FIDO2 and Web Authentication

STRONG AUTHENTICATION FOR THE MASSES

Joost van Dijk

23 may 2019 - NLUUG Spring Conference

SURF NET

about

- Technical Product Manager Security & Privacy @SURFnet
- Co-designer of tiqr
- Operating SURFsecureID stepup authentication service
- World Wide Web Consortium (W3C) member (w/445 others)
- Not a FIDO Alliance member

sa.test.surfconext.nl/registration/select-token

Registration Portal

Authentication in two steps

English | Sign out

1. Select token | 2. Link token | 3. Confirm | 4. Activate token

Select token

SMS

Log in with a one time SMS code. For all mobile phones.

Select

Tiqr

Log in with a smartphone app. For all smartphones with Apple iOS or Android.

Select

YubiKey

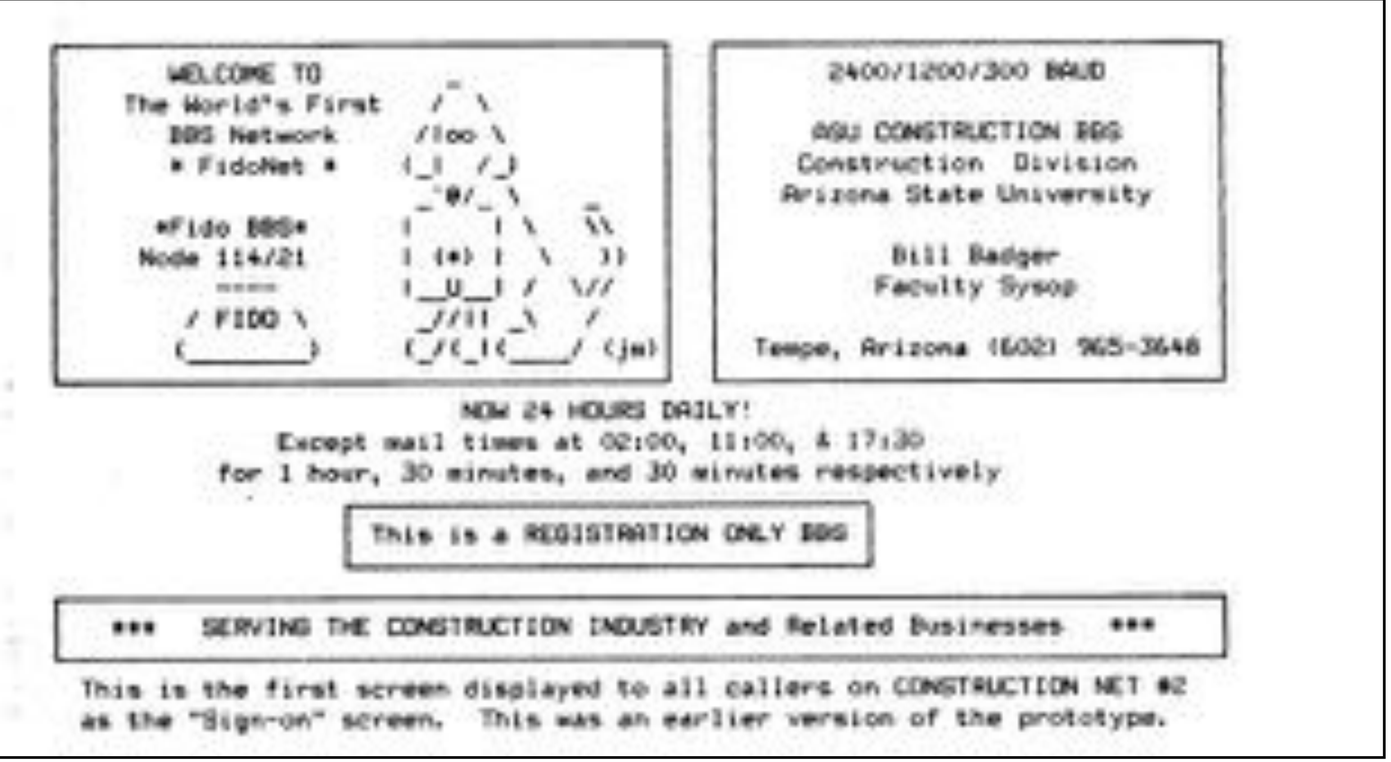
Log in with a USB hardware token. For all devices with a USB port.

Select

U2F

Sign in with a U2F device.

Select



FIDO?

Image credits: wikipedia


fido™
WebAuthn

www.w3.org/TR/2019/REC-webauthn-1

W3C Recommendation

Web Authentication: An API for accessing Public Key Credentials Level 1

W3C Recommendation, 4 March 2019

This version:
https://www.w3.org/TR/2019/REC-webauthn-1-20190304/

Latest version of Level 1:
https://www.w3.org/TR/webauthn-1/

Latest version of Web Authentication:
https://www.w3.org/TR/webauthn/

Editor's Draft:
https://w3c.github.io/webauthn/

Previous Versions:
https://www.w3.org/TR/2019/PR-webauthn-20190117/

Issue Tracking:
GitHub

Editors:
Dirk Balfanz (Google)
Alexei Czeskis (Google)
Jeff Hodges (Google)
J.C. Jones (Mozilla)
Michael B. Jones (Microsoft)
Akshay Kumar (Microsoft)

fidoalliance.org/specs/fido-v2.0-ps-201

Client to Authenticator Protocol (CTAP)

Proposed Standard, January 30, 2019

This version:
https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html

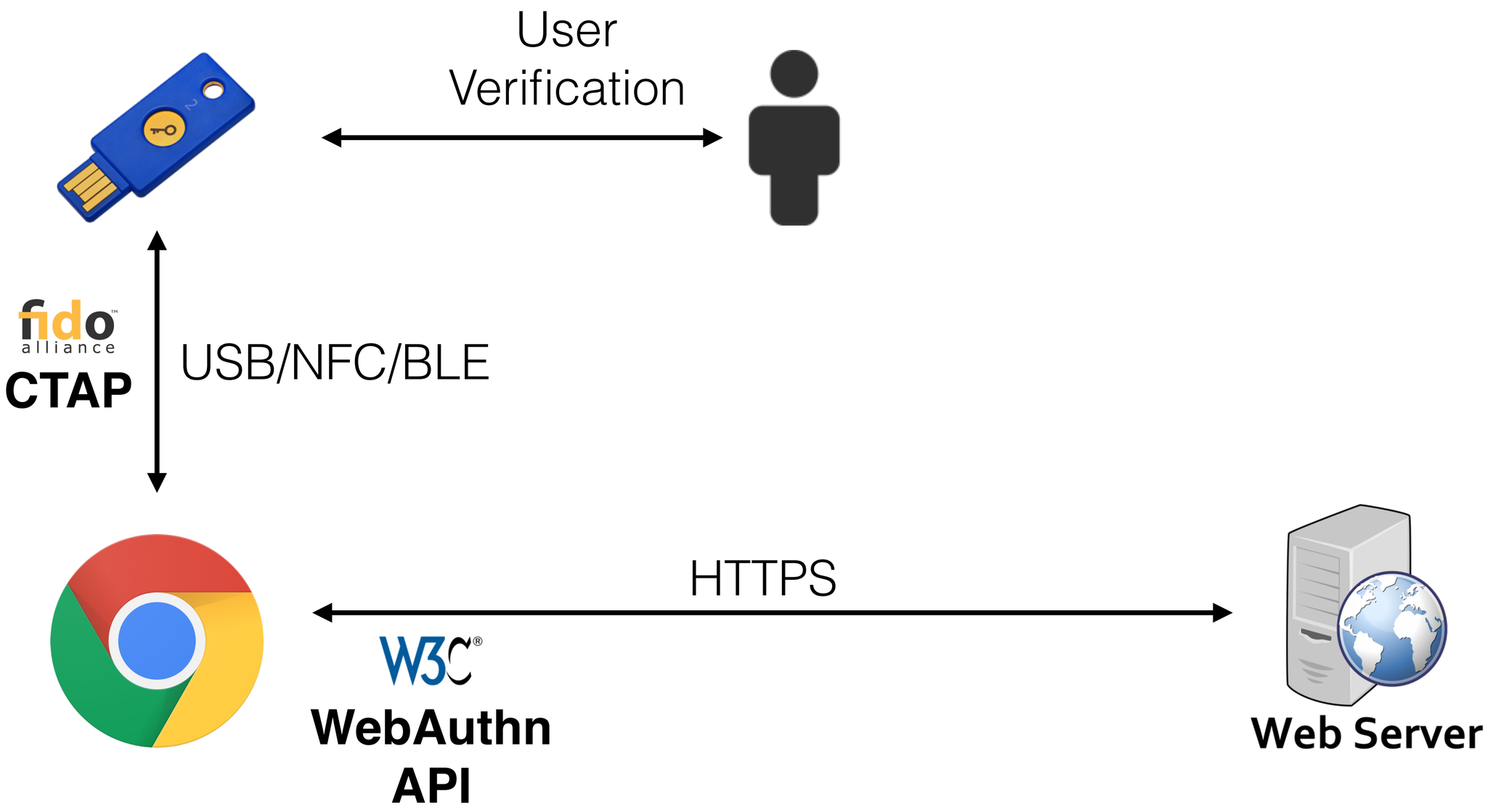
Previous Versions:
https://fidoalliance.org/specs/fido-v2.0-id-20180227/

Issue Tracking:
GitHub

Editors:
Christiaan Brand (Google)
Alexei Czeskis (Google)
Jakob Ehrensvärd (Yubico)
Michael B. Jones (Microsoft)
Akshay Kumar (Microsoft)
Rolf Lindemann (Nok Nok Labs)
Adam Powers (FIDO Alliance)
Johan Verrept (OneSpan)

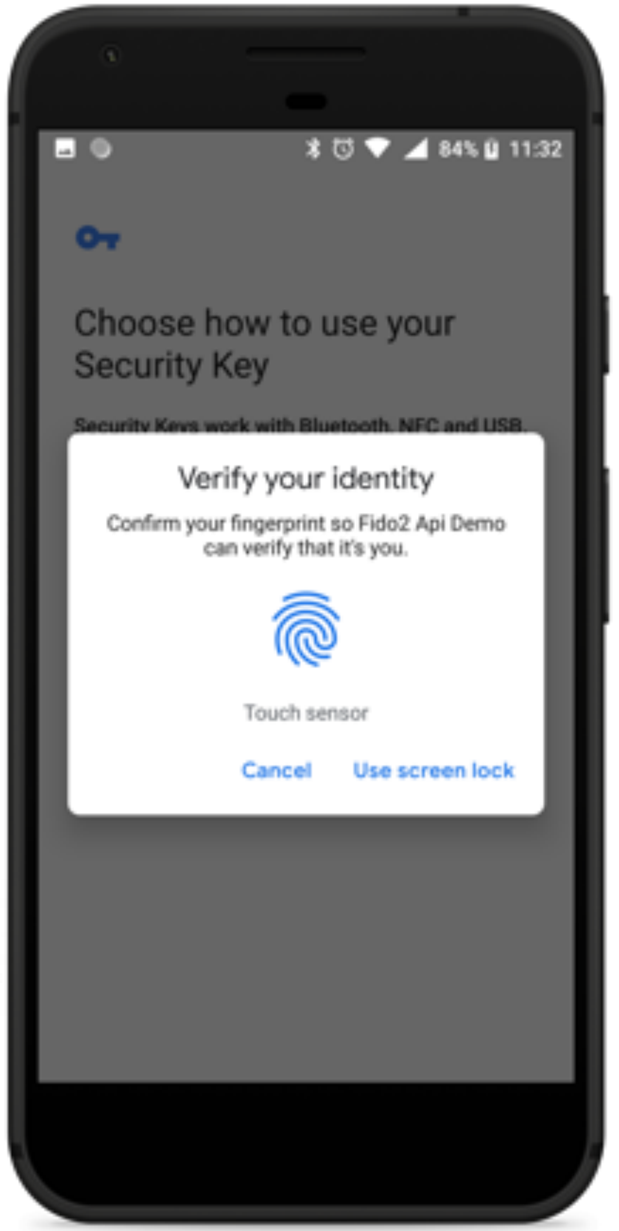
Former Editors:
Matthieu Antoine (Gemalto)
Arnar Birgisson (Google)
Vijay Bharadwaj (Microsoft)
Mirko J. Ploch (SurePassID)

Contributors:


User
Verification
fido alliance
CTAP
USB/NFC/BLE
HTTPS
W3C
WebAuthn
API
Web Server

Roaming Authenticators

Platform Authenticators



WebAuthn.io

https://webauthn.io

Apps YouTube Maps News

WebAuthn.io

A demo of the WebAuthn specification

username@example.com

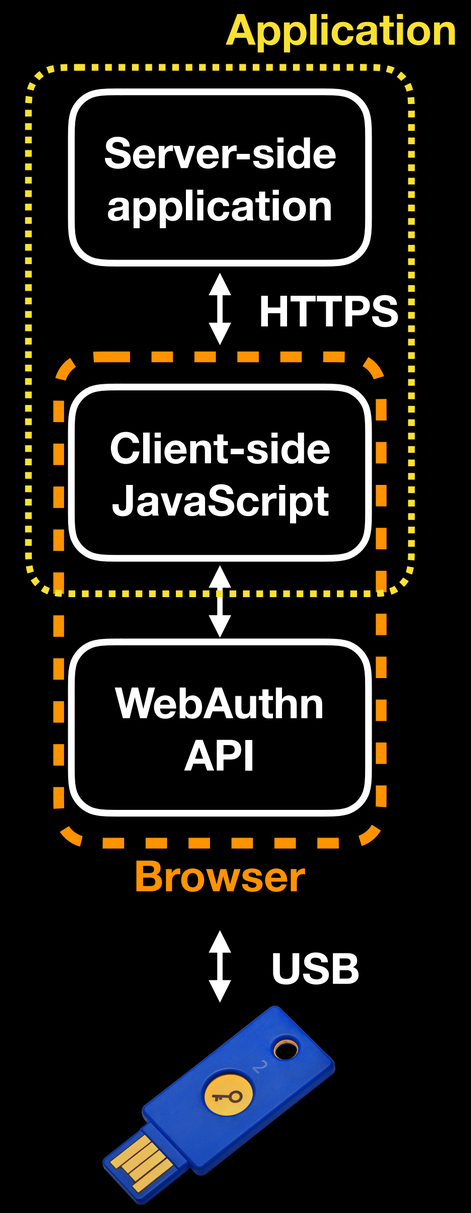
Attestation Type: None

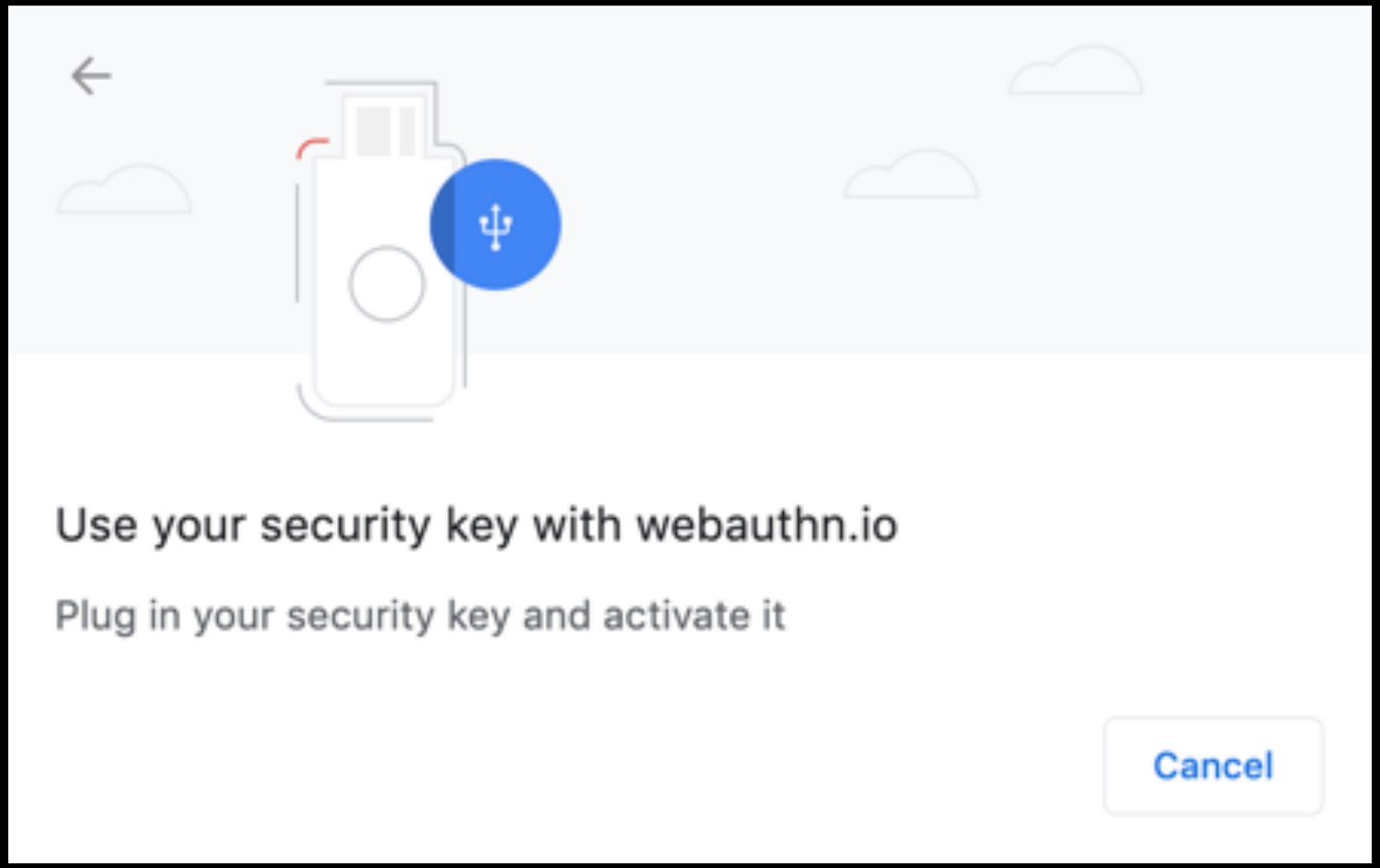
Authenticator Type: Unspecified

Register Login

JavaScript API

- `navigator.credentials.create()`
  register new key
- `navigator.credentials.get()`
  authenticate using a previously registered key




Use your security key with webauthn.io
Plug in your security key and activate it
Cancel

What’s there to like?

1. strong
2. attestable
3. affordable
4. no shared secrets
5. replay resistant
6. phishing resistent
7. MitM resistent
8. passwordless
9. scoped
10. interoperable
11. portable
12. certified
13. privacy-friendly
14. user-verified

affordable

amazon.de

All ▾ Fido2

Fashion Shop men and women's fashion

Deliver to Netherlands | Shop by Department ▾ | Your Amazon.de | Today's Deals | Gift Cards | Sell | Help | EN | Hello, Sign in Your Account ▾ | Discover Prime ▾ | Your Lists ▾ | Shopping Basket

Amazon.de | SALE | Warehouse Deals | Vouchers | Fashion Sale | Family | Students | Subscribe & Save | Pantry | Gift Central | Apps | Amazon Assistant

47 results for "Fido2"

Sort by: Featured ▾

Amazon Prime

- prime
- Free shipping for deliveries over EUR 29

For all customers with orders over €29 shipped by Amazon

Department

DIY & Tools
- Gate Hardware
- Garage Door Hardware

Computer & Accessories
- USB Gadgets
- Security Locks

Electronics & Photo
- Mobile Phones & Smartwatches Accessories

› See All 9 Departments

Avg. Customer Review

★★★★☆ & Up
★★★☆☆ & Up
★★☆☆☆ & Up
★☆☆☆☆ & Up

Brand

- Lilly
- Yubico

International Shipping

- International Shipping Eligible

Security Key by Yubico
★★★☆☆ · 10
€25.00
prime Get it by Friday, May 24
FREE Delivery on orders over €29 dispatched by Amazon
More buying choices
€24.99 (4 new offers)

YubiKey 5 NFC
★★★★☆ · 16
More buying choices
€48.65 (6 new offers)

Yubico NFC USB-A Security Key Two Factor Authenticity Key Blue
★★★☆☆ · 5
€35.00
prime Get it by Friday, May 24
FREE Delivery by Amazon
More buying choices
€29.90 (5 new offers)

BioPass FIDO2 Security Key
€55.66
prime Get it by Friday, May 24
FREE Delivery by Amazon
Only 5 left in stock.

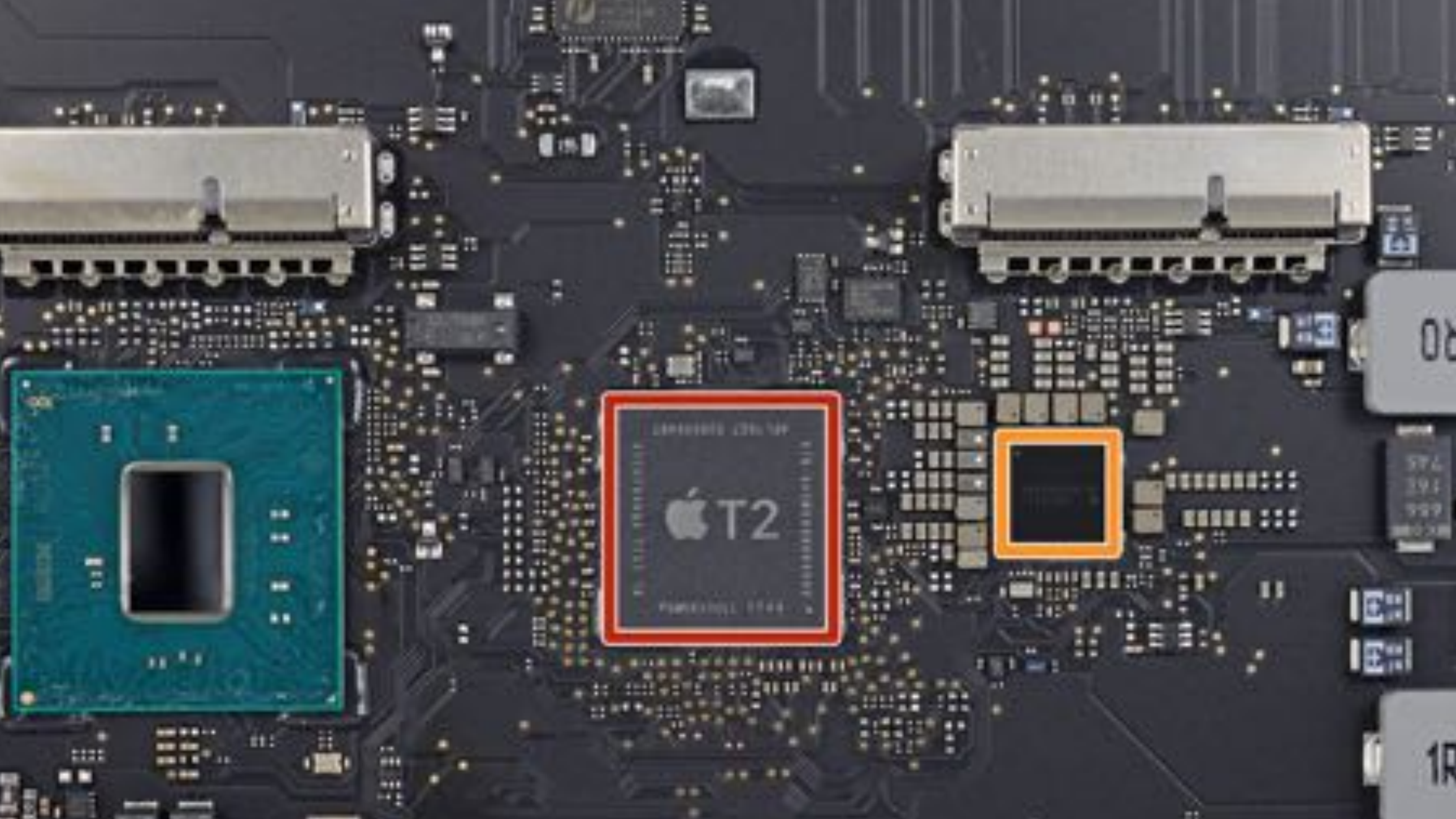
Amazon's Choice

Fido Key ID U2 'F' Security Key – Model 2017
★★★★½ · 22
€9.50
prime Get it by Friday, May 24
FREE Delivery on orders over €29 dispatched by Amazon

HERAKI

strong

secure hardware

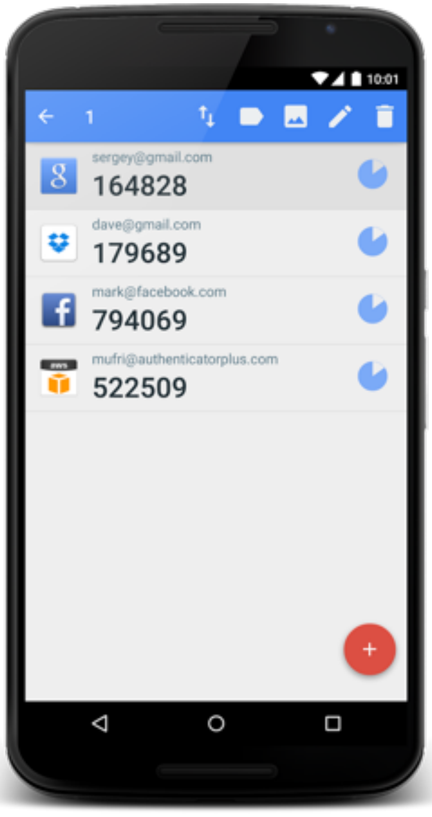

T2

no shared secrets

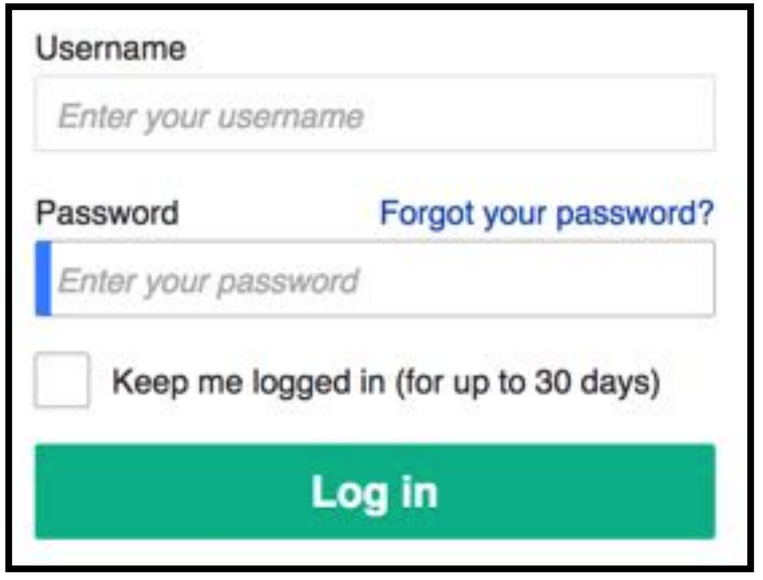
Public Key Cryptography


RSA
SecurID
159 759.

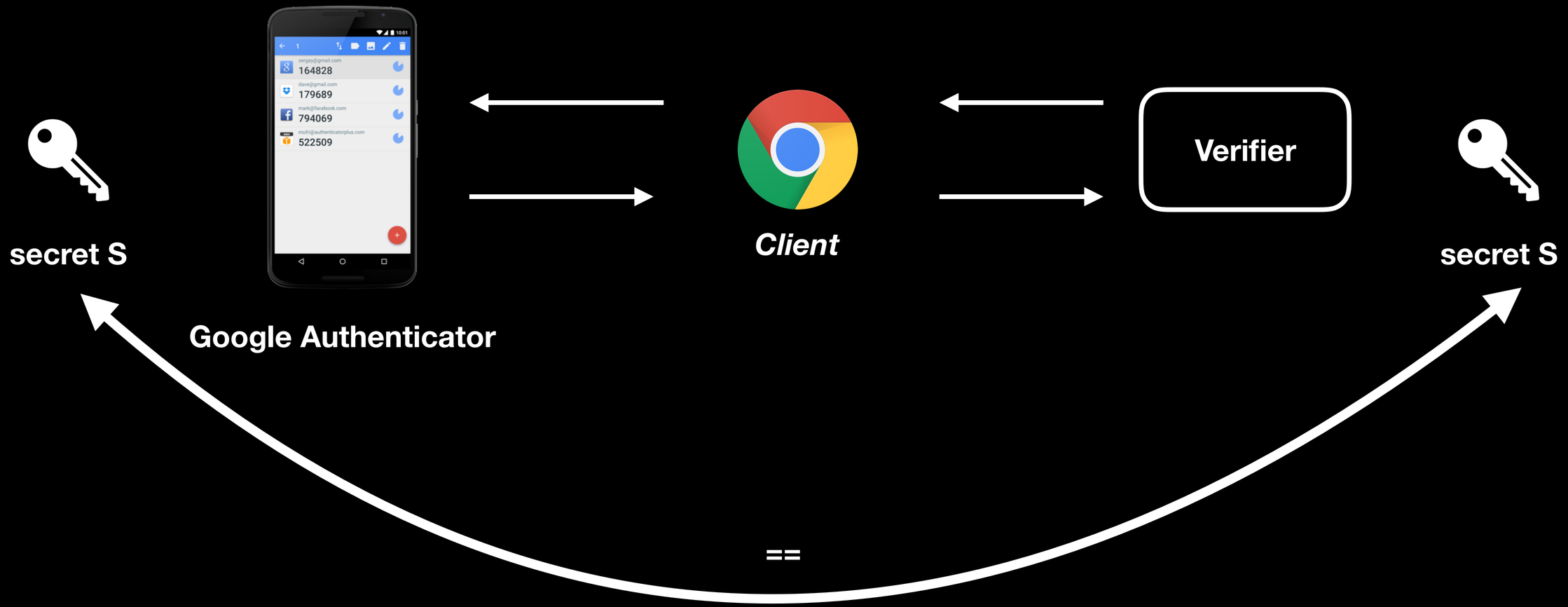

①
②
③
④


10:01
sergey@gmail.com
164828
dave@gmail.com
179689
mark@facebook.com
794069
mufri@authenticatorplus.com
522509


257324
OneSpan


Username
Enter your username
Password
Forgot your password?
Enter your password
Keep me logged in (for up to 30 days)
Log in

symmetric keys



asymmetric keys

replay prevention

challenge/response

Challenge/Response authentication

response = sign(k, challenge)

result = verify(p, response)

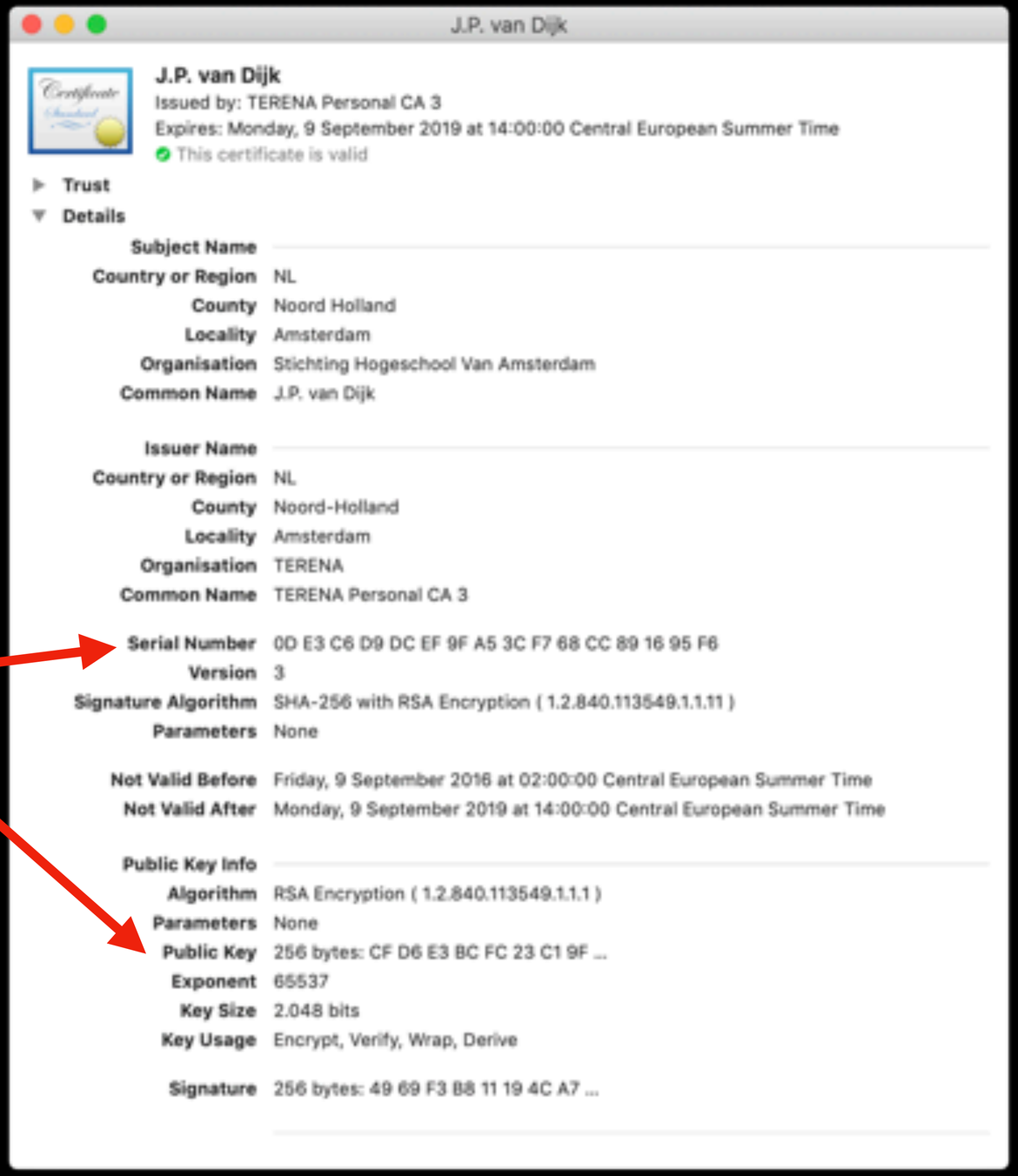
user presence

https://www.troyhunt.com/content/images/2018/11/robotguys.png

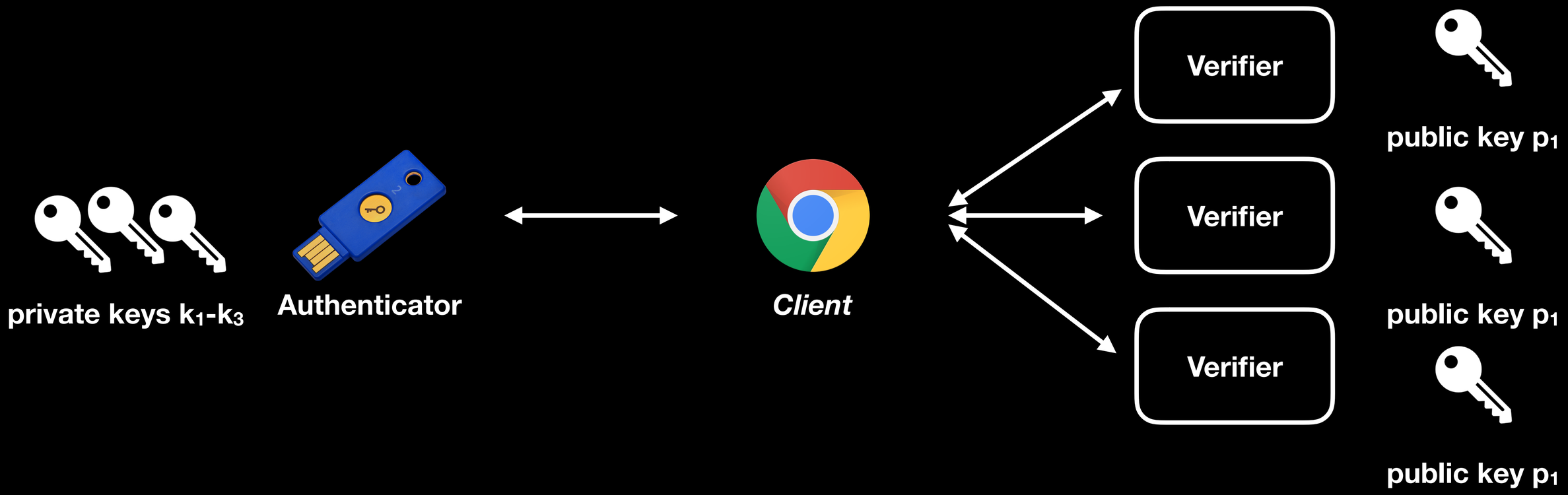
privacy

per-site key pairs

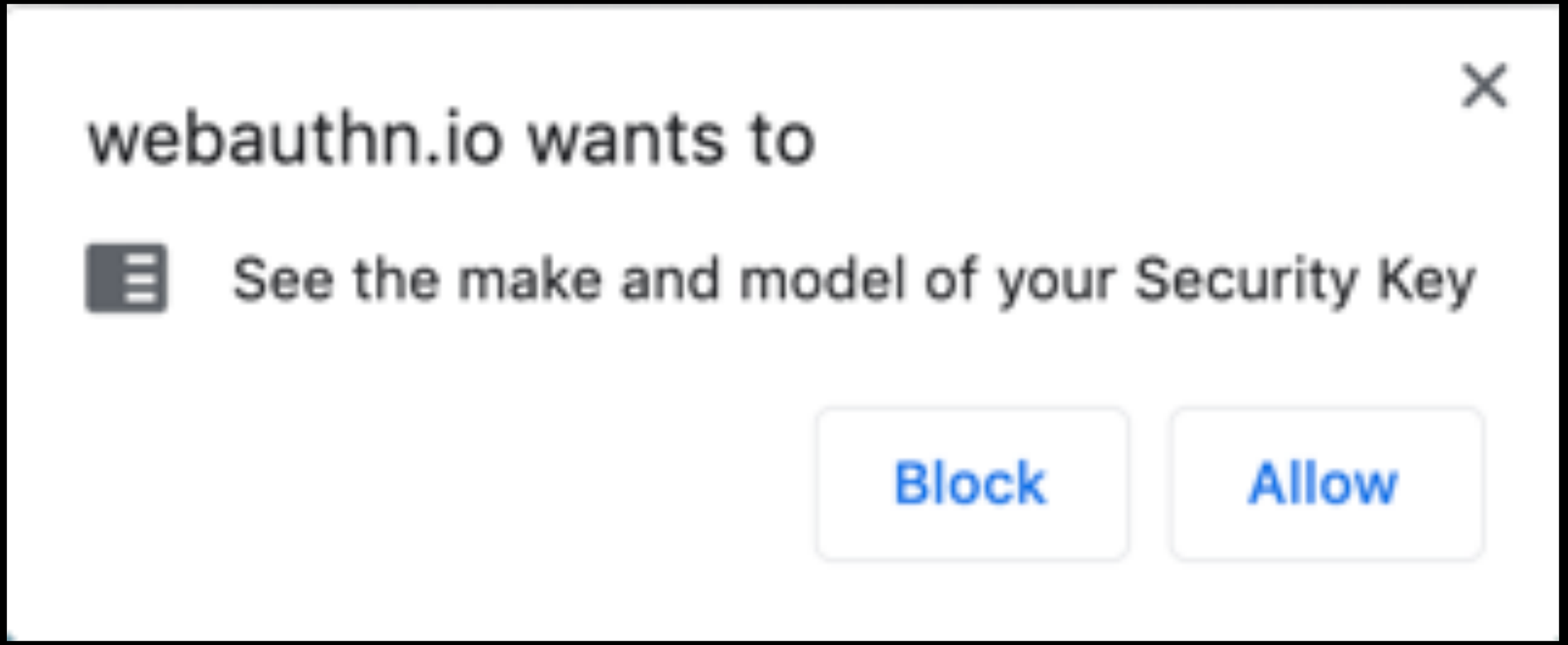
“super cookies”



per-site key pairs



Device Attestation


webauthn.io wants to
See the make and model of your Security Key
Block
Allow

FT-BioPass-FIDO2-USB.cer | Open with Keychain Access

FT BioPass FIDO2 USB

Subject Name
- Country or Region US
- Organisation Feitian Technologies
- Organisational Unit Authenticator Attestation
- Common Name FT BioPass FIDO2 USB

Issuer Name
- Country or Region US
- Organisation Feitian Technologies
- Common Name Feitian FIDO CA 01

Serial Number 1D F2 B5 5A 51 DC 4B 68 85 A3 D9 9E 69 7F ED 14
Version 3
Signature Algorithm ECDSA Signature with SHA-256 (1.2.840.10045.4.3.2)
- Parameters None

Not Valid Before Thursday, 21 June 2018 at 02:00:00 Central European Summer Time
Not Valid After Tuesday, 21 June 2033 at 01:59:59 Central European Summer Time

Public Key Info
- Algorithm Elliptic Curve Public Key (1.2.840.10045.2.1)
- Parameters Elliptic Curve secp256r1 (1.2.840.10045.3.1.7)
- Public Key 65 bytes: 04 60 50 F8 6E E1 24 D9 ...
- Key Size 256 bits
- Key Usage Any

Signature 72 bytes: 30 46 02 21 00 8D 0E 3F ...

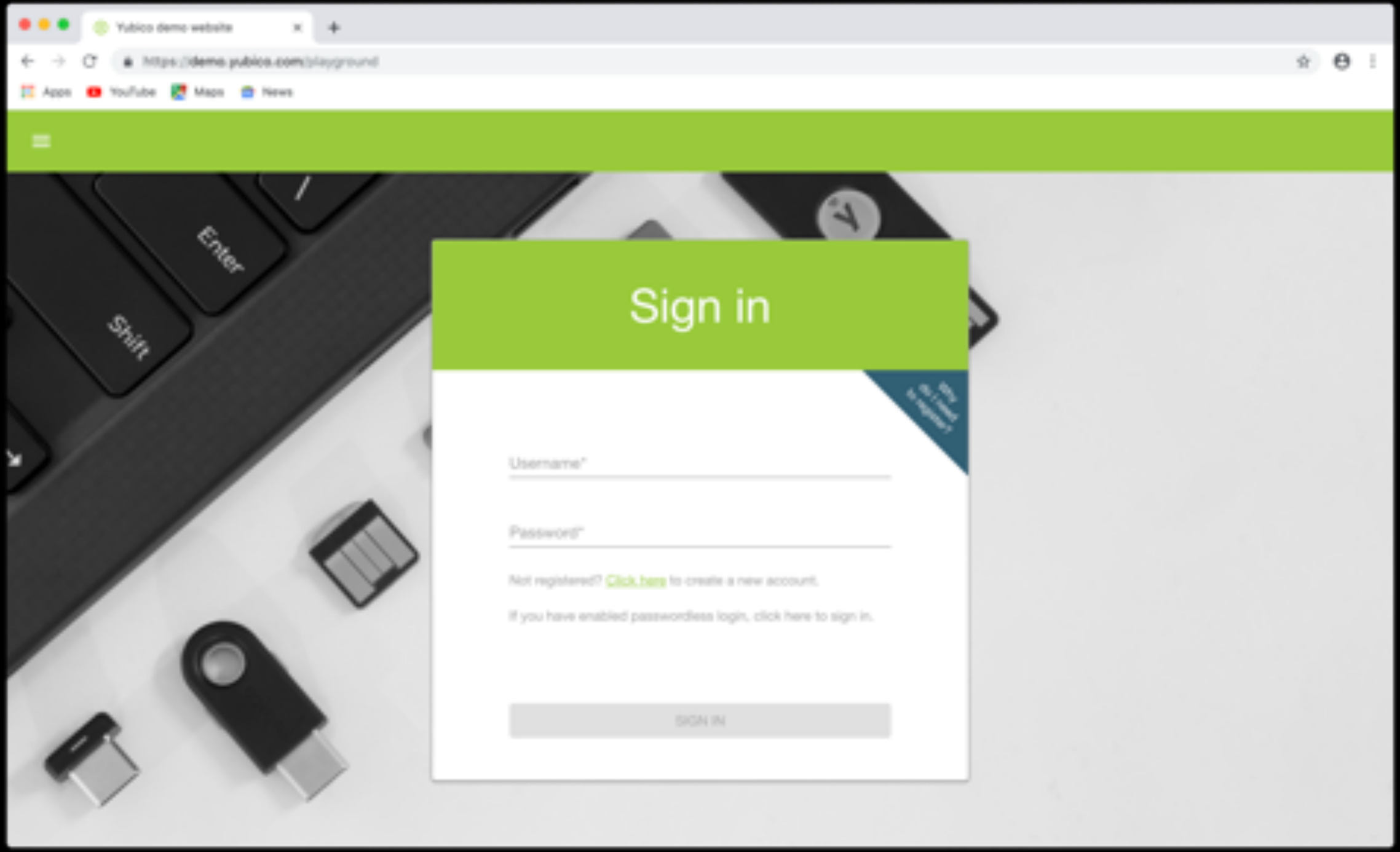
Extension Basic Constraints (2.5.29.19)
- Critical YES
- Certificate Authority NO

Extension Subject Key Identifier (2.5.29.14)
- Critical NO
- Key ID 01 F2 C2 B4 DC B9 5E 7B 86 1F D8 4E 99 CA 58 9F 37 7B 33 F5

Extension Authority Key Identifier (2.5.29.35)

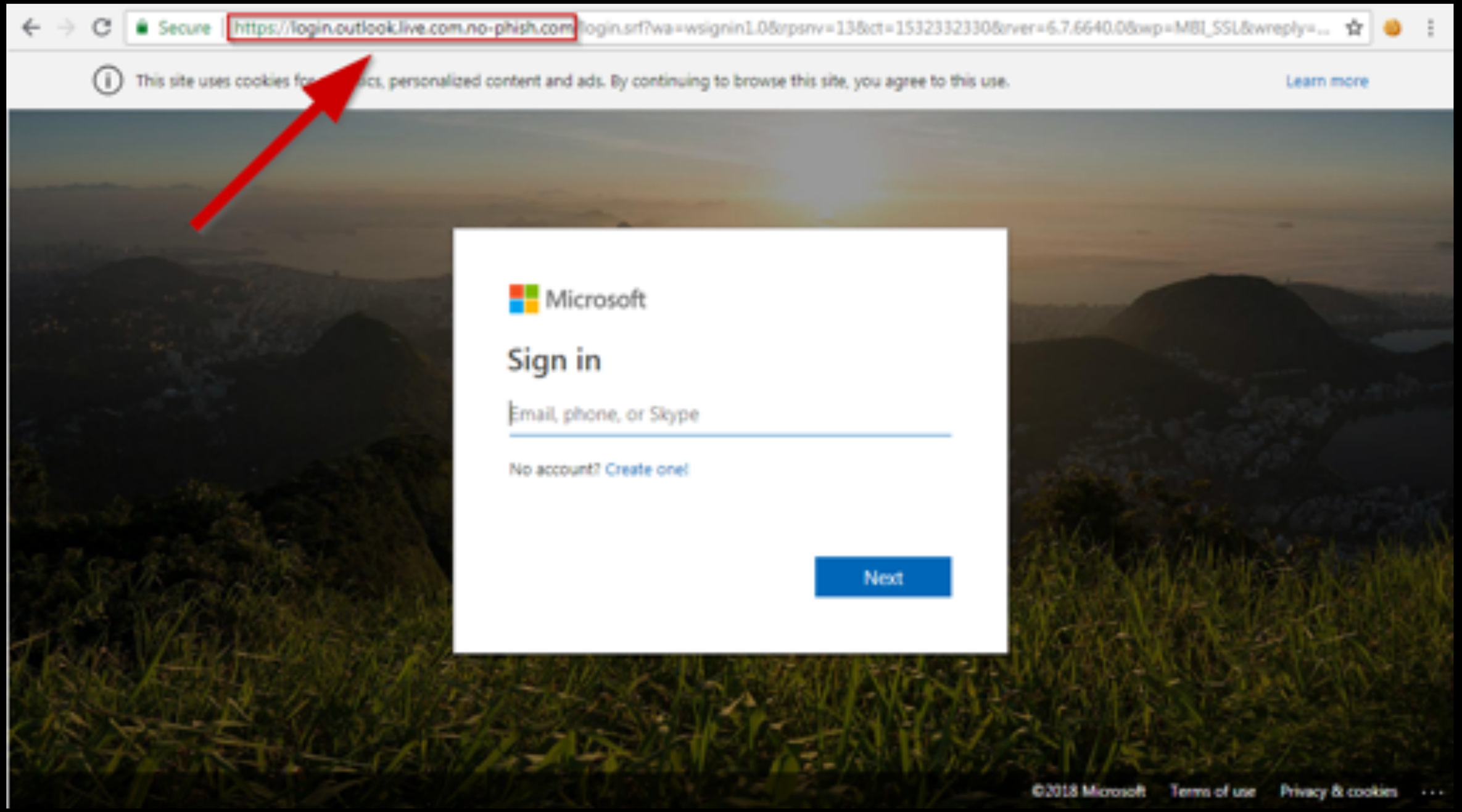
passwordless

resident keys


Yubico demo website
https://demo.yubico.com/playground
Apps
YouTube
Maps
News
Enter
Shift
Sign in
Username*
Password*
Not registered? Click here to create a new account.
If you have enabled passwordless login, click here to sign in.
SIGN IN

phishing resistance

Scoped Credentials



https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/

response = sign(k, challenge)

result = verify(p, response)

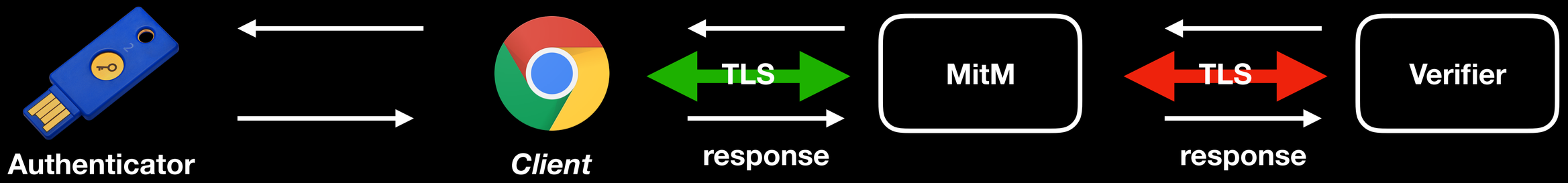
response = sign(k, challenge+origin)

result = verify(p, response) and
check origin

MitM resistance

Token Binding

Token Binding



caniuse.com/#feat=webauthn

Web Authentication API - REC

The Web Authentication API is an extension of the Credential Management API that enables strong authentication with public key cryptography, enabling password-less authentication and / or secure second-factor authentication without SMS texts.

Usage % of all users

Global 67.81%

unprefixed 67.81%

Current aligned | Usage relative | Date relative | Apply filters | Show all

IE	Edge	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser	Blackberry Browser	Opera Mobile	Chrome for Android	Firefox for Android	IE Mobile	UC Browser for Android	Samsung Internet
	12	2-59	4-66		10-53										
6-10	13-17	60-65	67-73	3.1-12	54-57	3.2-12.1		2.1-4.4.4	7	12-12.1			10		4-8
11	18	66	74	12.1	58	12.2	all	67	10	46	74	66	11	11.8	9.2
	75	67-68	75-77	TP											

Notes | Known issues (0) | Resources (8) | Feedback

WebKit status: In Development

[1] Can be enabled at about:flags

Edge 13 used an earlier draft syntax. As of Edge 14 the implementation is prefixed and based on the FIDO 2.0 Web APIs.

[2] Can be enabled using the Develop > Experimental Features menu. Currently supports USB-based CTAP & CTAP2 HID devices.

FIDO2 in 2019

- Jan 30: CTAP FIDO Alliance Proposed Standard
- Feb 25: Android 7.0+ is now FIDO2 Certified
- Mar 4: Web Authentication W3C Recommendation
- May 6: Microsoft for Windows Hello FIDO2 Certified
- May 13: Safari 12.1 Webauthn as experimental feature
- May 21: Windows 10, version 1903 released


Joost.vanDijk@surfnet.nl


@joostd


joostd@hotmail.com


https://www.linkedin.com/in/joostd/

SURF NET