RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Why is FIDO better than other 2FAs

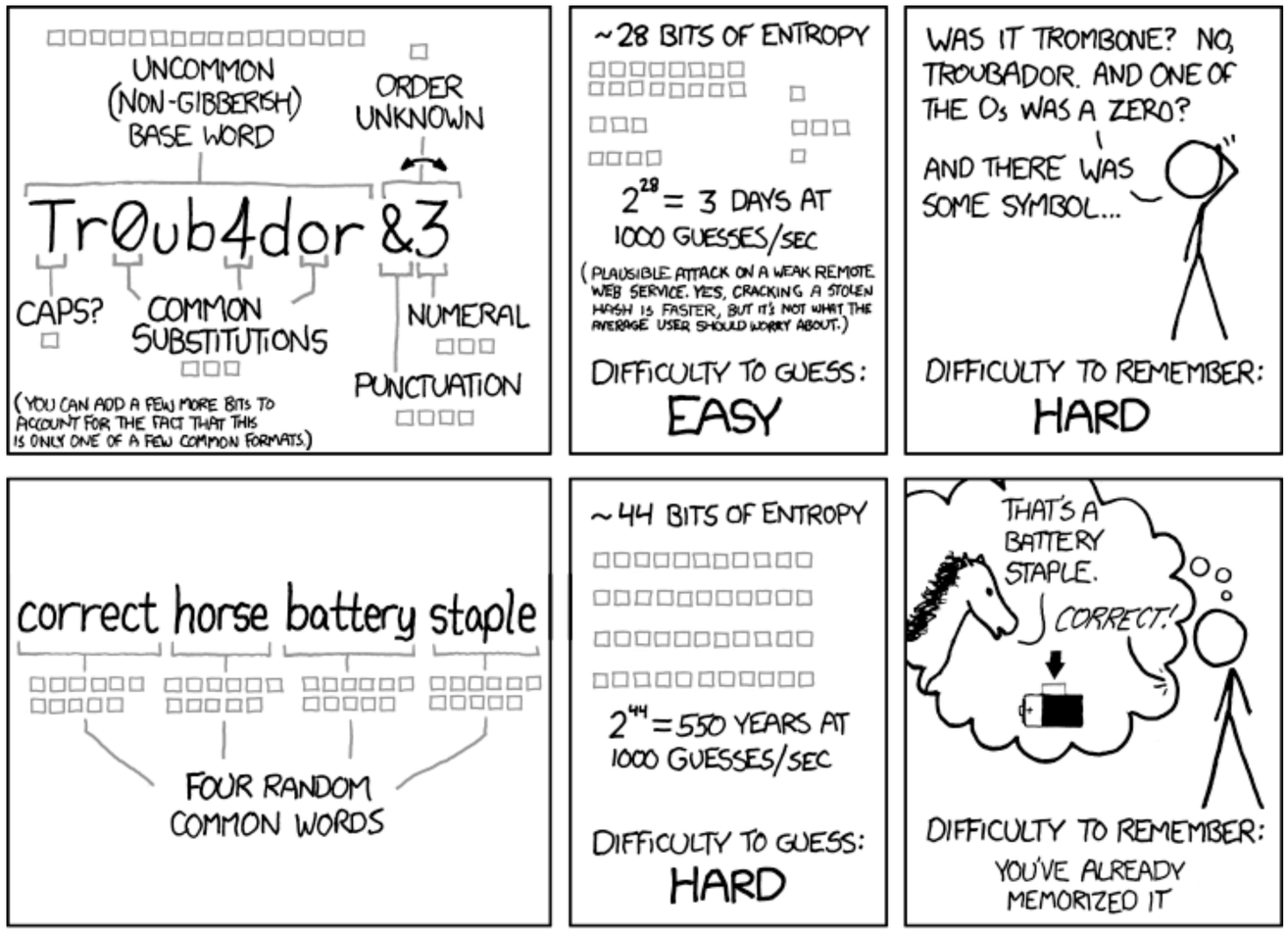
Magic behind Webauthn, U2F and others

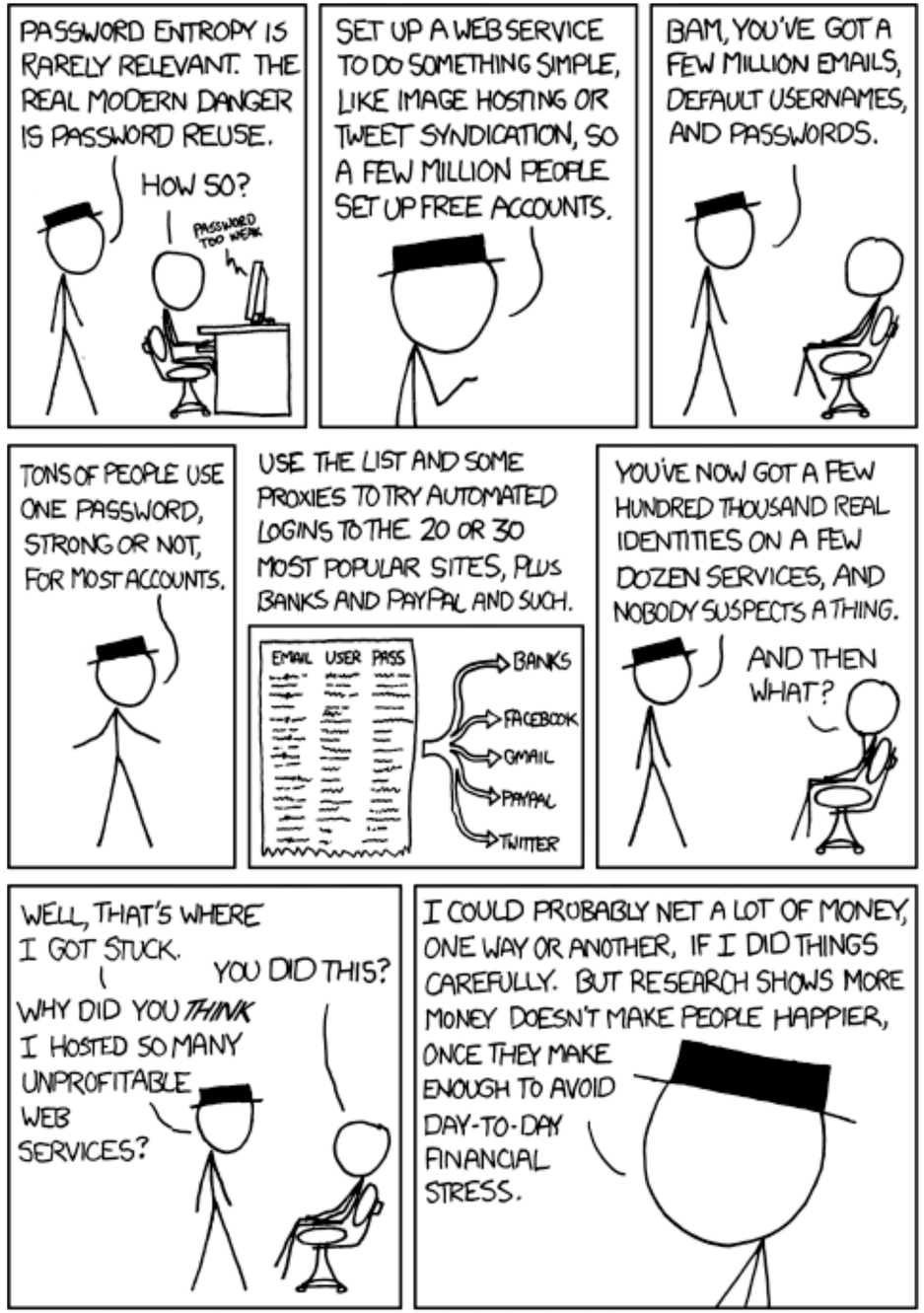
Ondřej Caletka | 23 March 2022 | Engineering Social

~~Passwords~~ People are bad

- People are in general very **careless** with passwords
- But often there's nothing better
- Some people don't even use a password manager
  - At least the one in the web browser
- **Phishing** is a problem
- Two general problems with passwords:
  - ~~Password getting weaker after a year or so~~
  - **Low complexity** (dictionary words)
  - **Password reuse** (data breaches are an issue)

xkcd has it covered





Multi Factor Authentication

- Something you **know**
  - password
- Something you **have**
  - your phone
  - bank card
- Something you **are**
  - biometry (complicated *revocation*)

Note: bank card + SMS is actually same type of factor.
EU directive PSD2 requires Strong Customer Authentication,
Card number + SMS is not sufficient anymore for 3-D Secure.

The state of authentication on the Web

- **TL;DR: Disaster**
- A Challenge/Response authentication **does** exist (HTTP Digest)
  - Supported by every browser
  - With native, hardly phishable interface
  - Not **sexy enough,** nobody uses it
  - Problematic logouts
- We just send our passwords in **cleartext** to servers and *hope for the best*
  - Will they at least **hash the password**? With something **better than MD5**?
- Data breaches happen all the times

Second factor validation methods

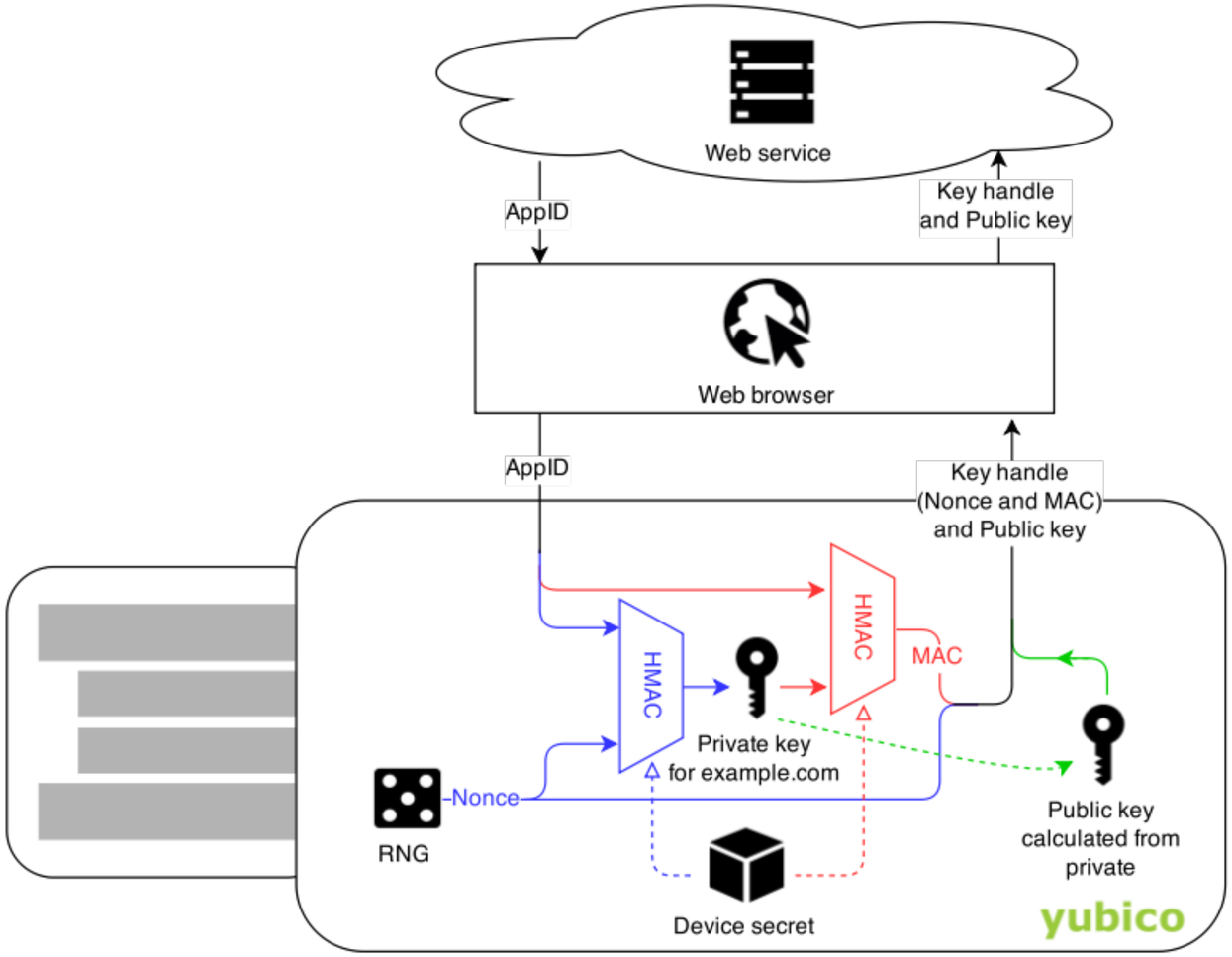
- SMS codes
  - expensive
  - SIM swapping
  - phishable
  - user unfriendly
- Auth. calculators
  - **super expensive**
  - phishable
  - user unfriendly

- HOTP/TOTP
  - cheap
  - phishable
  - user unfriendly

- FIDO
  - *getting cheaper*
  - tied to a device
  - **non-phishable**
  - **user friendly**
  - developer friendly
  - not supported by all browsers

FIDO: non-phishable, non-trackable

- Challenge-response authentication *reinvented*
- Every account uses its **own** private/public key pair
- The correct key pair is selected by website URL + nonce
- Phishing site will never have the same URL
- Authenticator does not require writable memory



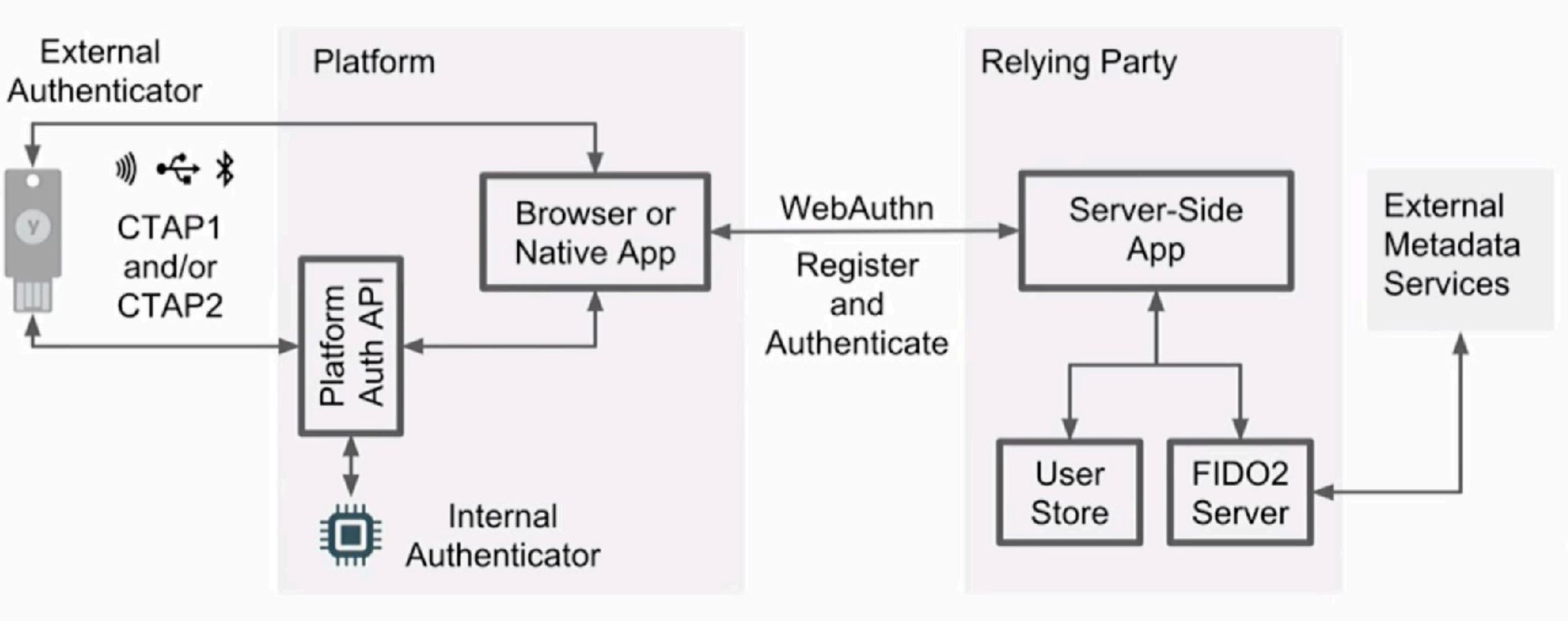
Source: https://www.yubico.com/blog/yubicos-u2f-key-wrapping/

FIDO2/Webauthn vs. FIDO U2F

- Example FIDO2/WebAuthn authenticator flows:
  - **Single factor**: Username + FIDO2 credential
  - **Second factor**: Username + password + FIDO2 credential
  - **Password-less MFA**: Username + FIDO2 credential + PIN
  - **Password- and username-less single factor**: FIDO2 discoverable credential (a '*discoverable credential*' stores user data on the authenticator - a.k.a. resident key)
  - **Password- and username-less MFA**: FIDO2 discoverable credential + PIN
- Backwards-compatible with FIDO U2F authenticators
  - **Single factor**: Username + FIDO U2F credential
  - **Second factor**: Username + password + FIDO U2F credential

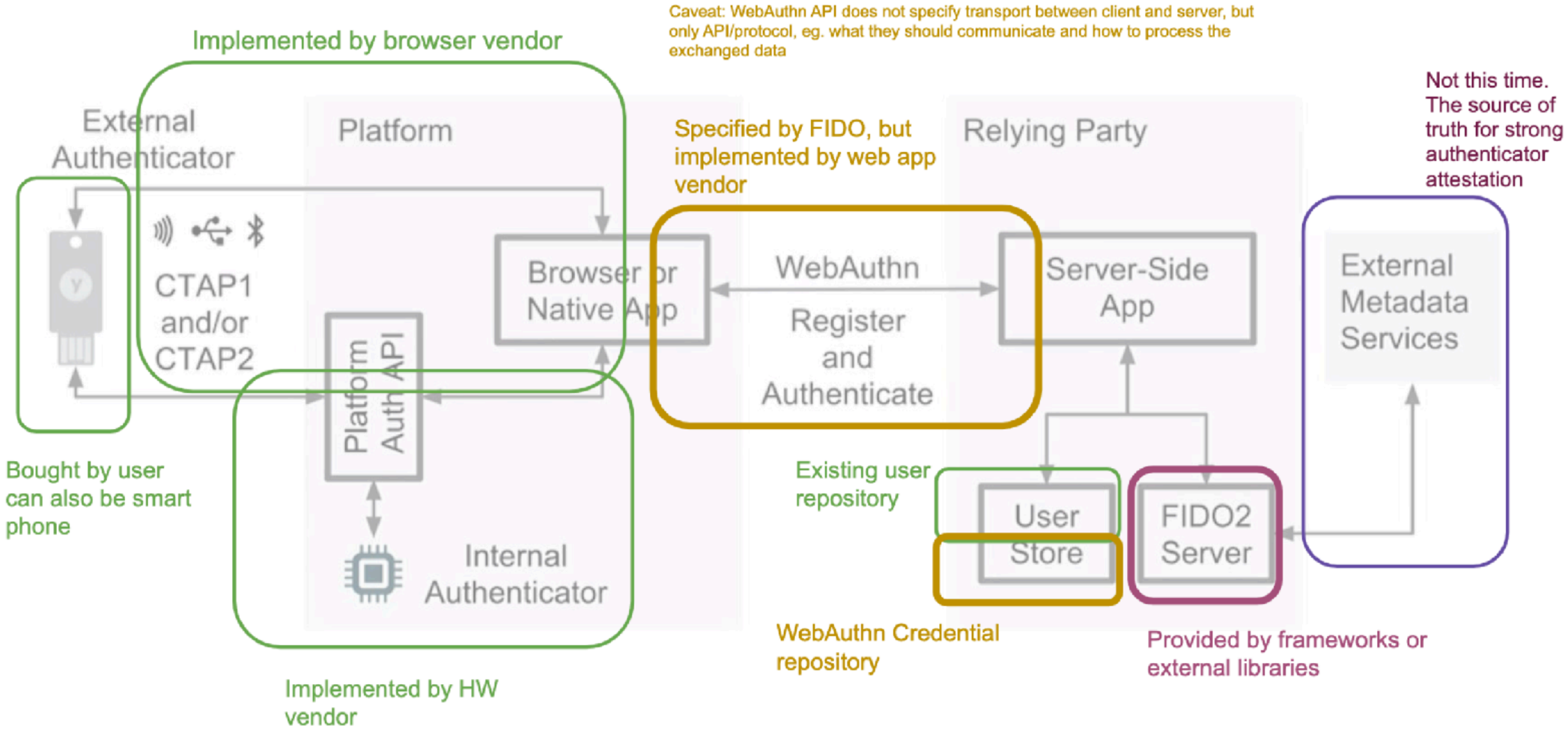
Source: Webauthn Developer Guide

Webauthn flow



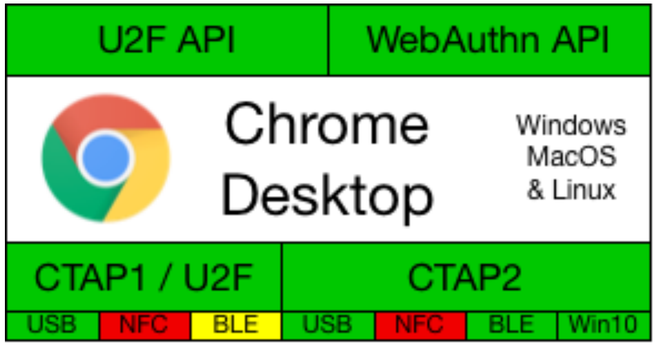
Source: https://github.com/bodik/flask-webauthn-example/

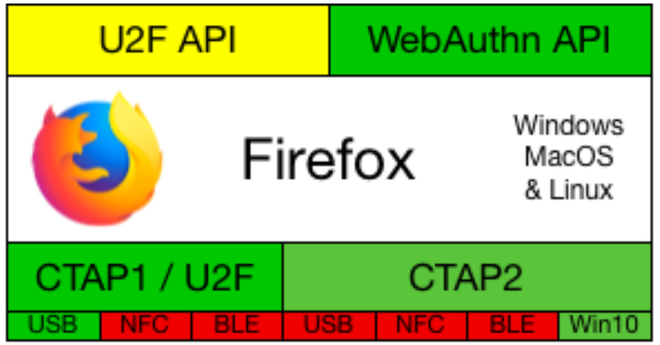
Webauthn flow

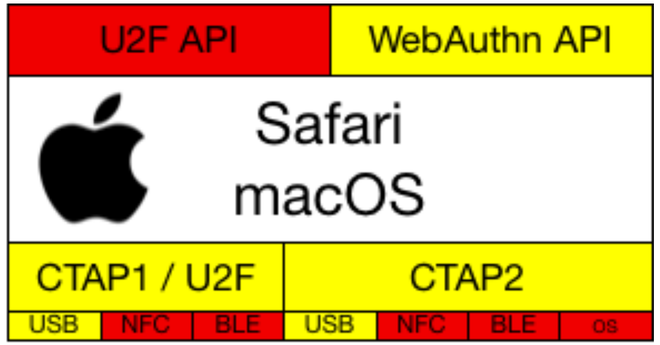


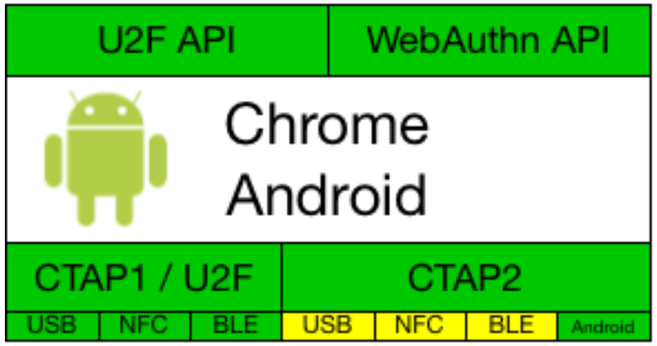
Source: https://github.com/bodik/flask-webauthn-example/

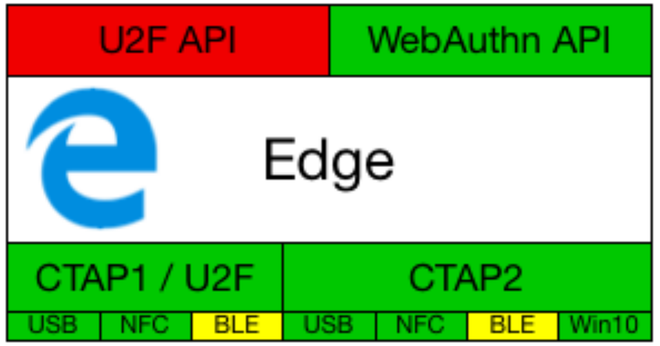
Browser support

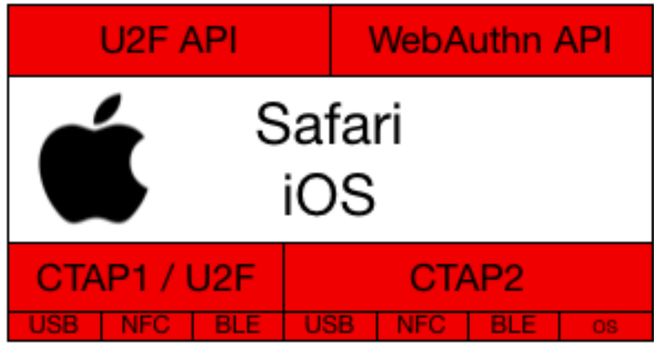












Legend:

Source: https://github.com/webauthn-open-source/fido2-webauthn-status

The downsides of FIDO

- Still not widely supported
- External tokens are expensive
  - **platform authenticators** are the way forward
- There is no recovery of lost authenticators
  - in addition, some authenticators may be **tied to a particular device**
  - the web app has to support multiple authenticators for the same account
- Virtually no support outside the web
  - OpenSSH 8.2 supports U2F-based SSH keys but both **client and server** needs to be updated

Questions

Ondřej Caletka
https://ondřej.caletka.nl