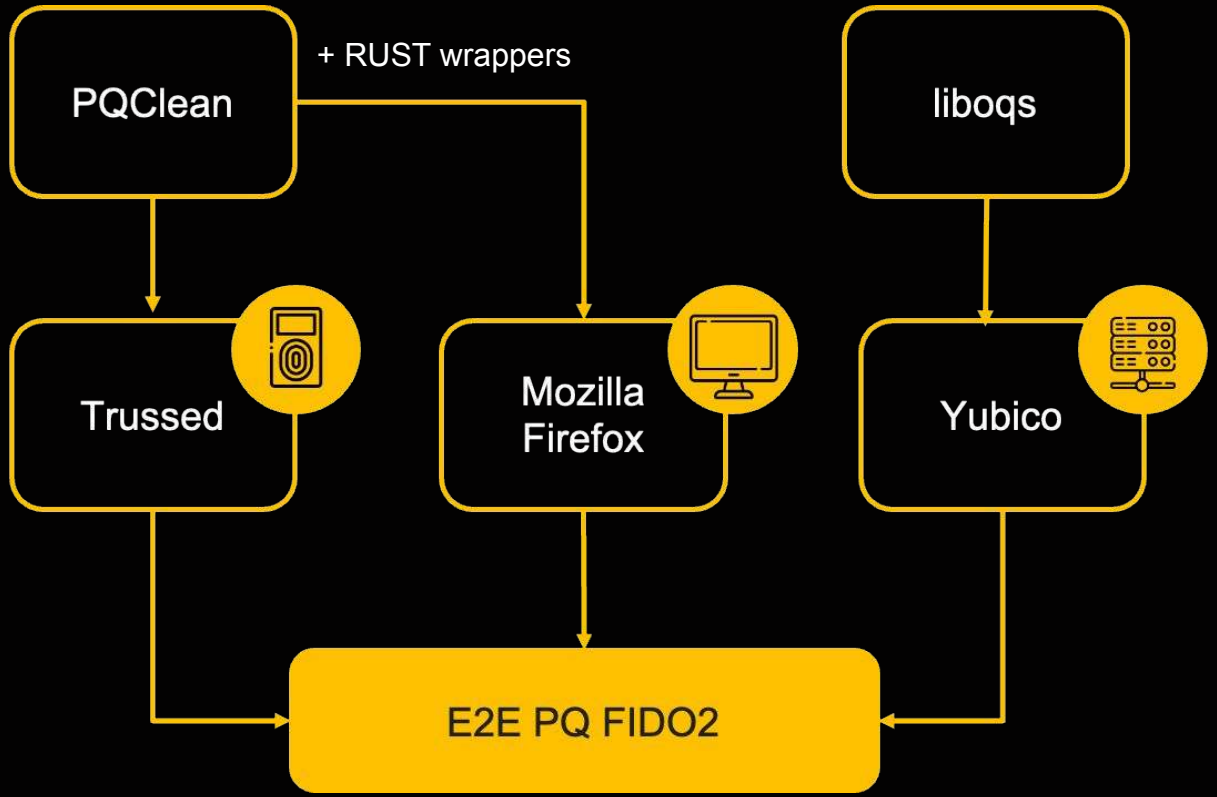
End-to-end flow is PQ secure

Open source on https://github.com/sandbox-quantum/pqc-fido2-impl

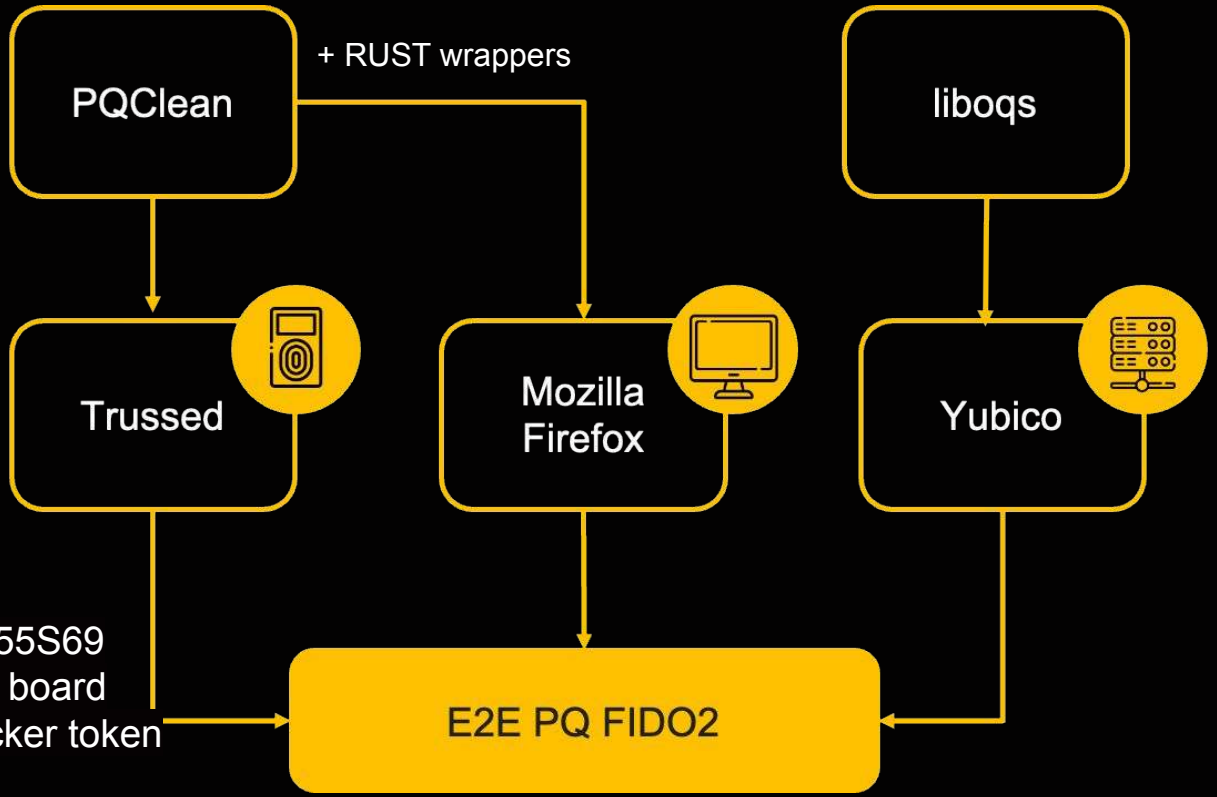
Libraries are where it all begins (Rita Dove)

Libraries are where it all begins (Rita Dove)

Libraries are where it all begins (Rita Dove)



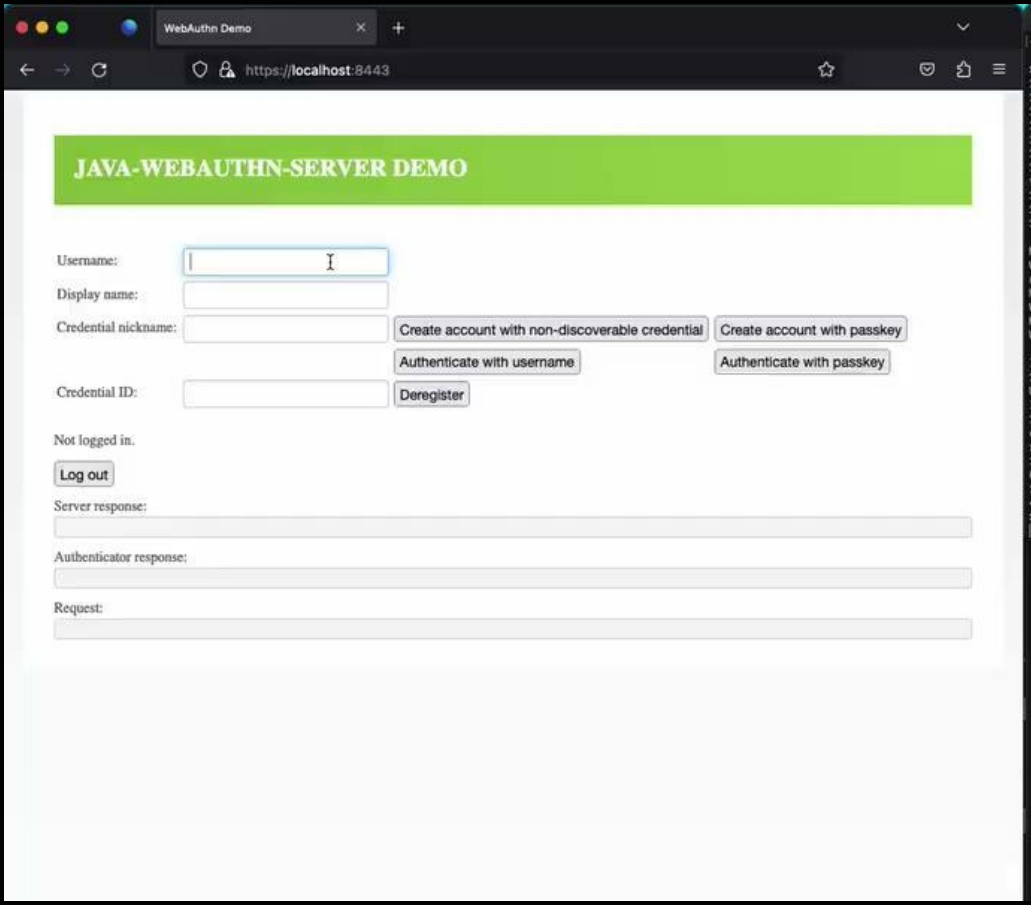
Libraries are where it all begins (Rita Dove)



Tested on

- LPCXpresso55S69 development board
- NitroKey Hacker token

PQ Extension of Yubico's Java-Webauthn-server



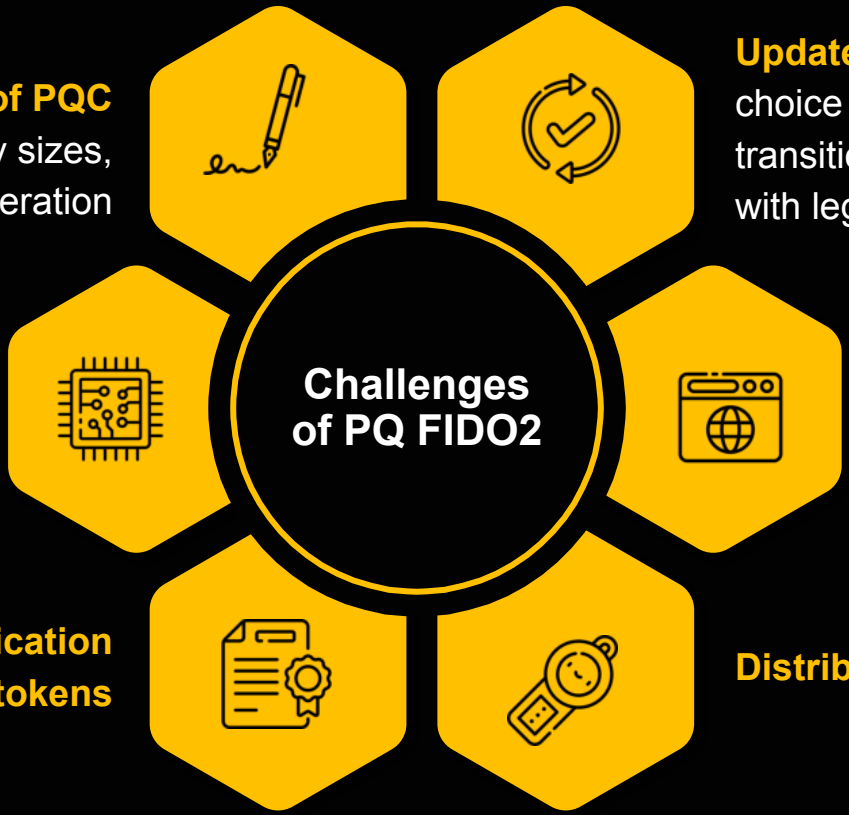
AGENDA

01 **FIDO2**
Introduction to the FIDO2 protocol

02 **PQ-readiness of FIDO2**
Analysis of WebAuthn and CTAP

03 **E2E PQ FIDO2 OSS**
Implementation details

04 **Challenges and future work**
Additional modes to be considered in the PQ migration



Efficiency of PQC
large key sizes, slower signature generation

Update FIDO2 specs
choice algorithms, smooth transition, backwards compatibility with legacy hardware, etc

Change of hardware

Update CAs, browsers and web applications

Re-certification of hardware tokens

Distribute new hardware

Summary

- First steps in migrating FIDO2 protocol to use PQC taken
- Steps ahead:
  - benchmarking of different PQ algorithms (including hybrid algorithms)
  - while considering different modes (attestation, key storage, credential synchronization, extensions)

  to guide the decision for future specs
- Get involved!

Summary

- First steps in migrating FIDO2 protocol to use PQC taken
- Steps ahead:
  - benchmarking of different PQ algorithms (including hybrid algorithms)
  - while considering different modes (attestation, key storage, credential synchronization, extensions)

  to guide the decision for future specs
- Get involved!

We are hiring!

Check out sandboxaq.com/careers

Resources

Research papers

- FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation. Bindel, Cremers, Zhao. [eprint]
- Attest or not to attest, this is the question – Provable attestation in FIDO2. Bindel et al. [eprint]

Open source implementation

- E2E PQ FIDO2 OSS using Kyber and Dilithium

Blog posts

- Is FIDO2 Ready for the Quantum Era?
- All the Things PQ – End-to-End PQ-Secure FIDO2 Protocol

Thank you!