



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

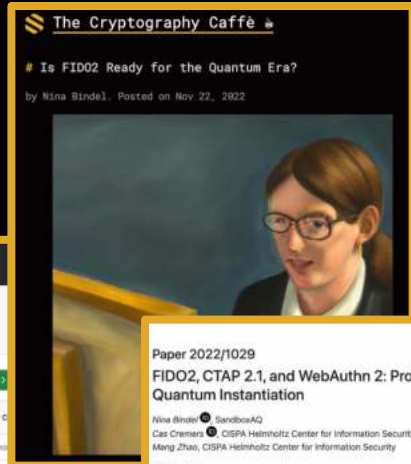
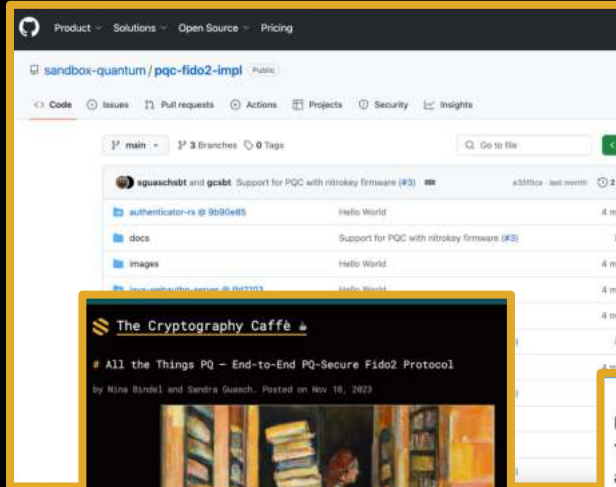
Nina Bindel, Staff Researcher
Open Source Cryptography Workshop
March 28, 2024

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.

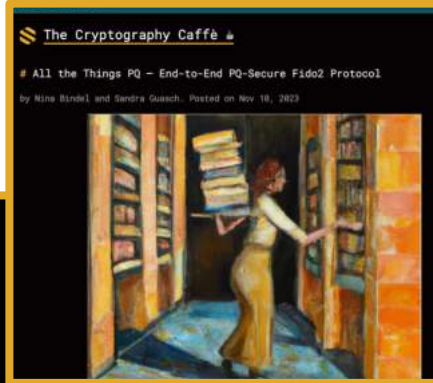


Paper 2022/1029
FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation

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.



Paper 2023/1398

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

Nina Bindel, SandboxAQ
Nicolas Gama, SandboxAQ
Sandra Guasch, SandboxAQ
Eyal Ronen, Tel Aviv University

Abstract

FIDO2 is currently the main initiative for passwordless authentication in web servers. It mandates the use of secure hardware authenticators to protect the authentication protocol's secrets from compromise. However, to ensure that only secure authenticators are being used, web servers need a method to attest their properties.



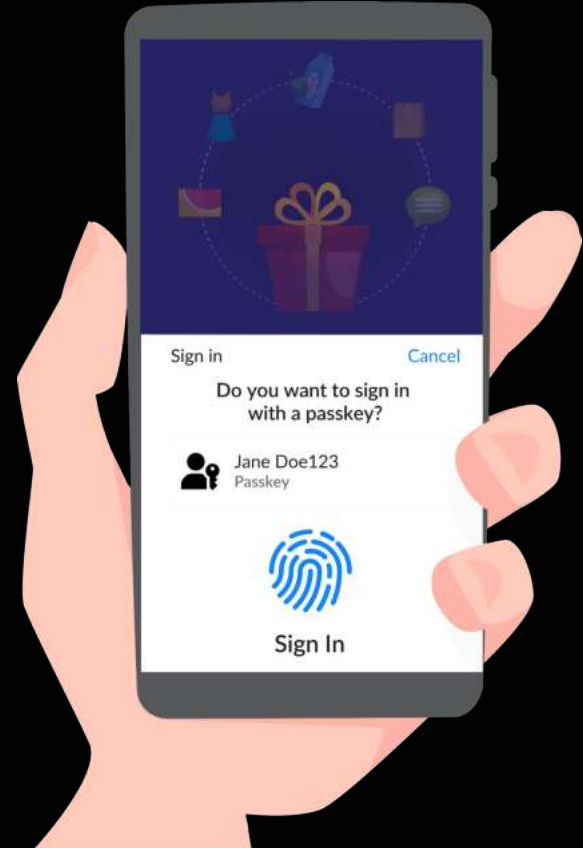
Comprised by more than **40 key companies**, including Amazon, Apple, Google, Intel, Microsoft, RSA, VISA, and Yubico

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

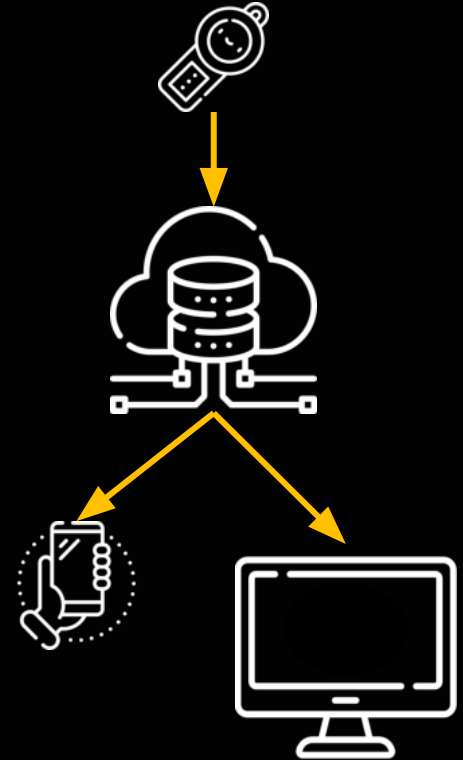
2022

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



Authenticator

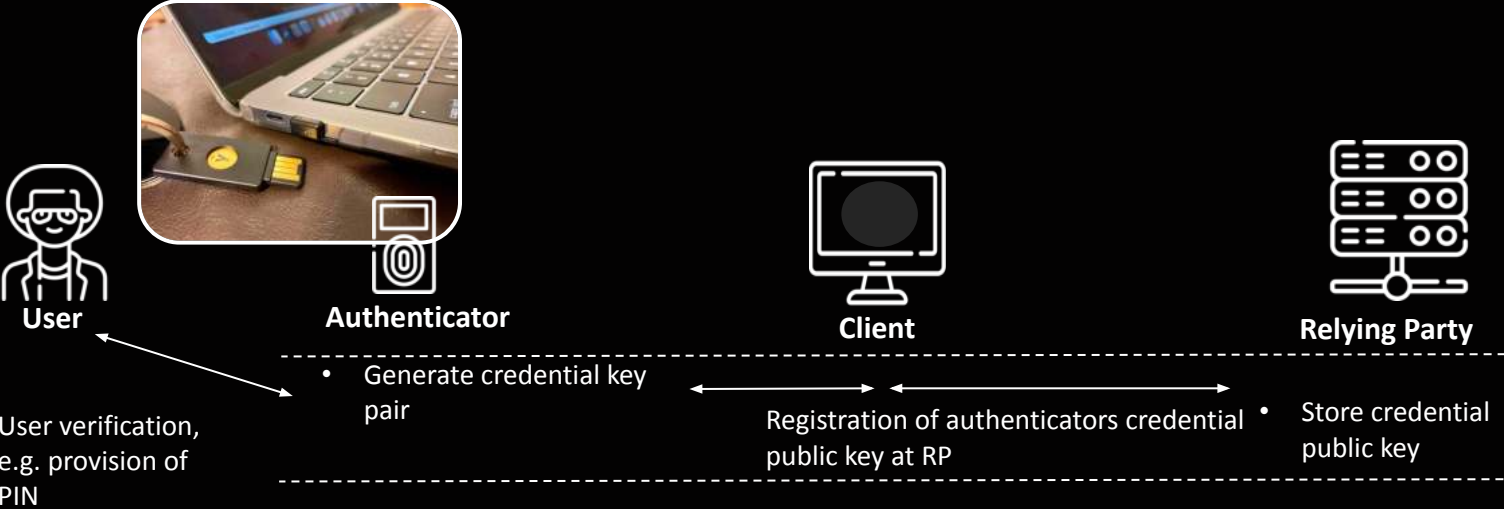


Client

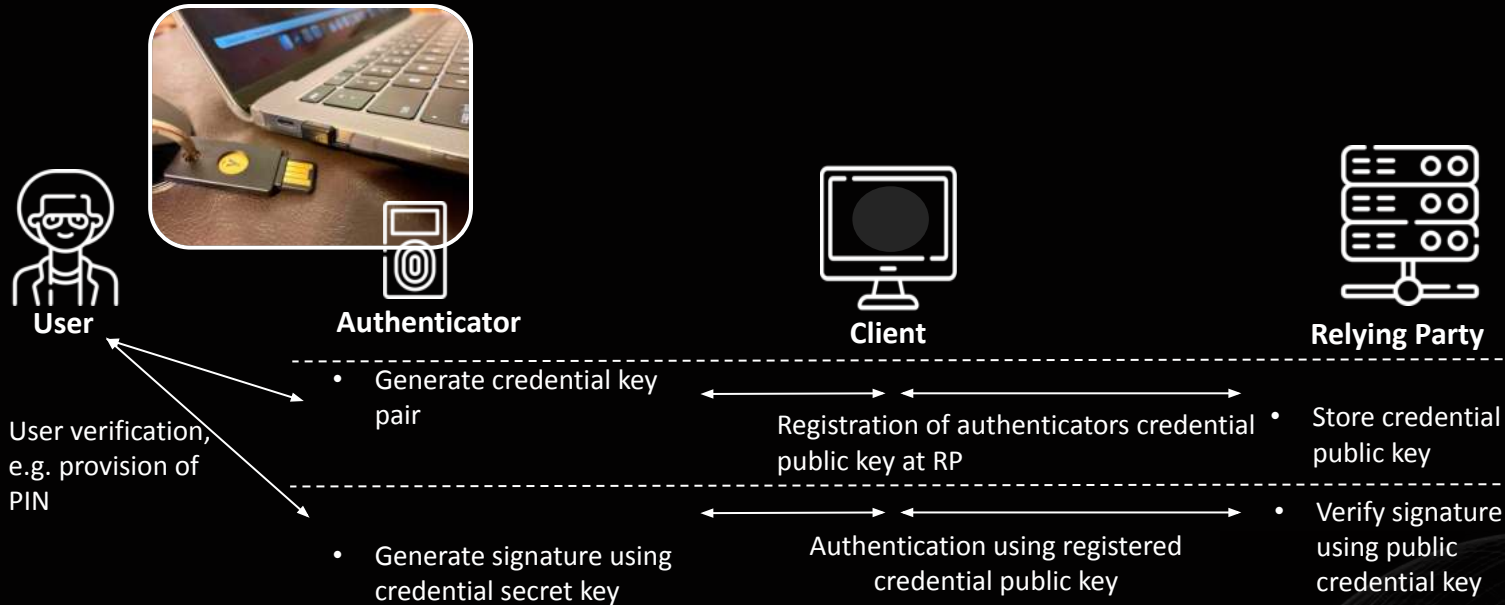


Relying Party

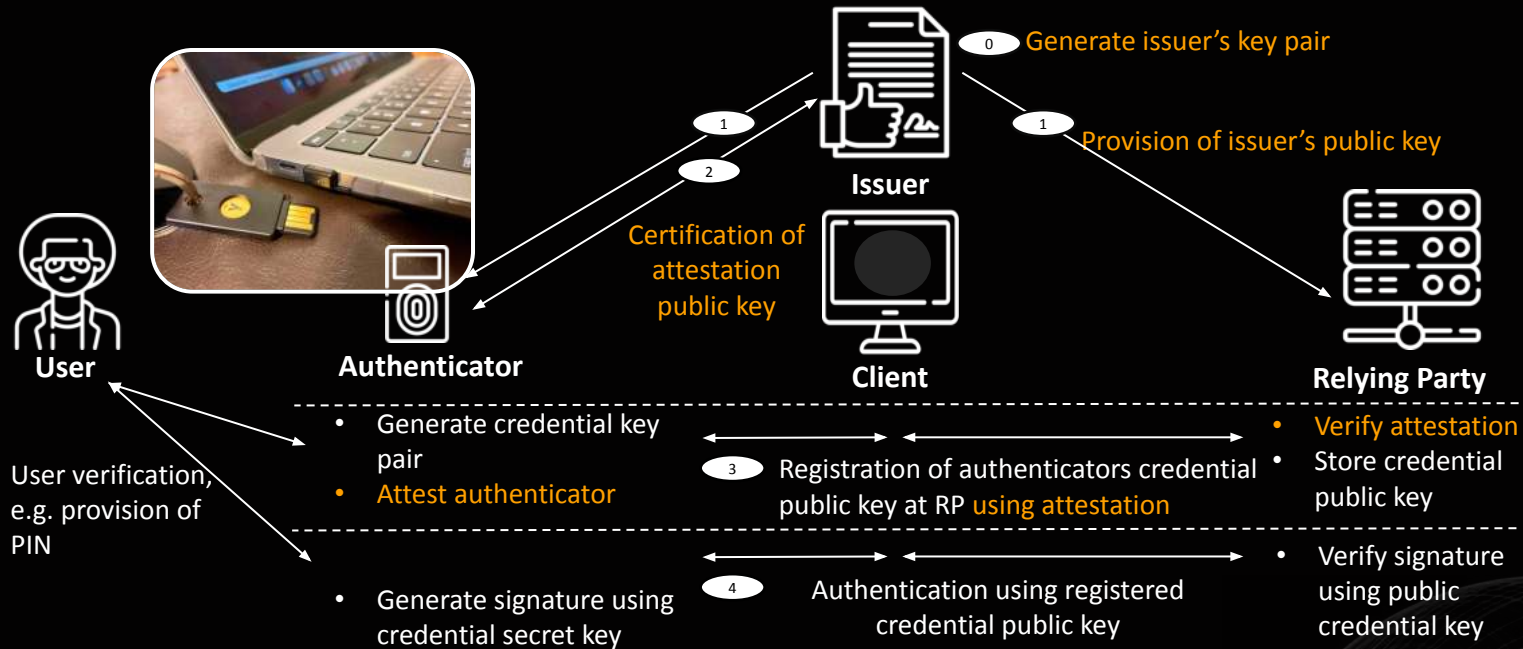
Basic FIDO2 operation flow



Basic FIDO2 operation flow



FIDO2 with token attestation



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.

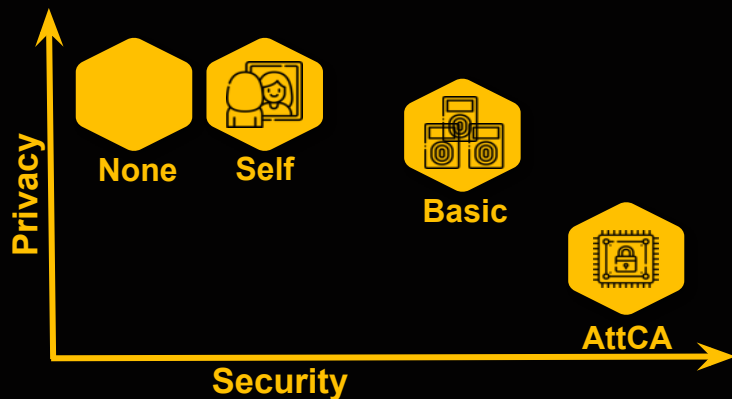
Origin of signed attestation records is indistinguishable within the group.



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

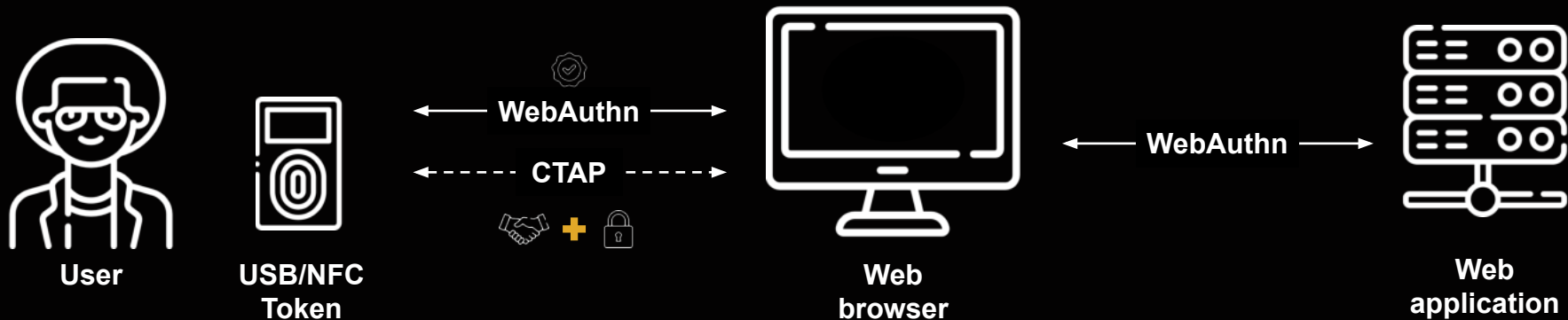
Implementation details

04

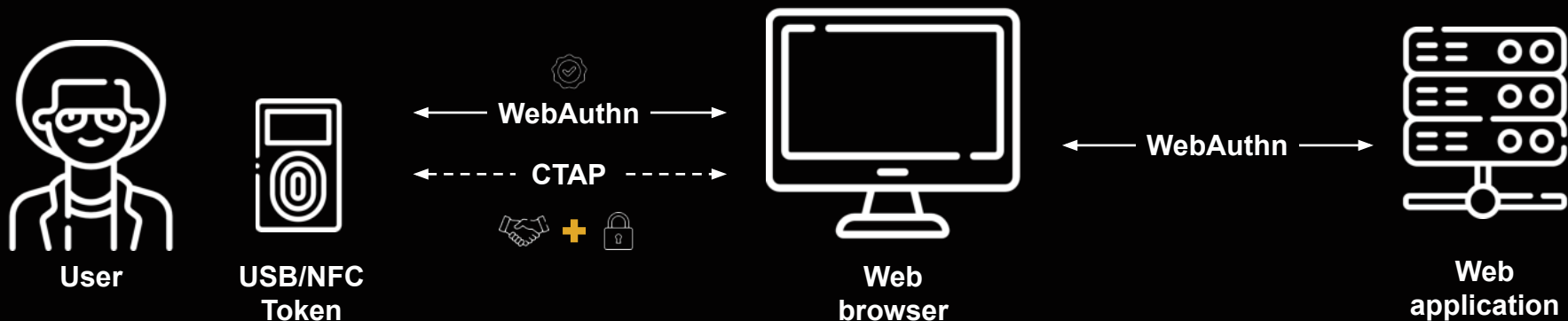
Challenges and future work

Additional modes to be considered in the PQ migration

FIDO2 protocol



FIDO2 = WebAuthn + CTAP



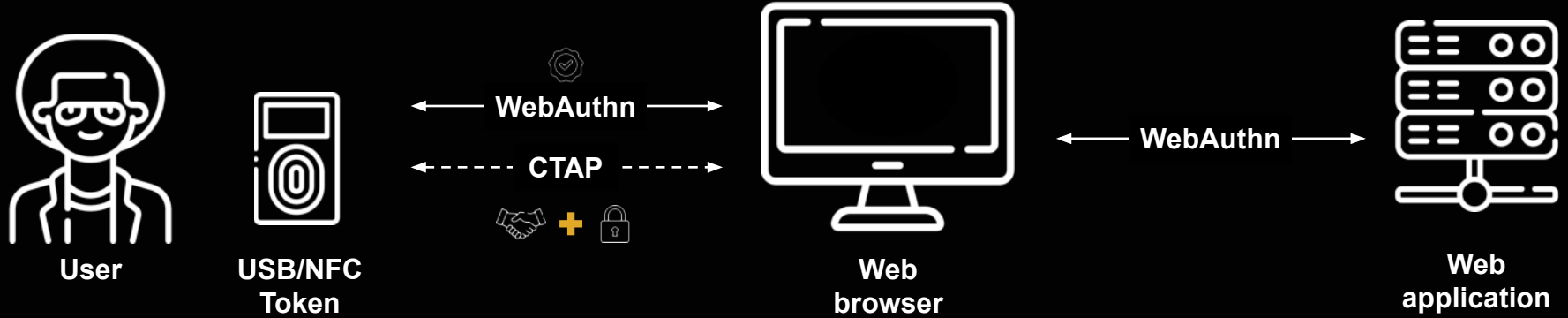
WebAuthn

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

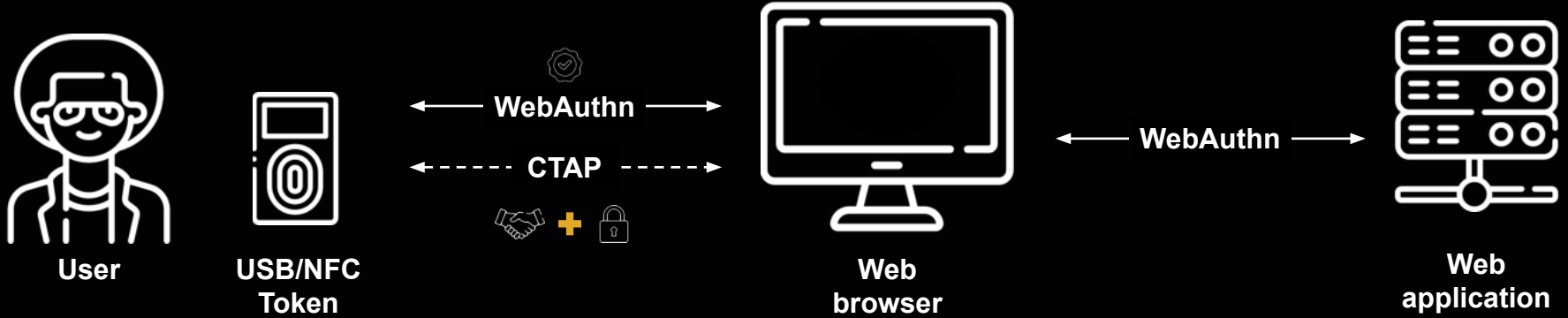


vk, att, more info



- *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>

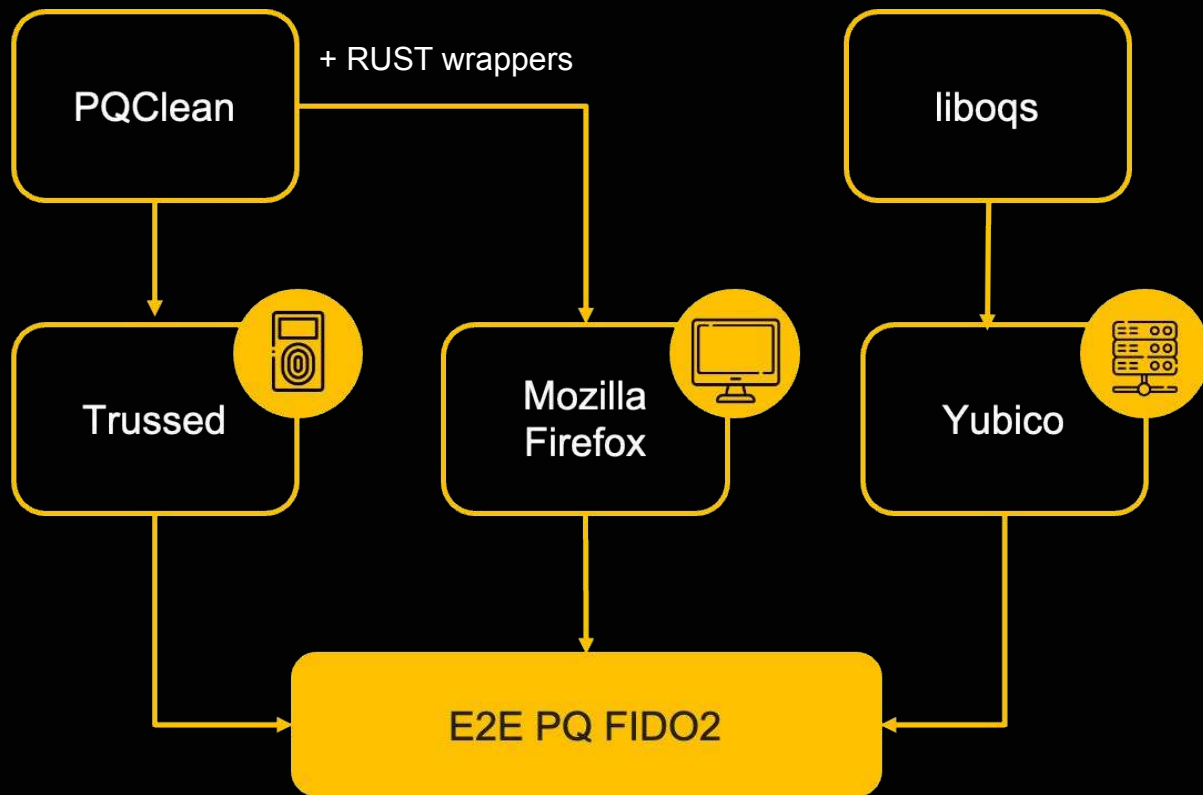
Libraries are where it all begins (Rita Dove)

E2E PQ FIDO2

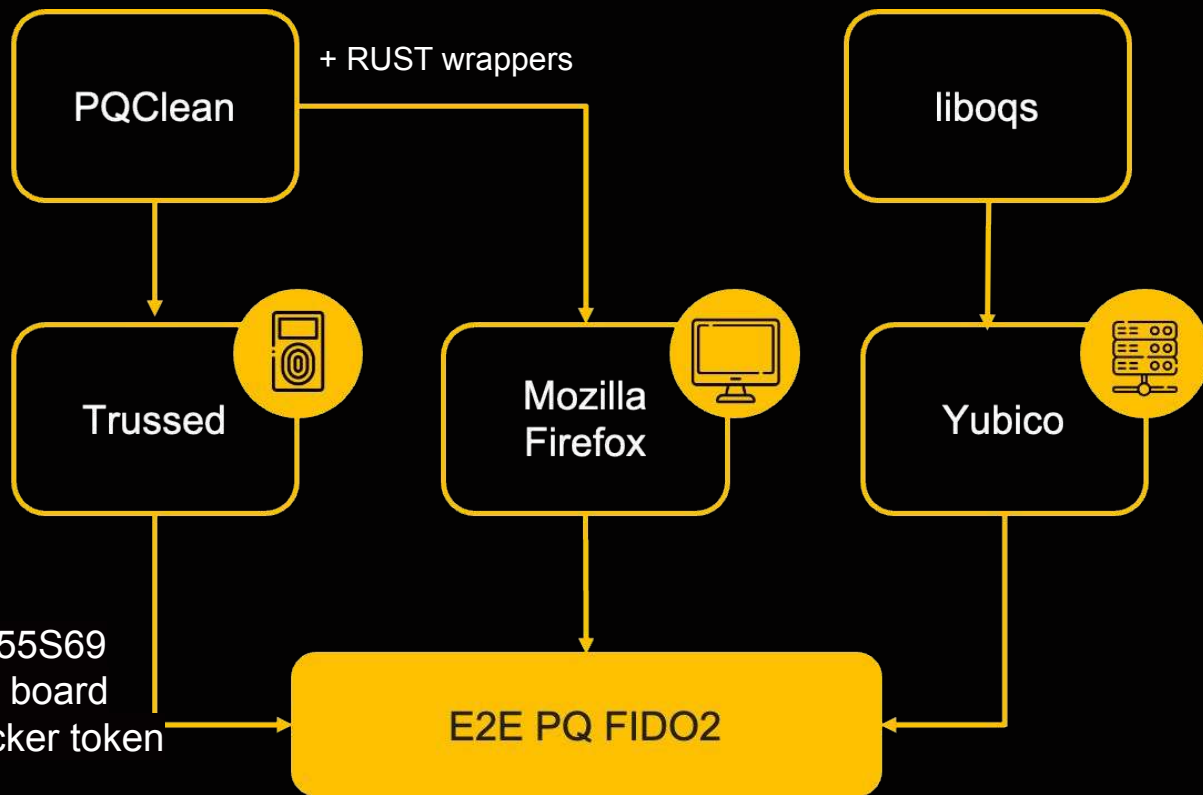
Libraries are where it all begins (Rita Dove)



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

WebAuthn Demo

https://localhost:8443

JAVA-WEBAUTHN-SERVER DEMO

Username:

Display name:

Credential nickname:

Credential ID:

Not logged in.

Server response:

Authenticator response:

Request:

```
java-webauthn-server -- ./gradlew run -- ./gradlew -- java -Xms64m -Xmx64m -Dorg.gradle.appname=gradlew -classpath ...
> Task :webauthn-server-demo:run
17:09:08.442+0100 [main] DEBUG demo.webauthn.Config - YUBICO_WEBAUTHN_ALLOWED_ORIGINS: null
17:09:08.444+0100 [main] INFO demo.webauthn.Config - Origins: [https://localhost:8443]
17:09:08.444+0100 [main] DEBUG demo.webauthn.Config - RP name: null
17:09:08.444+0100 [main] DEBUG demo.webauthn.Config - RP ID: null
17:09:08.445+0100 [main] DEBUG demo.webauthn.Config - RP name not given - using default.
17:09:08.445+0100 [main] DEBUG demo.webauthn.Config - RP ID not given - using default.
17:09:08.445+0100 [main] INFO demo.webauthn.Config - RP identity: RelyingPartyIdentity(name=Yubico WebAuthn demo, id=localhost)
17:09:08.483+0100 [main] INFO demo.webauthn.WebAuthnServer - Using only Yubico JSON file for attestation metadata.
17:09:08.660+0100 [main] INFO org.eclipse.jetty.util.log - Logging initialized @415ms to org.eclipse.jetty.util.log.Slf4jLog
17:09:08.701+0100 [main] INFO org.eclipse.jetty.server.Server - jetty-9.4.9.v20180320; built: 2018-03-20T13:21:10+01:00; git: 1f8159b1e4a42d3f79997021ea1609f2fbac0de5; jvm 17.0.9+0
Mar 21, 2024 5:09:08 PM org.glassfish.jersey.message.internal.MessagingBinders$EnabledProvidersBinder bindToBinder
WARNING: A class javax.activation.DataSource for a default provider MessageBodyWriter<javax.activation.DataSource> was not found. The provider is not available.
Mar 21, 2024 5:09:08 PM org.glassfish.jersey.server.wadl.WadlFeature configure
WARNING: JAX-B API not found. WADL feature is disabled.
Mar 21, 2024 5:09:08 PM org.glassfish.jersey.internal.inject.Providers checkProviderRuntime
WARNING: A provider demo.webauthn.WebAuthnRestResource registered in SERVER runtime does not implement any provider interfaces applicable in the SERVER runtime. Due to constraint configuration problems the provider demo.webauthn.WebAuthnRestResource will be ignored.
17:09:08.952+0100 [main] INFO o.e.j.server.handler.ContextHandler - Started o.e.j.s.ServletContextHandler@267517e4{/file:///Users/sandra.guasch/Documents/pqfido_test_140224/pq-fido2-impl/java-webauthn-server/webauthn-server-demo/src/main/webapp/,AVAILABLE)
17:09:08.964+0100 [main] INFO o.e.jetty.util.ssl.SslContextFactory - x509=x509077a281fc(serverkey, h=[], w=[]) for SslContextFactory@4912d525[provider=null, keyStore=file:///Users/sandra.guasch/Documents/pqfido_test_140224/pq-fido2-impl/java-webauthn-server/webauthn-server-demo/keystore.jks, trustStore=null]
17:09:09.020+0100 [main] INFO o.e.jetty.server.AbstractConnector - Started ServerConnector@2f61f937[SSL, [ssl, http/1.1]]{127.0.0.1:8443}
17:09:09.020+0100 [main] INFO org.eclipse.jetty.server.Server - Started @777ms
<=====> 95% EXECUTING [1s]
> :webauthn-server-demo:run
[]
```



Sandra Guasch Castello

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



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!