authenticate 2024
THE FIDO CONFERENCE

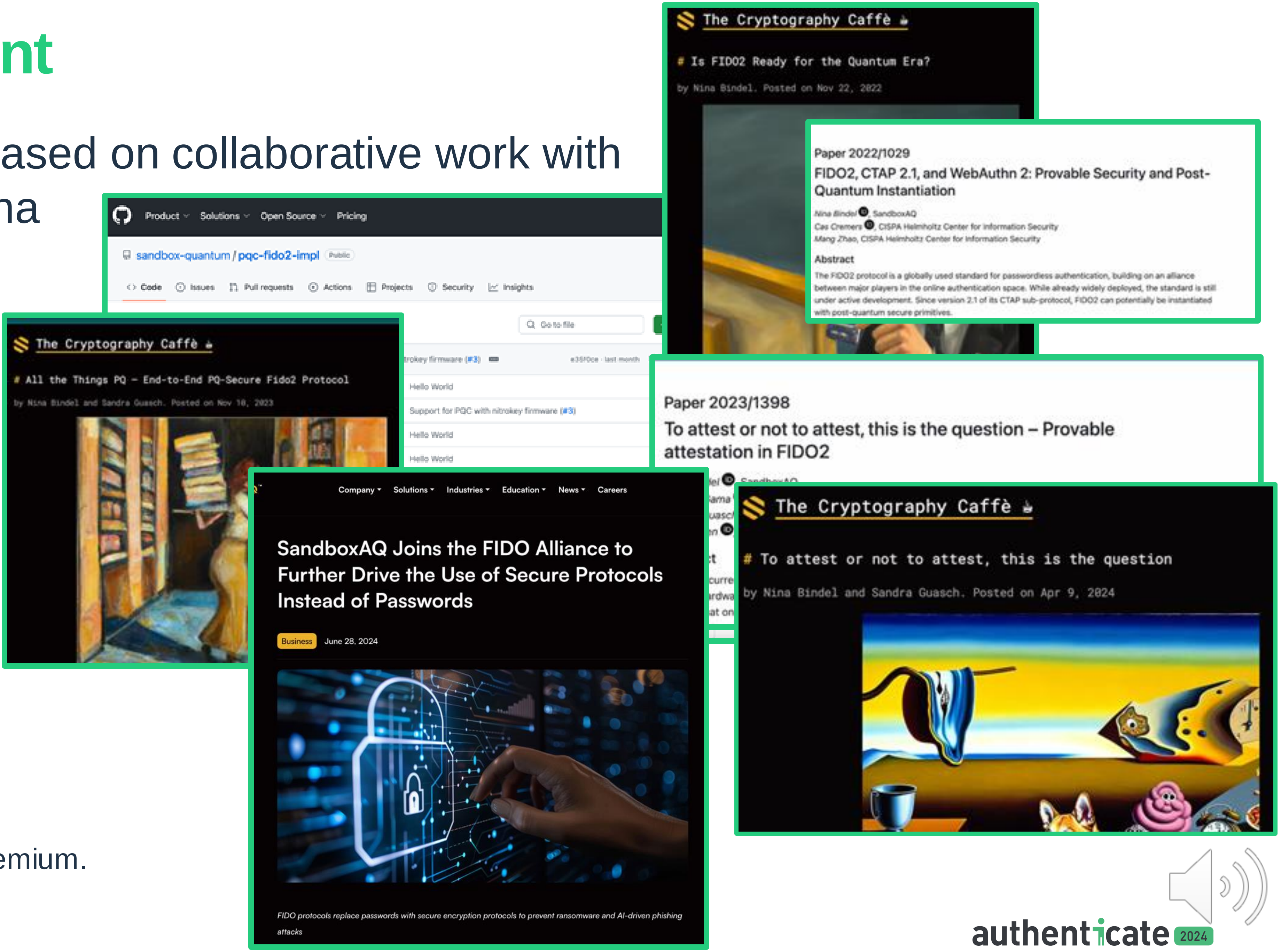
All the Things PQ – End-to-End PQ-Secure FIDO2 Protocol

Dr. Nina Bindel
Staff Research Scientist, SandboxAQ

Acknowledgment

This presentation is based on collaborative work with

Gabriel Campagna
Cas Cremers
Nicolas Gama
Sandra Guasch
James Howe
Kyle Kotowick
Duc Nguyen
Eyal Ronen
Spencer Wilson
Tarun Yadav
Mang Zhao



The Cryptography Caffè

Is FIDO2 Ready for the Quantum Era?

by Nina Bindel. Posted on Nov 22, 2022

Paper 2022/1029

FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation

Nina Bindel, SandboxAQ
Cas Cremers, CISPA Helmholtz Center for Information Security
Mang Zhao, CISPA Helmholtz Center for Information Security

Abstract

The FIDO2 protocol is a globally used standard for passwordless authentication, building on an alliance between major players in the online authentication space. While already widely deployed, the standard is still under active development. Since version 2.1 of its CTAP sub-protocol, FIDO2 can potentially be instantiated with post-quantum secure primitives.

sandbox-quantum / pqc-fido2-impl Public

Hello World
Support for PQC with nitrokey firmware (#3)
Hello World
Hello World

The Cryptography Caffè

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

by Nina Bindel and Sandra Guasch. Posted on Nov 10, 2023

Paper 2023/1398

To attest or not to attest, this is the question – Provable attestation in FIDO2

SandboxAQ Joins the FIDO Alliance to Further Drive the Use of Secure Protocols Instead of Passwords

Business June 28, 2024

FIDO protocols replace passwords with secure encryption protocols to prevent ransomware and AI-driven phishing attacks

The Cryptography Caffè

To attest or not to attest, this is the question

by Nina Bindel and Sandra Guasch. Posted on Apr 9, 2024

All icons are from flaticon premium.

AGENDA

01 The Quantum Threat and How to Mitigate it

02 The FIDO2 Cryptographic Protocol Flow

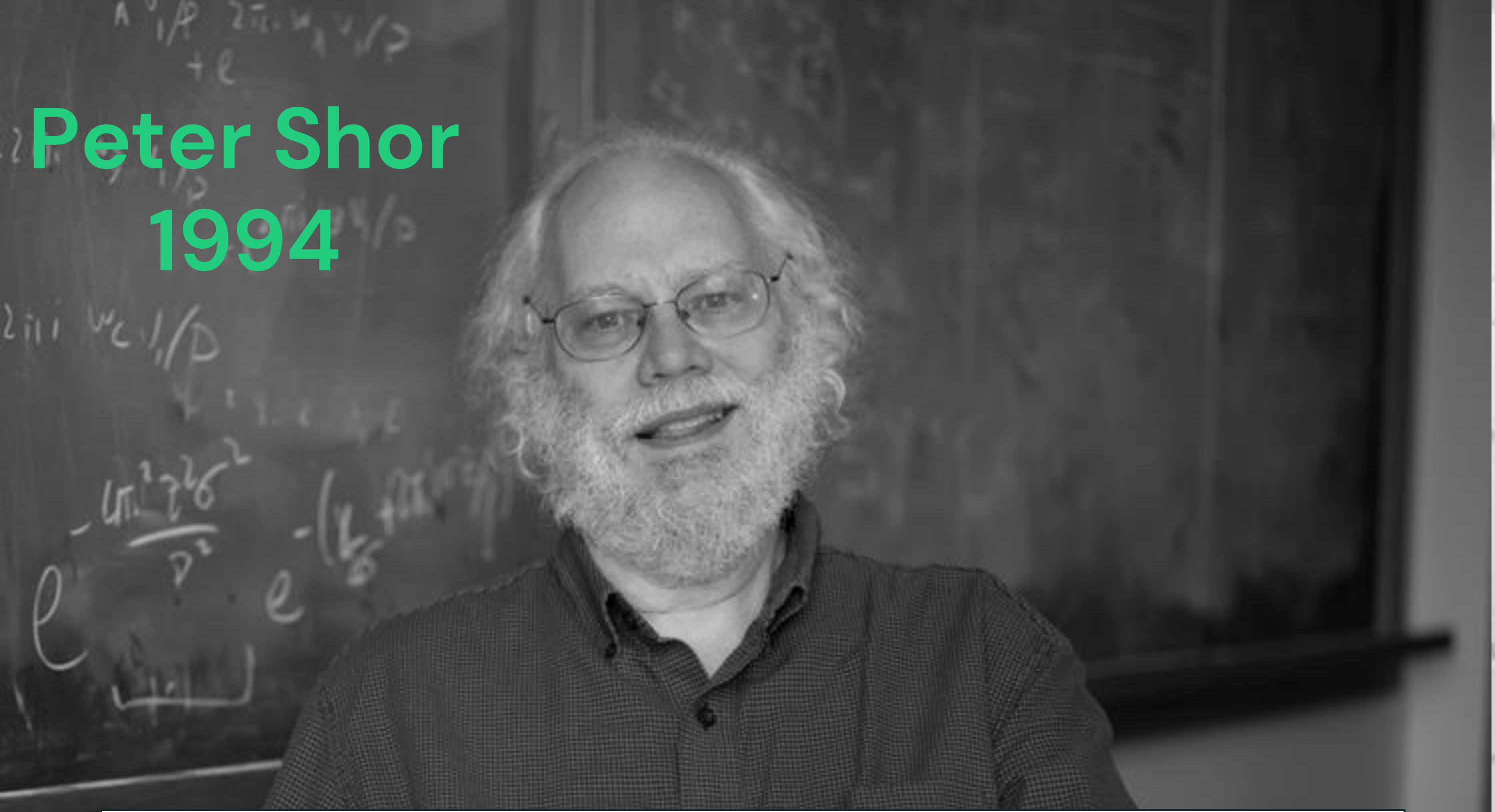
03 End-to-End Post-Quantum FIDO2 Open-Source Implementation

04 Challenges and Future Work

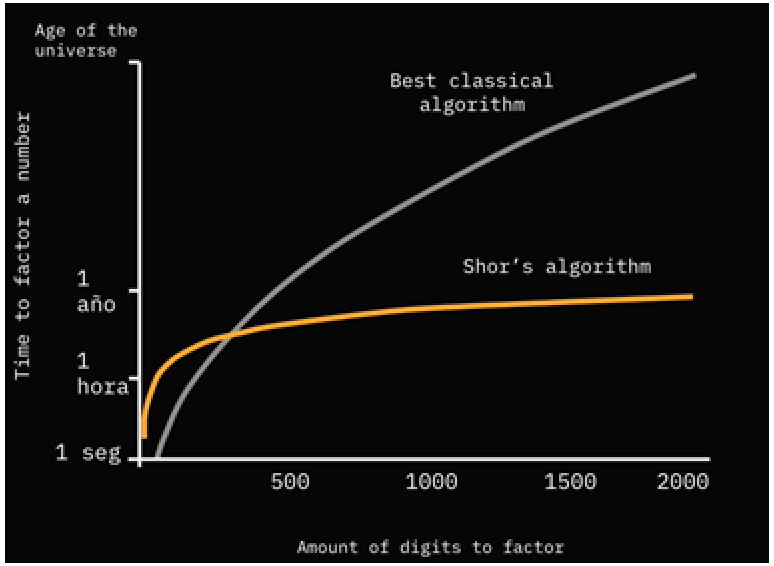
01

The Quantum Threat and How to Mitigate it

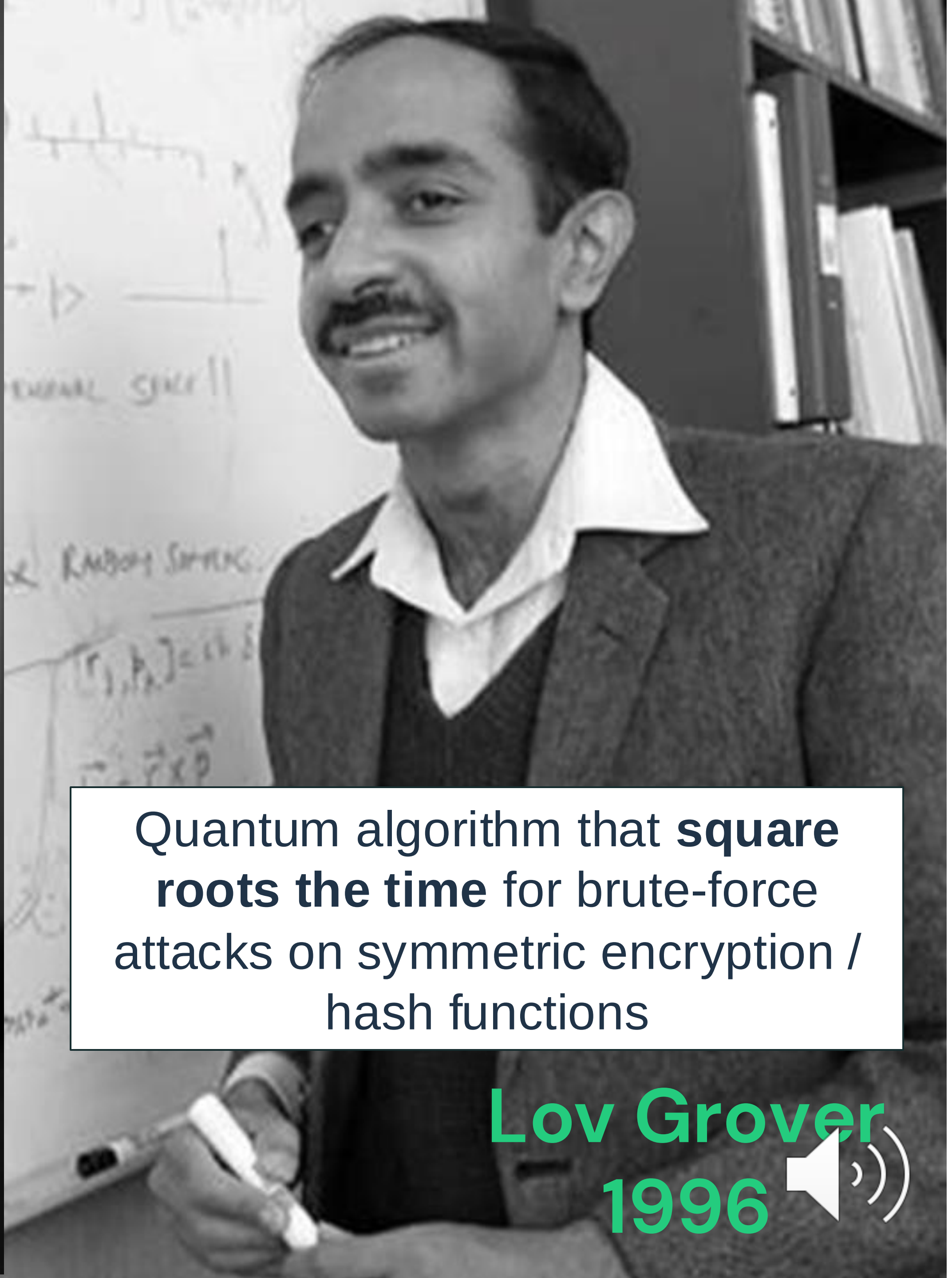
Peter Shor
1994



Quantum algorithm for **exponential speed-up** on solving RSA and DH problems

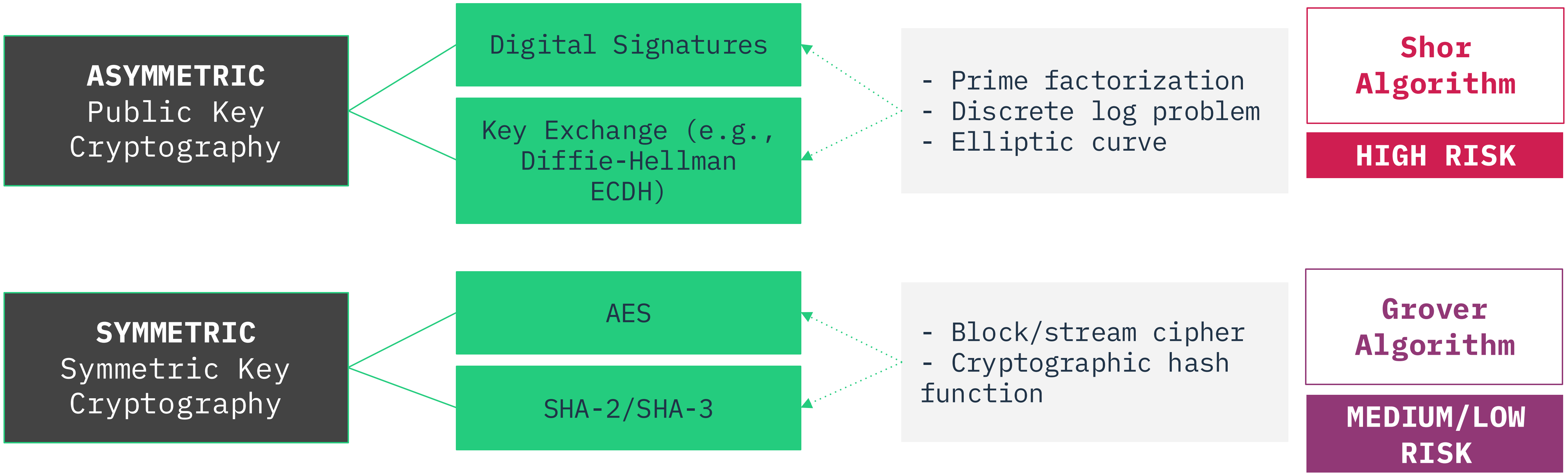


Quantum algorithm that **square roots the time** for brute-force attacks on symmetric encryption / hash functions



Lov Grover
1996

Cryptography at Risk



ASYMMETRIC
Public Key
Cryptography

Digital Signatures

Key Exchange (e.g., Diffie-Hellman ECDH)

- Prime factorization
- Discrete log problem
- Elliptic curve

Shor Algorithm

HIGH RISK

SYMMETRIC
Symmetric Key
Cryptography

AES

SHA-2/SHA-3

- Block/stream cipher
- Cryptographic hash function

Grover Algorithm

MEDIUM/LOW RISK

NIST - PQC Process #1
6 year process to select the first set of algorithms

Submissions **(2016)**	82
Accepted round 1	69
Accepted round 2	26
Accepted round 3	15
Accepted round 4	4

NIST - PQC Process #1

¡We finally have standards for PQC!

- The 5th of July 2023 NIST announced its first set of standards
- They selected **4 candidates**:
  - CRYSTALS-KYBER (**ML-KEM**): **FIPS 203** (key exchange)
  - CRYSTALS-Dilithium (**ML-DSA**): **FIPS 204** (digital signature)
  - SPHINCS+ (**SLH-DSA**): **FIPS 205** (digital signature) → **SandboxAQ Participation**
  - Falcon: *coming soon*
- Initial drafts are done (+200 pages of comments), final versions summer 2024 a priori

NIST’s Post-Quantum Cryptography Competitions

#1

2016
First PQC Competition

Key Exchange
Digital Signatures

#2

2023
Second PQC Competition

Digital Signatures

#3

Coming soon
Threshold cryptography competition

Digital Signatures
Key Exchange
PKE
Key Generation
…

(Some) challenges of PQC to existing systems

- Larger keys, signatures, ciphertexts, certificates, etc.
- Migration to new algorithms requires cryptographic agility
- Interconnected systems, dependencies
- Compatibility with legacy systems

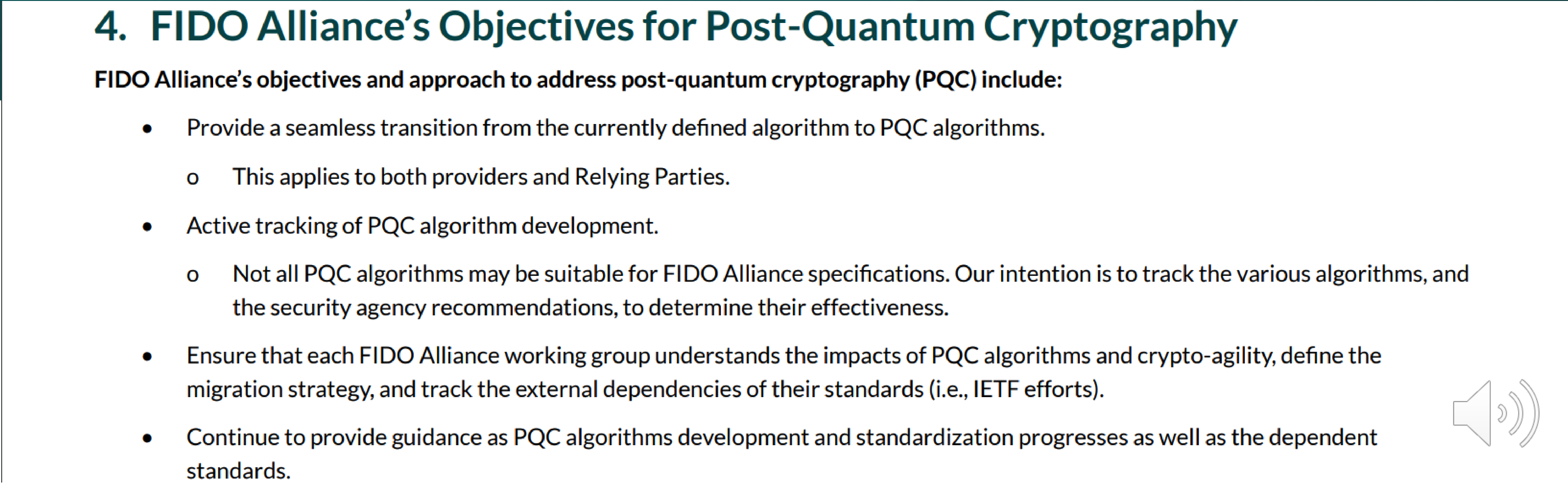
(Some) challenges of PQ authentication

Larger keys, signatures, ciphertexts, certificates, etc.	Low capacity devices (hardware tokens, smartcards, NFC, etc)
Migration to new algorithms requires cryptographic agility	Large scale of authentication systems, including end-user distribution
Interconnected systems, dependencies	Start of migration with CAs vs end-user devices
Compatibility with legacy systems	Reliance on hardware

fido ALLIANCE | simpler stronger authentication

Addressing FIDO Alliance’s Technologies in Post Quantum World

January 2024



4. FIDO Alliance’s Objectives for Post-Quantum Cryptography

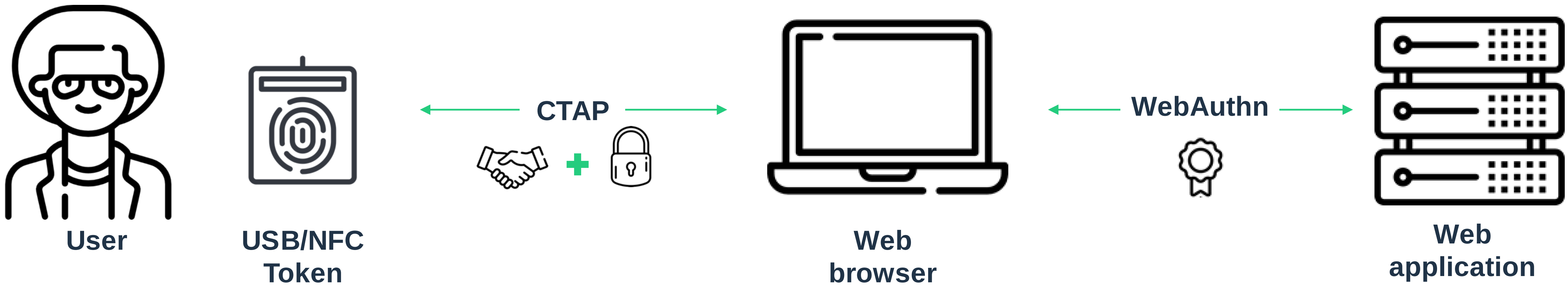
FIDO Alliance’s objectives and approach to address post-quantum cryptography (PQC) include:

- Provide a seamless transition from the currently defined algorithm to PQC algorithms.
  - This applies to both providers and Relying Parties.
- Active tracking of PQC algorithm development.
  - Not all PQC algorithms may be suitable for FIDO Alliance specifications. Our intention is to track the various algorithms, and the security agency recommendations, to determine their effectiveness.
- Ensure that each FIDO Alliance working group understands the impacts of PQC algorithms and crypto-agility, define the migration strategy, and track the external dependencies of their standards (i.e., IETF efforts).
- Continue to provide guidance as PQC algorithms development and standardization progresses as well as the dependent standards.

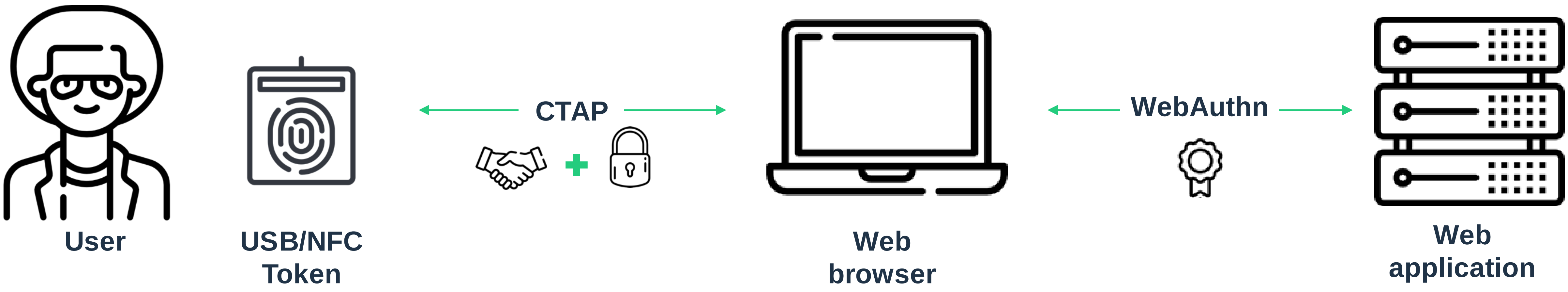
02

The FIDO2 Cryptographic Protocol Flow

FIDO2 = WebAuthn + CTAP



FIDO2 = WebAuthn + CTAP



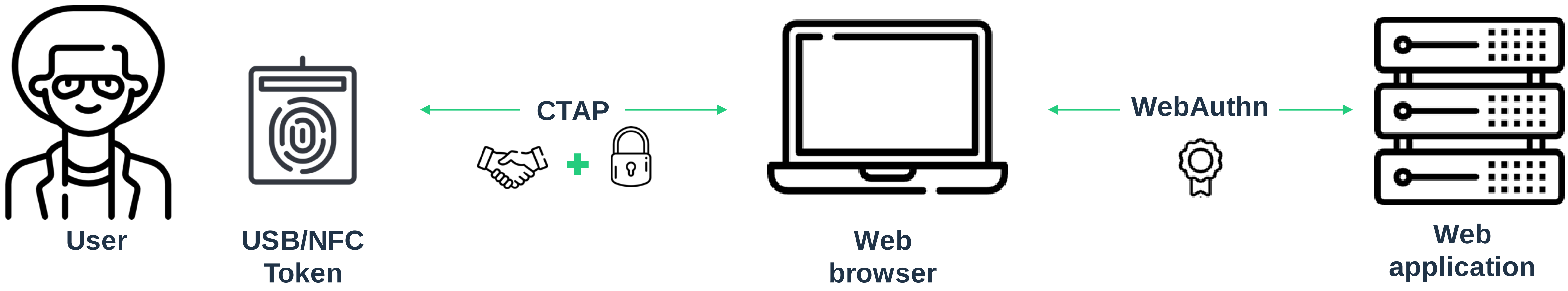
WebAuthn

Sub-protocol between the client and the server to let the user authenticate into the web service with the hardware token

CTAP (Client To Authenticator Protocol)

Sub-protocol between the token and the client to also ensure only browsers trusted by the user can communicate directly with the token

Registration



User

USB/NFC Token

CTAP

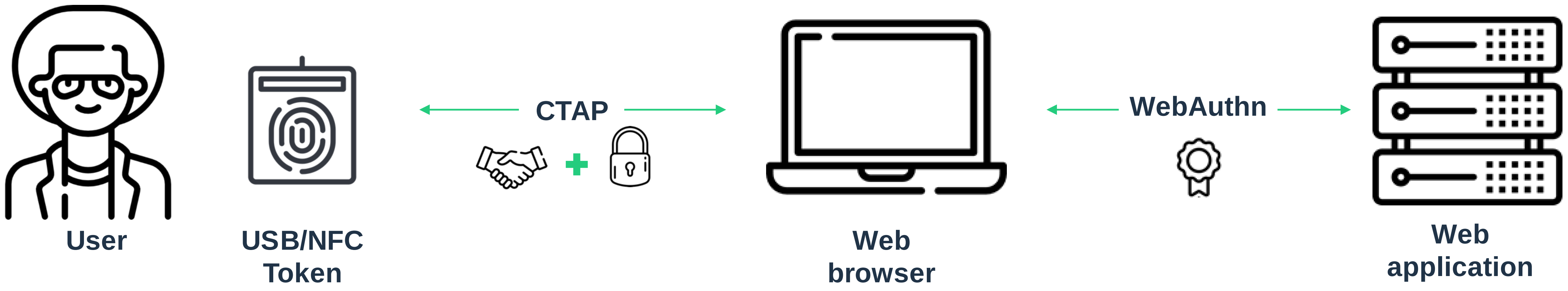
Web browser

WebAuthn

Web application

challenge random
info session info

Registration



User

USB/NFC Token

CTAP

Web browser

WebAuthn

Web application

challenge random
info session info

← *challenge, info*

← *challenge, info*

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

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

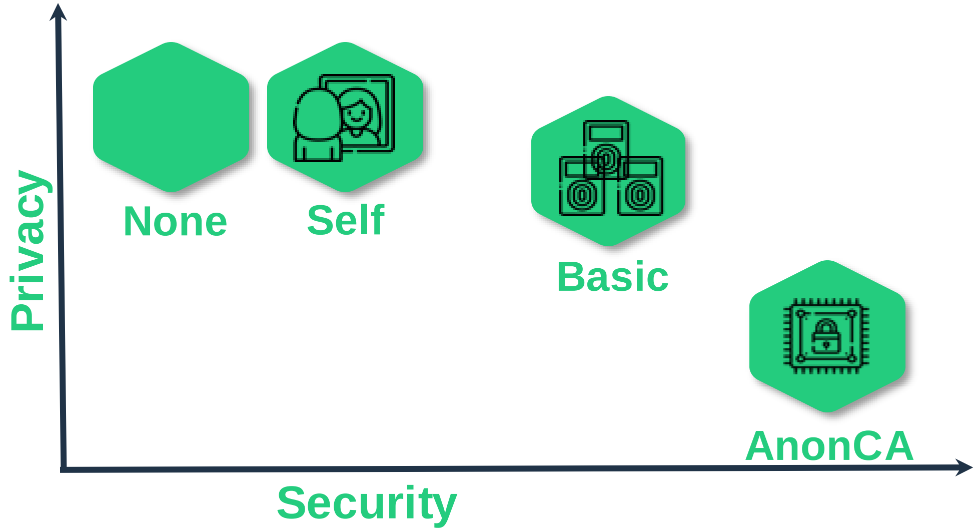
A group of devices share the same attestation keypair.

Origin of signed attestation records is indistinguishable within the group.

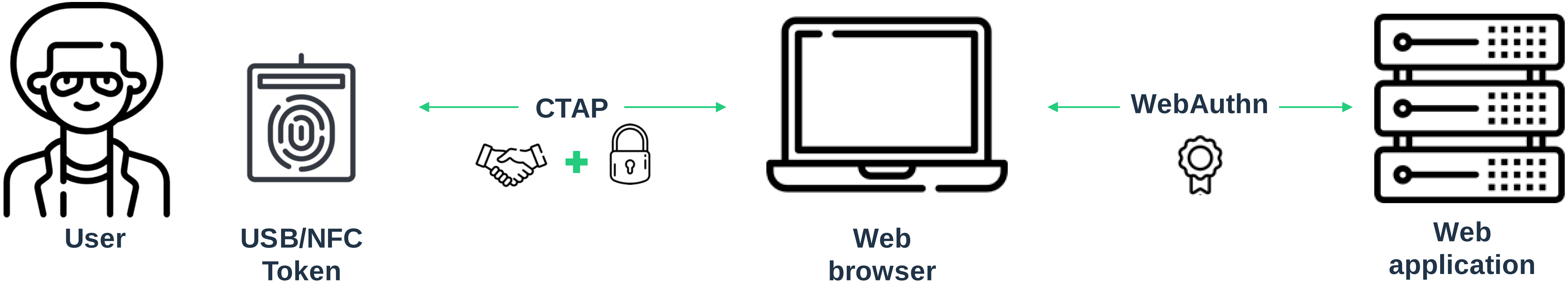
Privacy / Anonymity CA

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.



Registration



User

USB/NFC Token

CTAP

Web browser

WebAuthn

Web application

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

← *challenge, info*

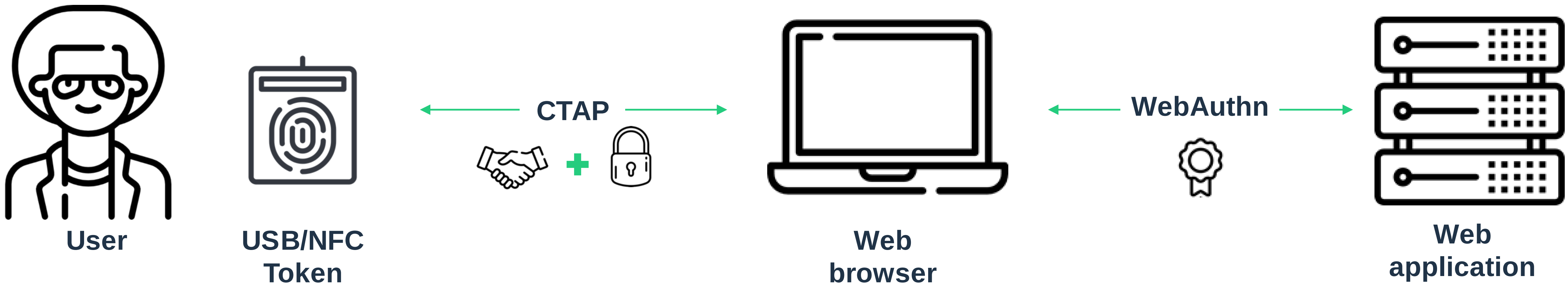
← *challenge, info*

challenge random
info session info

vk, att, more info →

verify *info, att*
save *vk*

Authentication



User

USB/NFC Token

CTAP

Web browser

WebAuthn

Web application

challenge random
info session info

← *challenge, info*

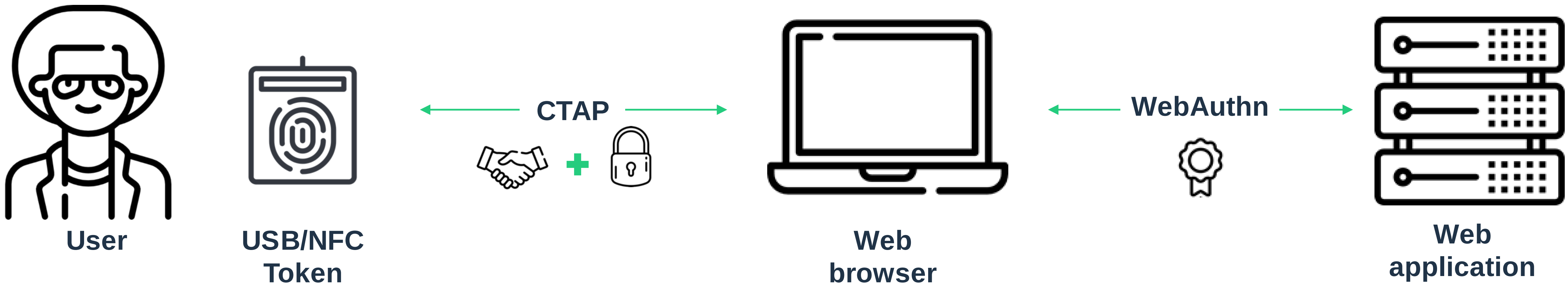
← *challenge, info*

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

~~*vk,*~~ *sig, more info* →

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

Quantum threat



User

USB/NFC Token

CTAP

Web browser

WebAuthn

Web application

challenge random
info session info

← *challenge*, *info*

← *challenge*, *info*

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

~~*vk*,~~ *sig*, *more info* →

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

Theoretical Analysis of FIDO2's Post-Quantum Security

PQ readiness

Yes,
if **signature scheme** is **PQ secure** and if **DH-based CTAP subroutine** is instantiated with a **(PQ) KEM**.

PQ instantiation

- Use PQ signature and PQ KEM.
- Increase output length of hash functions.
- Use negotiation in WebAuthn to include PQ/hybrid signature algorithms.
- Use negotiation in CTAP 2.1 to include PQ/hybrid KEM.

Theoretical Analysis of FIDO2’s Post-Quantum Security

PQ readiness

Yes,
if **signature scheme** is **PQ secure** and if **DH-based CTAP subroutine** is instantiated with a **(PQ) KEM**.

PQ instantiation

- Use PQ signature and PQ KEM.
- Increase output length of hash functions.
- Use negotiation in WebAuthn to include PQ/hybrid signature algorithms.
- Use negotiation in CTAP 2.1 to include PQ/hybrid KEM.

Backwards Compatibility

- Cryptographic negotiations between User and Web Service similar to TLS.
- Ensures backwards compatibility with legacy systems.

03

E2E PQ FIDO2 OSS

Implementation details

Post-quantum secure, in particular using Dilithium and Kyber

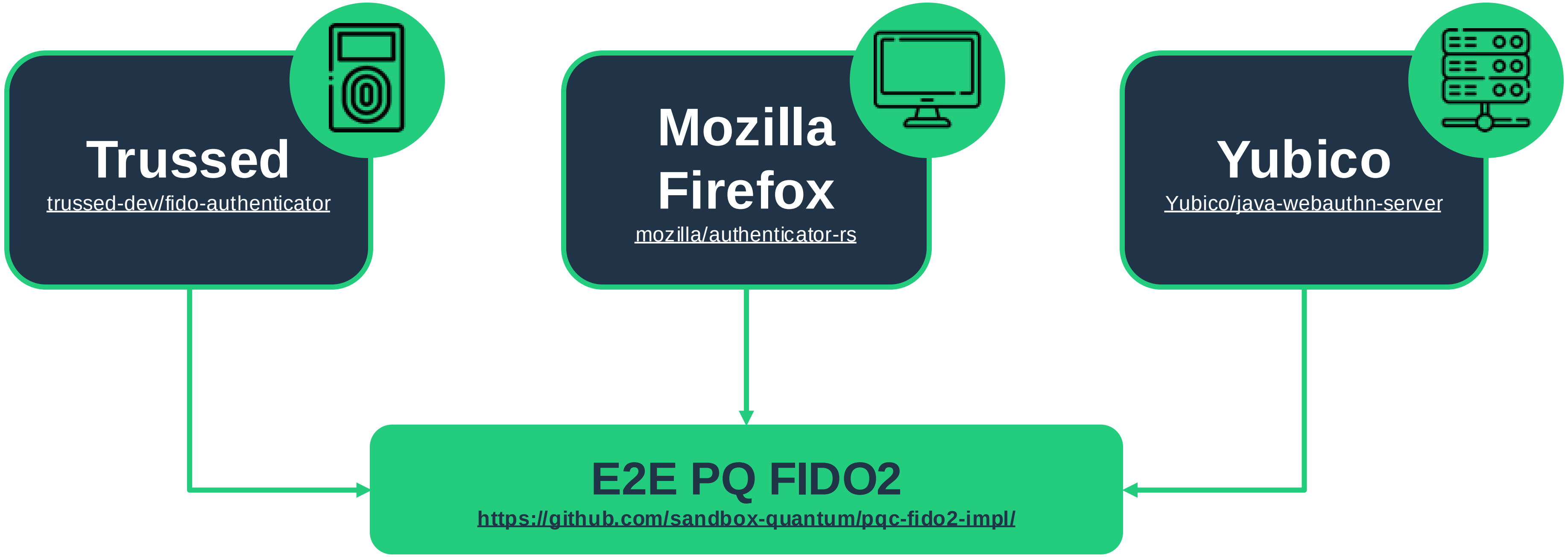
End-to-end flow is PQ secure

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

E2E PQ FIDO2

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

“Libraries are where it all begins” – Rita Dove



Trussed

trussed-dev/fido-authenticator

Mozilla Firefox

mozilla/authenticator-rs

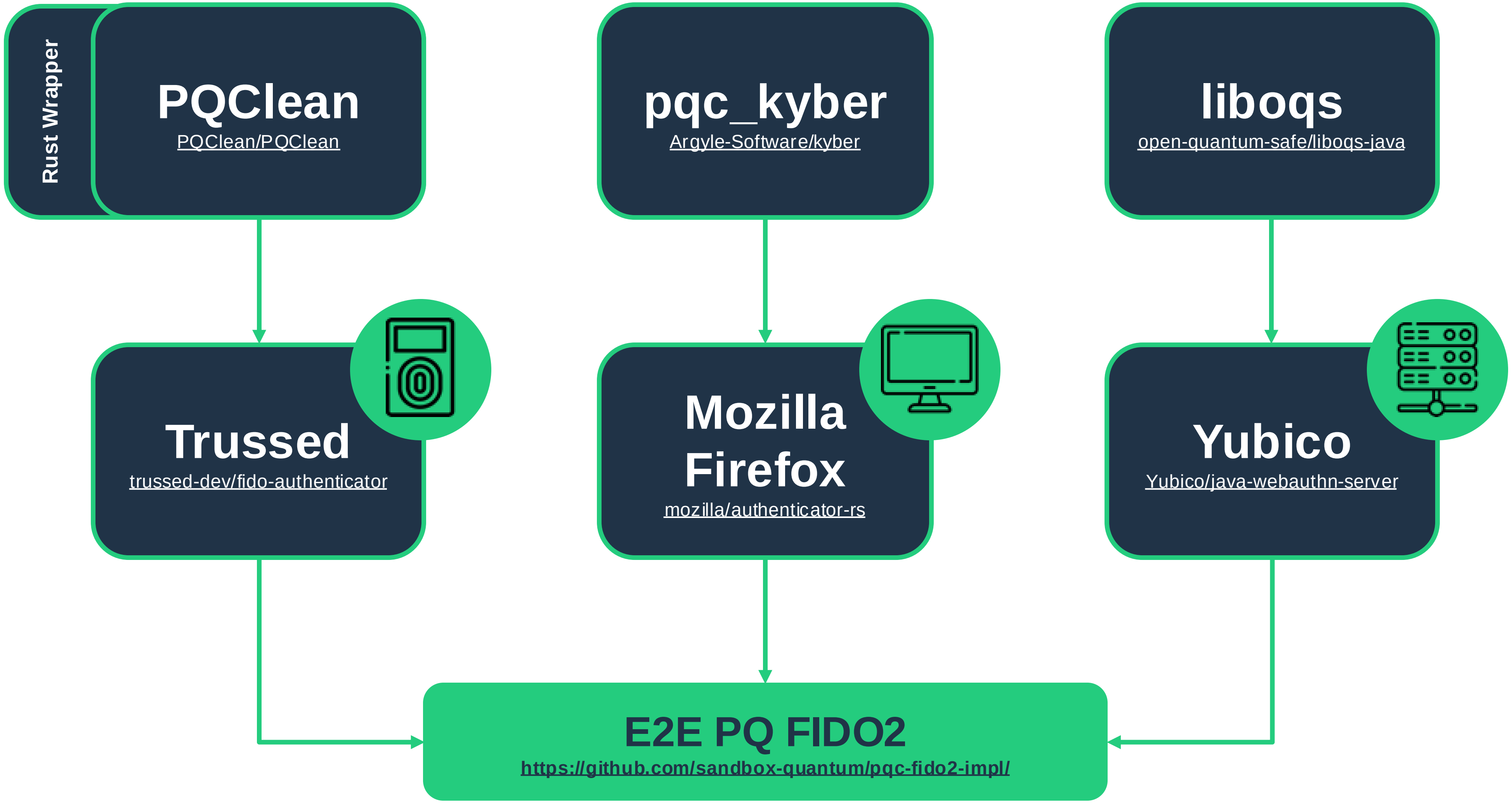
Yubico

Yubico/java-webauthn-server

E2E PQ FIDO2

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

“Libraries are where it all begins” – Rita Dove



Rust Wrapper

PQClean
PQClean/PQClean

pqc_kyber
Argyle-Software/kyber

liboqs
open-quantum-safe/liboqs-java

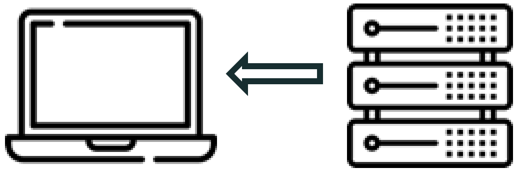
Trussed
trussed-dev/fido-authenticator

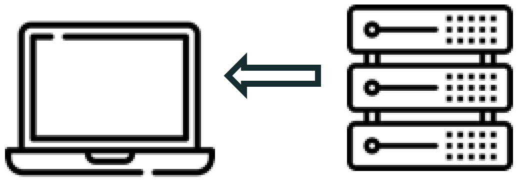
Mozilla Firefox
mozilla/authenticator-rs

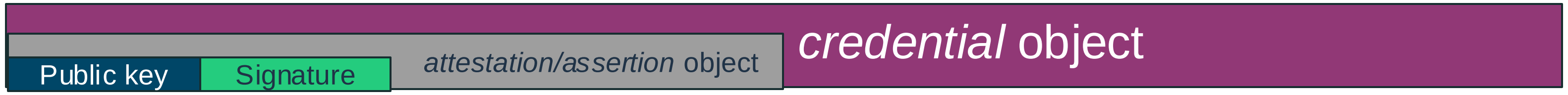
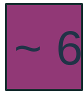
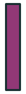
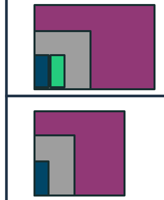
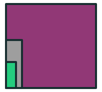
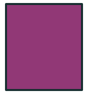
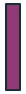
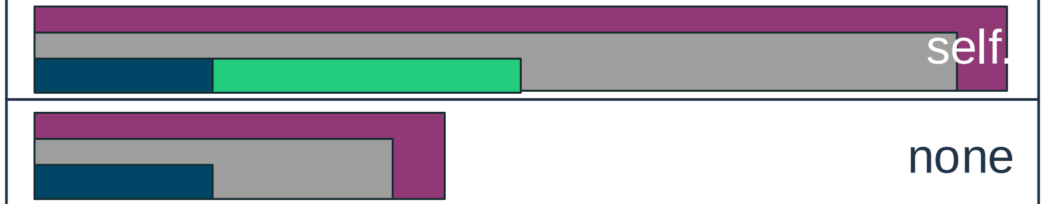
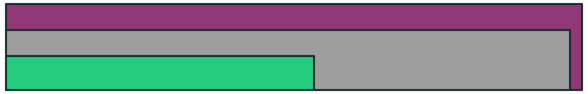
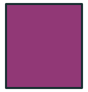
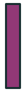
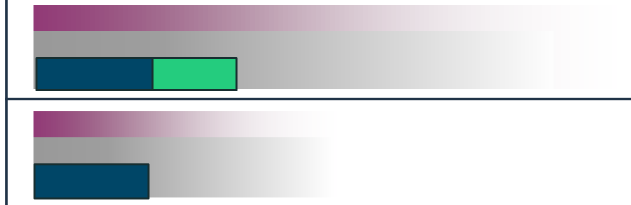
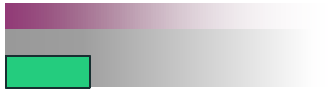
Yubico
Yubico/java-webauthn-server

E2E PQ FIDO2
https://github.com/sandbox-quantum/pqc-fido2-impl/

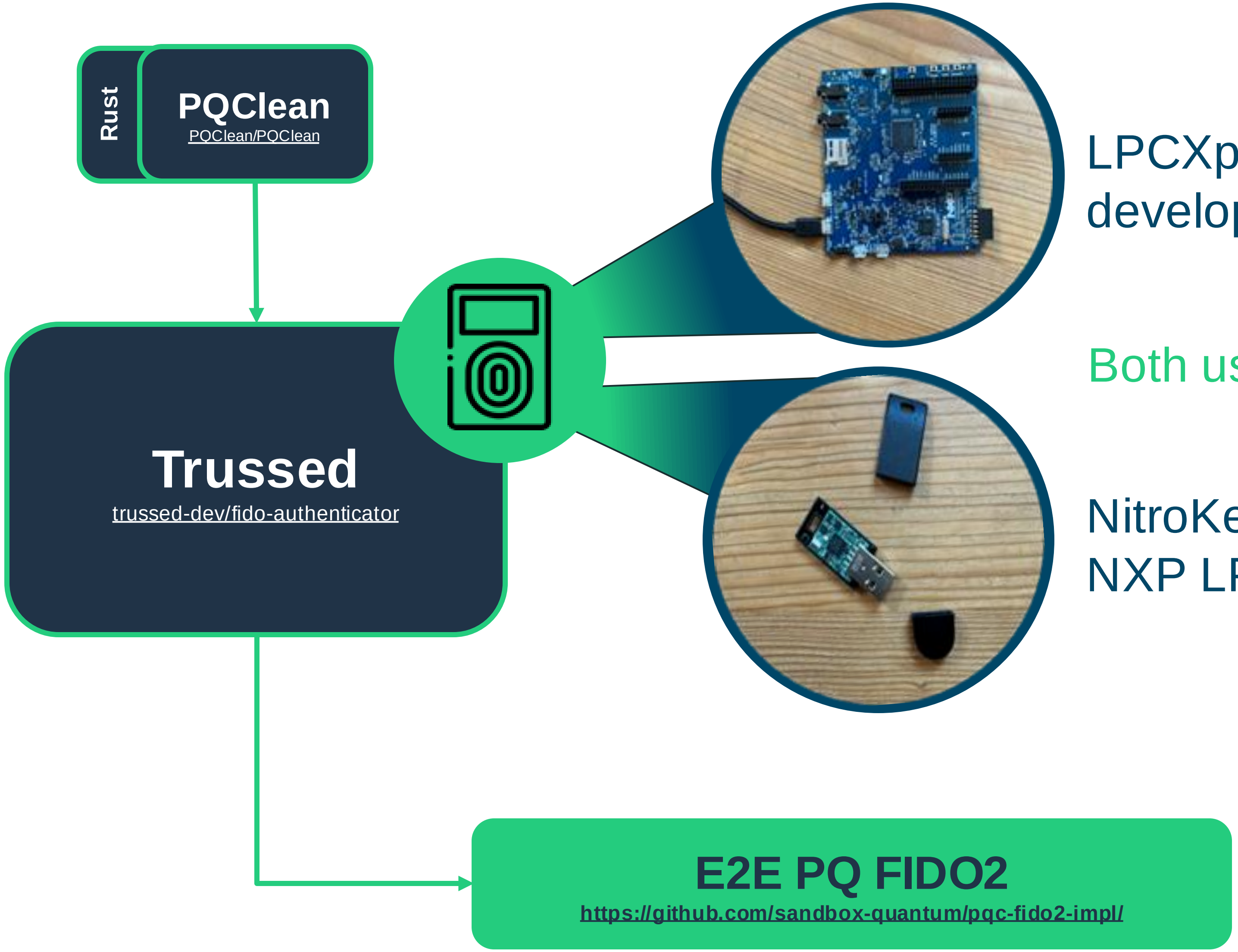
Object sizes of PQ WebAuthn





Algorithm	PQ	*option* object		 Public key Signature *attestation/assertion* object *credential* object	
		reg.	auth.	registration	authentication
ECDSA256 (observed)	👎	 ~ 600	 94	 self attestation no attestation	
Dilithium-3 (observed)	👍			 self. none	
Falcon-512 (planned)	👍			 self none	

“Libraries are where it all begins” – Rita Dove



Rust

PQClean

PQClean/PQClean

Trussed

trussed-dev/fido-authenticator

E2E PQ FIDO2

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

LPCXpresso55S69 development board

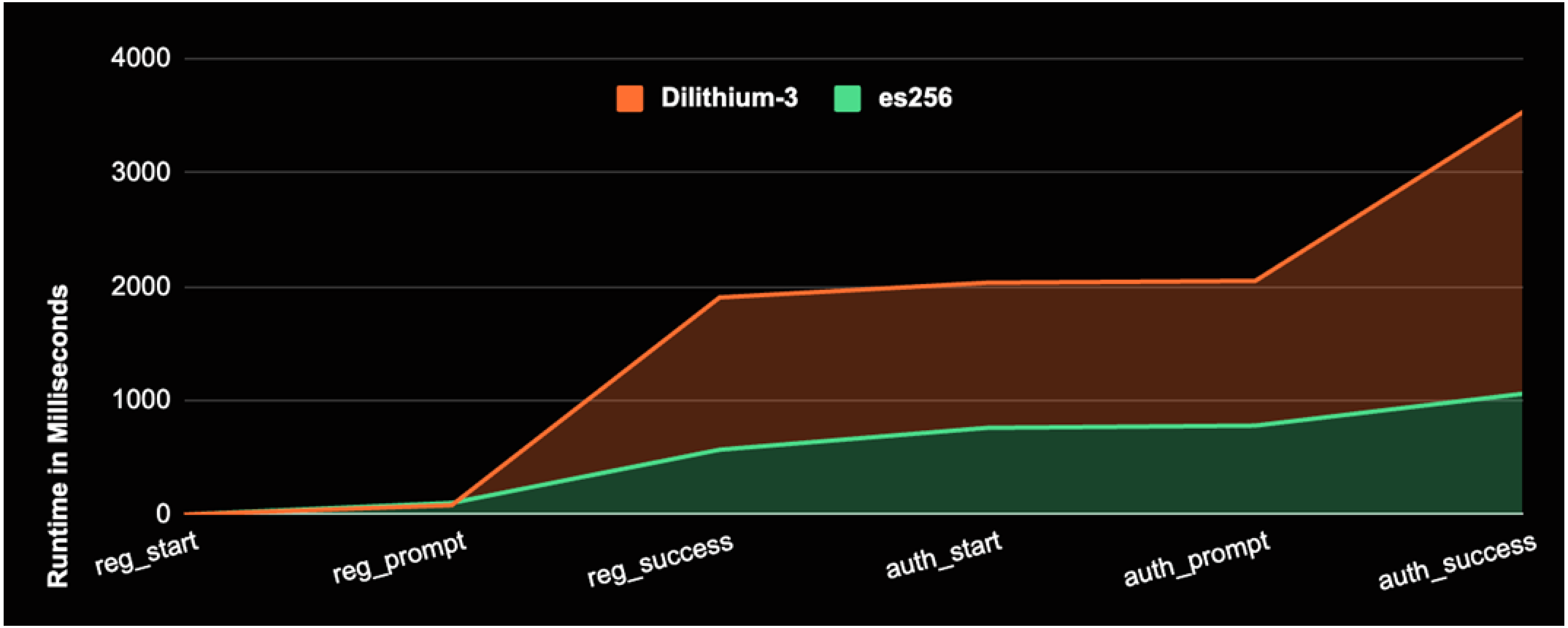
↑

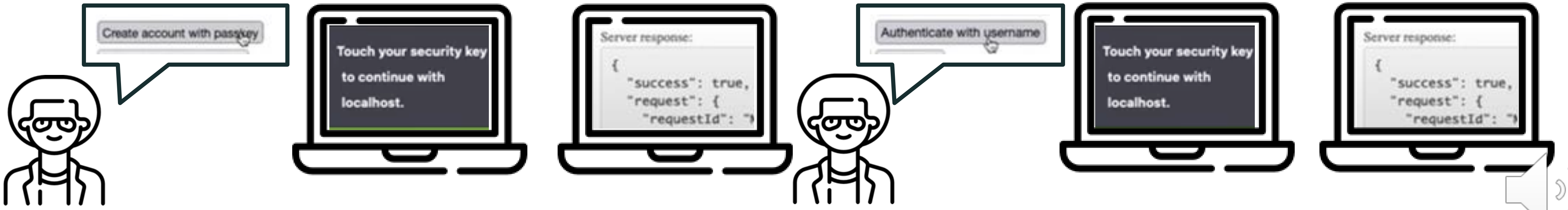
Both use ARM Cortex-M33 or similar

↓

NitroKey Hacker token with NXP LPC55S69JEV98

Performance of PQ WebAuthn




Create account with passkey

Touch your security key to continue with localhost.

Server response:

```
{
  "success": true,
  "request": {
    "requestId": "
```

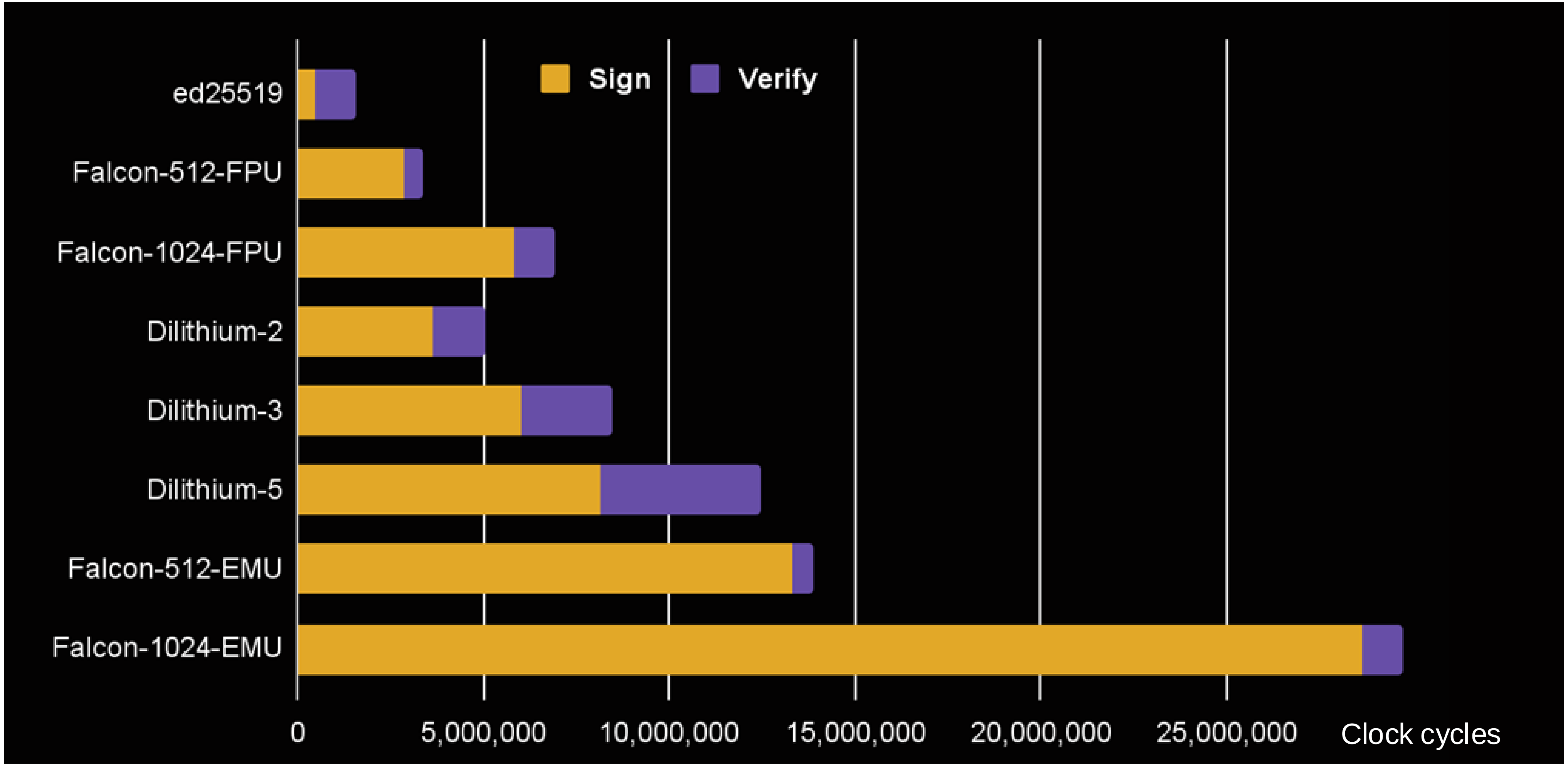
Authenticate with username

Touch your security key to continue with localhost.

Server response:

```
{
  "success": true,
  "request": {
    "requestId": "
```

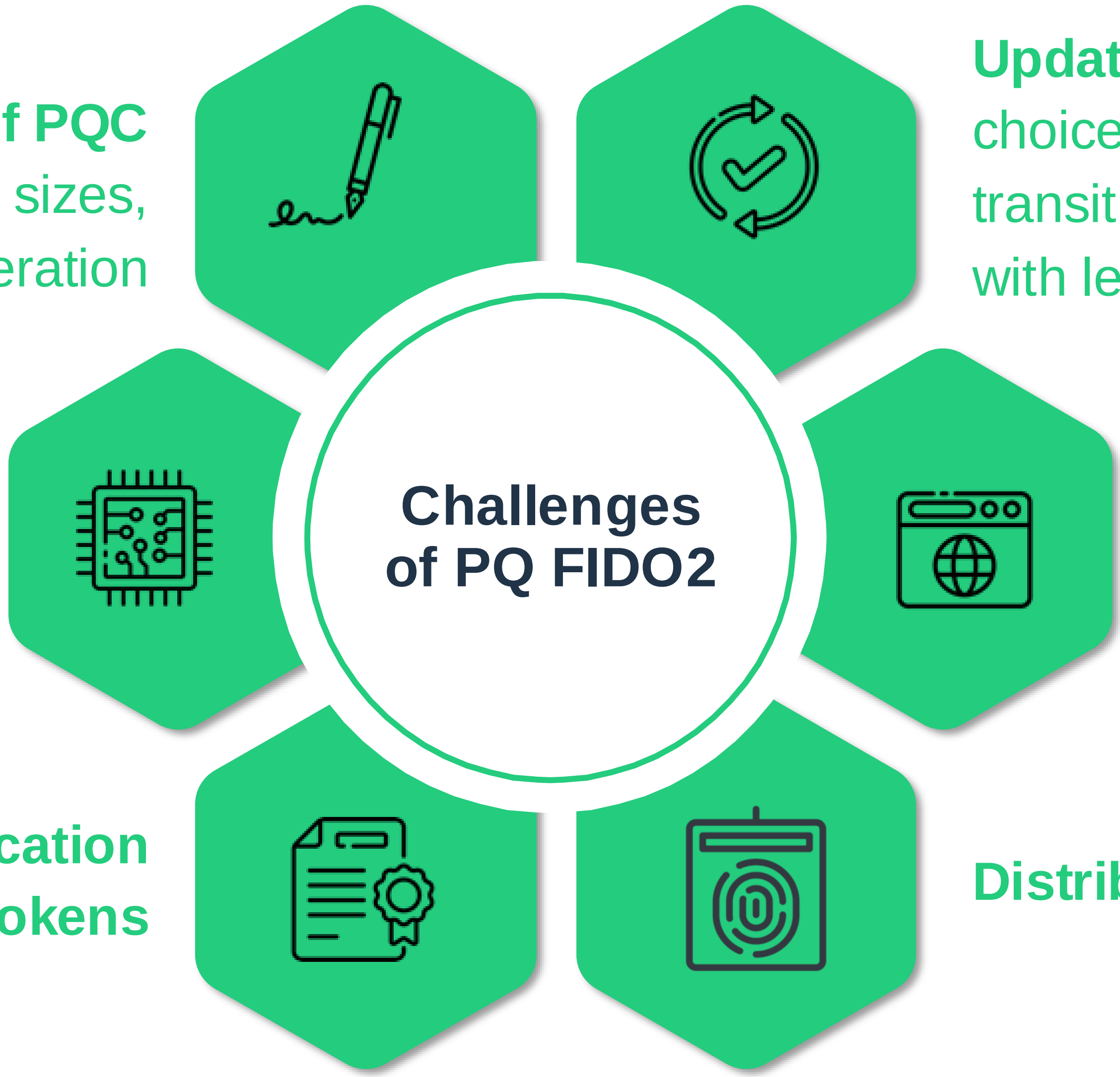
Comparing Signature Schemes on ARM Cortex M7



https://eprint.iacr.org/2022/405

04

Challenges and future work



Challenges of PQ FIDO2

Efficiency of PQC
large key sizes,
slower signature generation

Update FIDO2 specs
choice of 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 to guide the decision for future specs:
  - benchmarking different PQ algorithms (including hybrid).
  - while considering different modes (attestation, key storage, credential synchronization, extensions).
- Get involved!

authenticate 2024

THE FIDO CONFERENCE

Summary

- First steps in migrating FIDO2 protocol to use PQC taken
- Steps ahead to guide the decision for future specs:
  - benchmarking different PQ algorithms (including hybrid)
  - while considering different modes (attestation, key storage, credential synchronization, extensions)
- Get involved!

We are hiring

Check out sandboxaq.com/careers

Signature Sponsors:

Cisco | Microsoft | yubico | Google

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?
- End-to-End PQ-Secure FIDO2 Protocol
- To attest or not to attest, this is the question
- SandboxAQ joins the FIDO Alliance

Thank you

authenticatecon.com