

**Universal Second Factor
authentication
or why 2FA today is
wubalubadubdub**

Yuriy Ackermann

Sr. Certification Engineer

@FIDOAlliance

twitter/github: @herrjemand

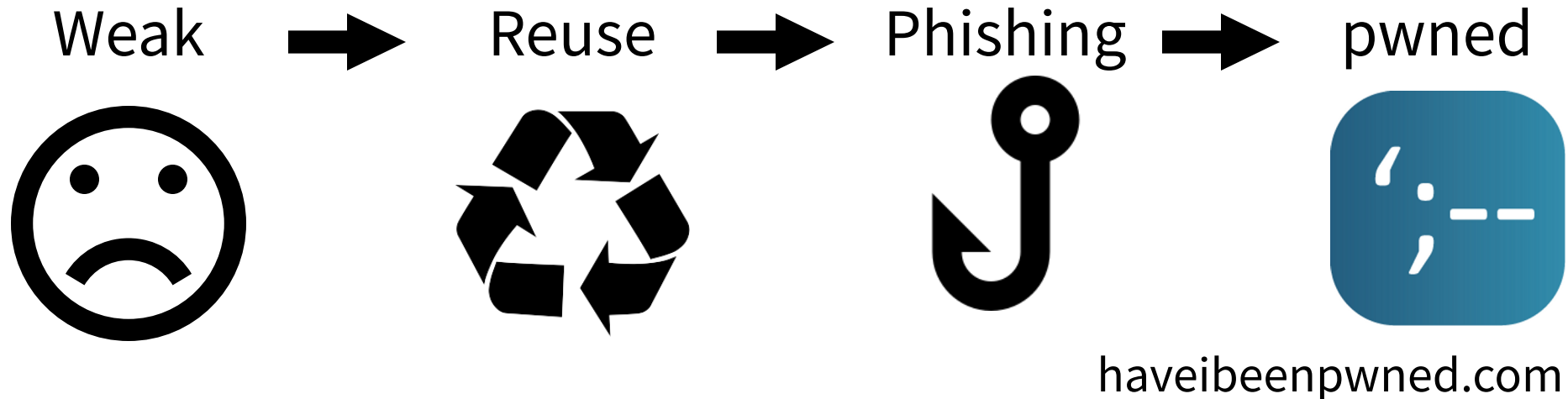


Today we will learn

- Why passwords not enough
- Why 2FA has not succeeded
- Introduction to U2F
- DEMO
- Q&A

Why not just passwords?

Typical passwords life cycle



SOLUTION!

Two Factor Authentication - aka 2FA

What is 2FA?

Passwords verify
2FA authenticate

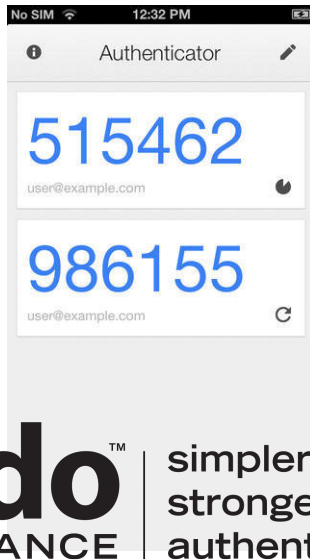
Do you use 2FA?

What does 2FA looks like?

Three main types

Apps

(TOTP and HOTP)



Tokens

(PKI and OTP)



SMS



So we solved it?

Right?

Why 2FA has not succeeded?

Apps

- Phishing!!
- UX
- Shared key
- Synced time

Tokens

- Cost
- DRIVERS
- Phishing
- UX
- Centralised
- Fragile

SMS

- Still phishable
- UX
- Privacy
- Security
 - SIM reissue
 - SIM spoof
- Coverage
- NIST Ban



Internet of Shit

@internetofshit



Читаю

Two factor sucks, so... why not just point a webcam at your token?

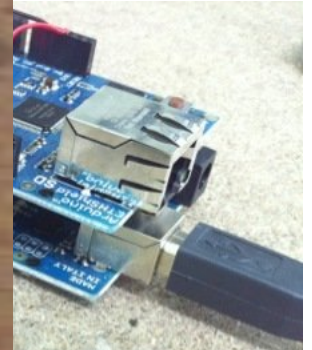
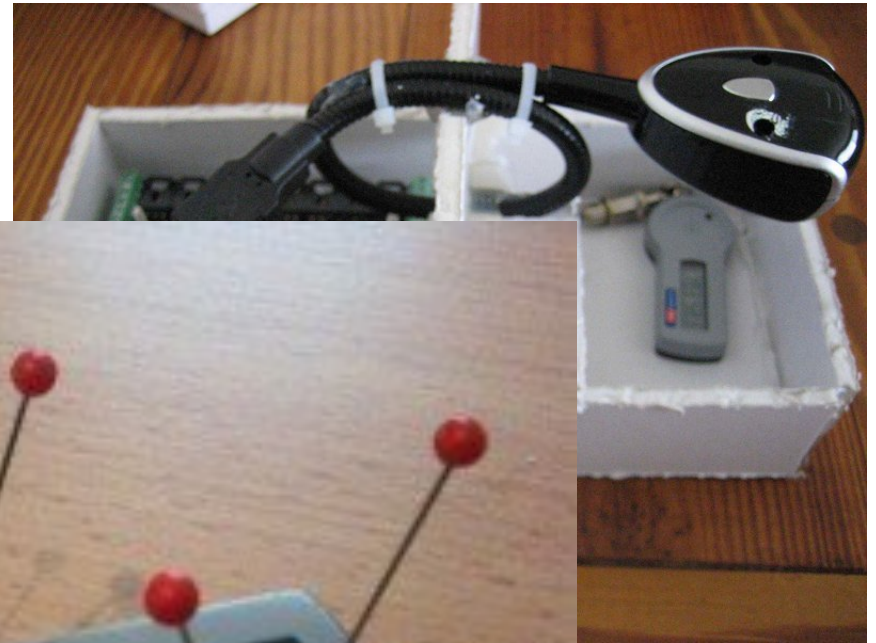
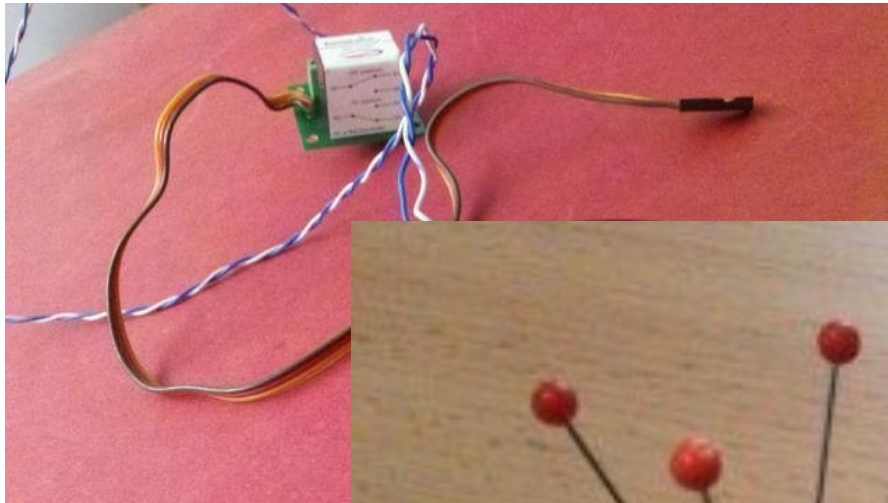
shodan.io/host/198.2.49.... via @djvc1993

Показать перевод

D-Link/Airlink IP webcam http config Version: 1.0

```
HTTP/1.0 200 OK
Server: Camera Web Server/1.0
Author: Steven Wu
MIME-version: 1.0
Cache-Control: no-cache
Content-Type: text/html
Content-Length: 1681
```





Current state of 2FA

W U B A
L U B A
D U B D U B...
.....



I am in the deep pain,
please help!

So how do we solve it?

We need:

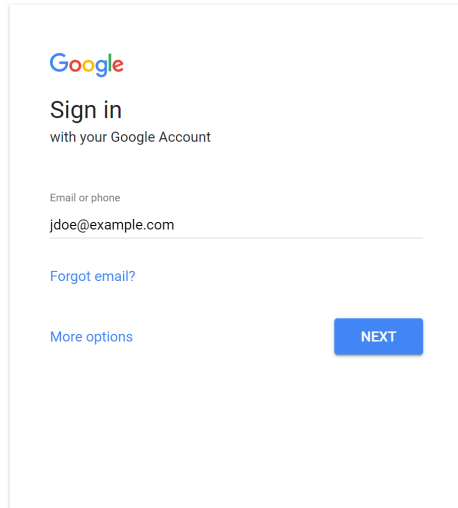
- Easy to use
- Open
- Secure
- Standardized

protocol.

Introducing Universal Second Factor aka FIDO U2F

How does U2F works?

User layer



Google

Sign in
with your Google Account

Email or phone
jdoe@example.com

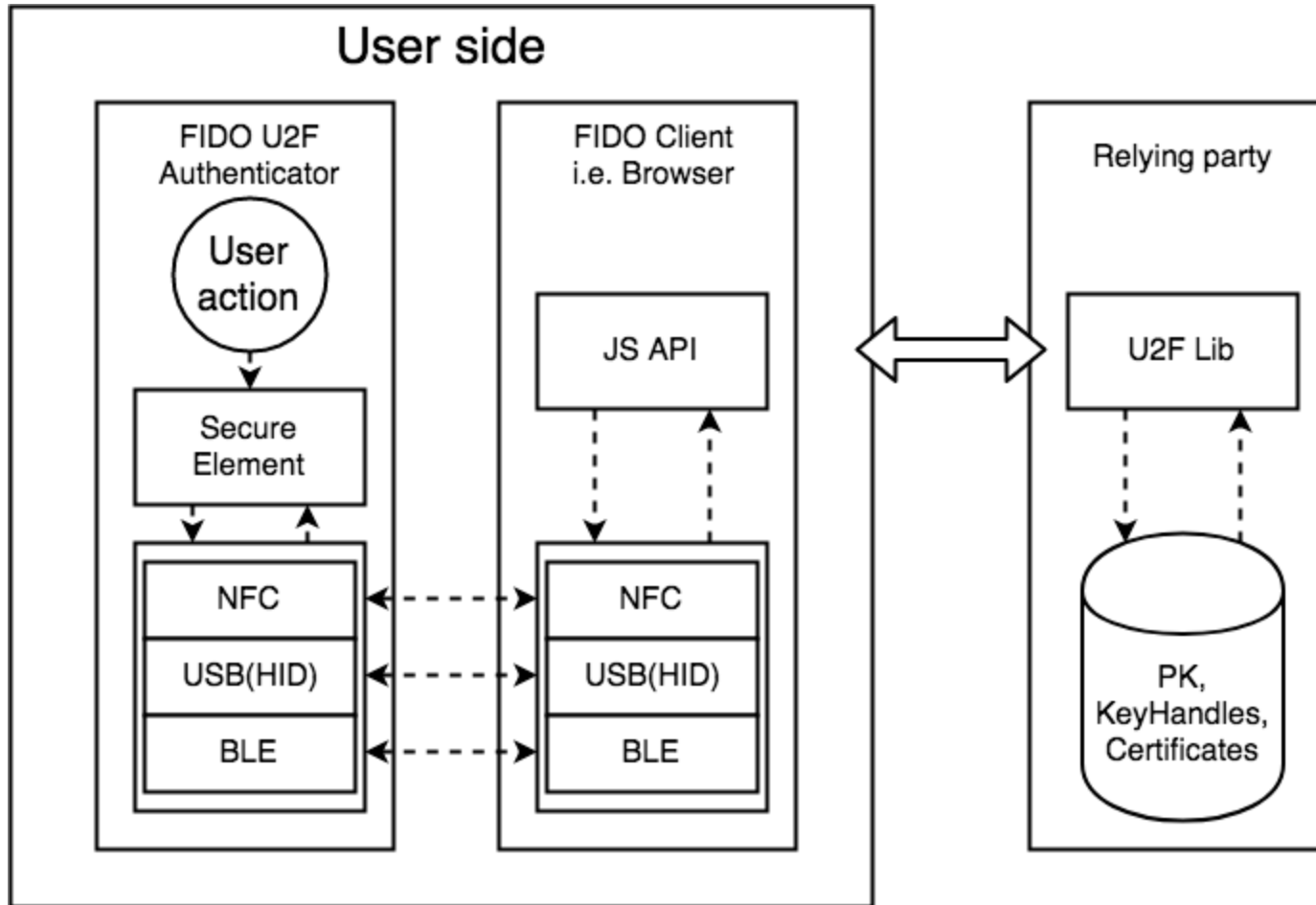
[Forgot email?](#)

[More options](#)

NEXT

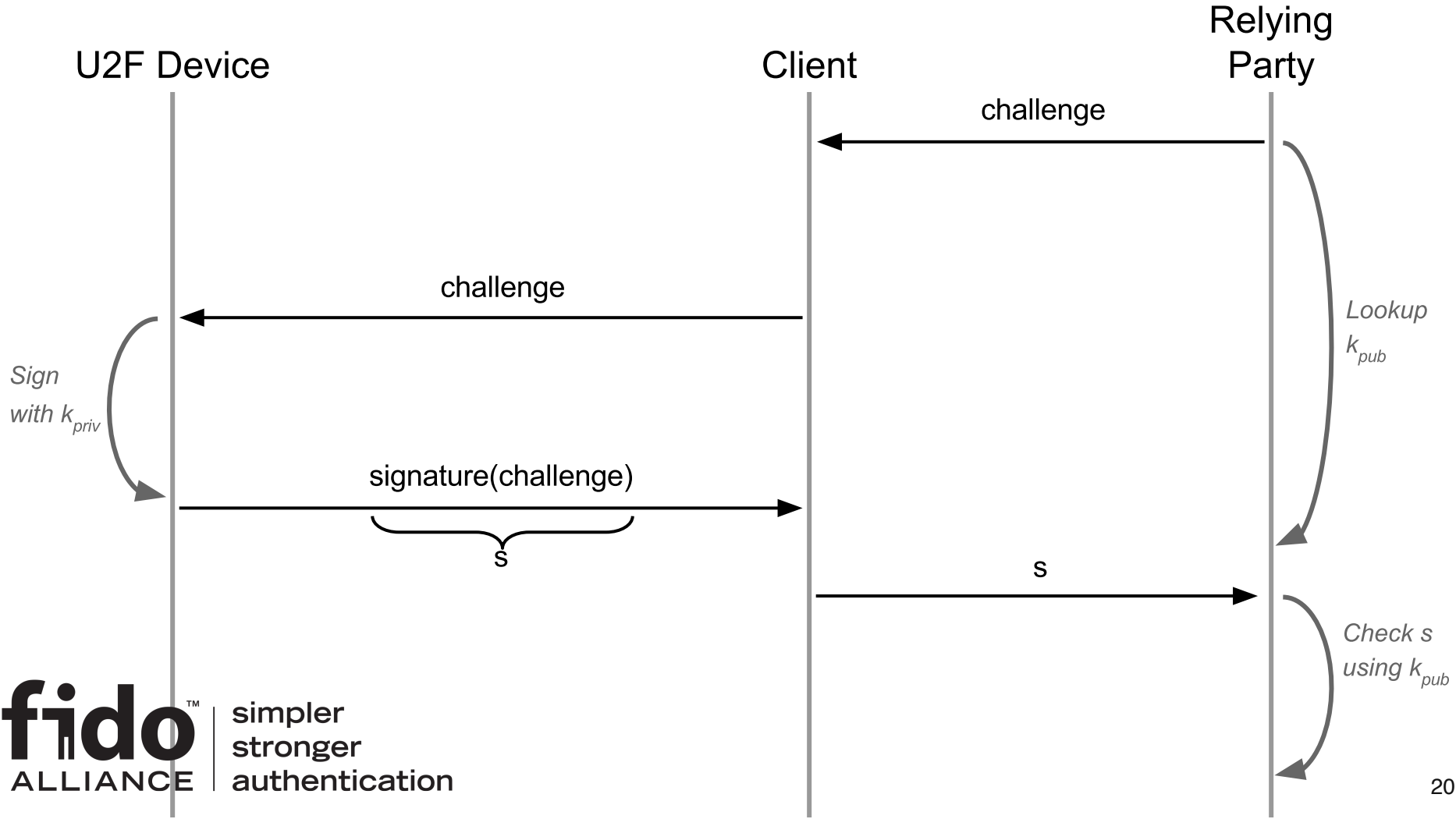


Browser layer

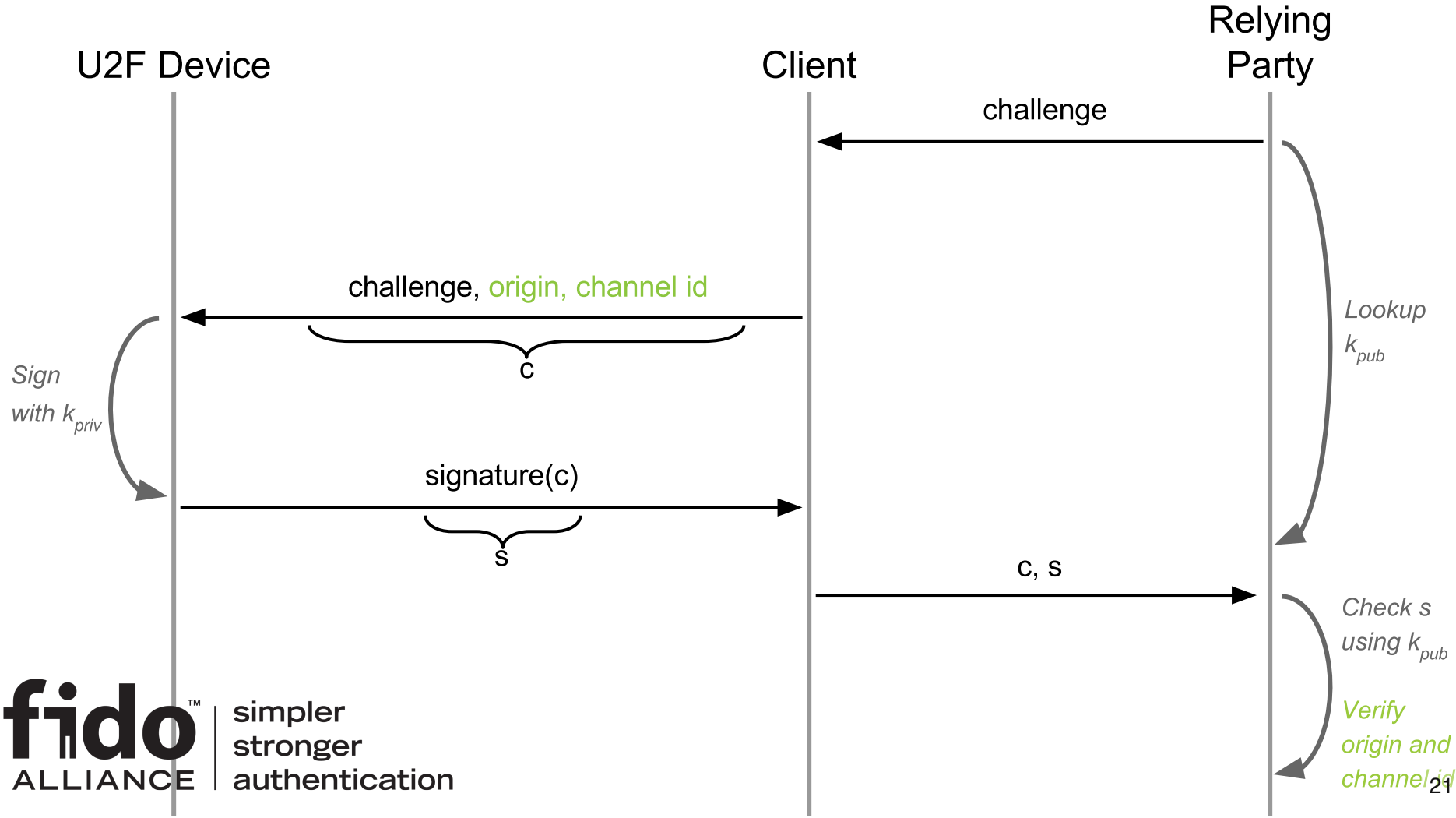


Protocol Layer

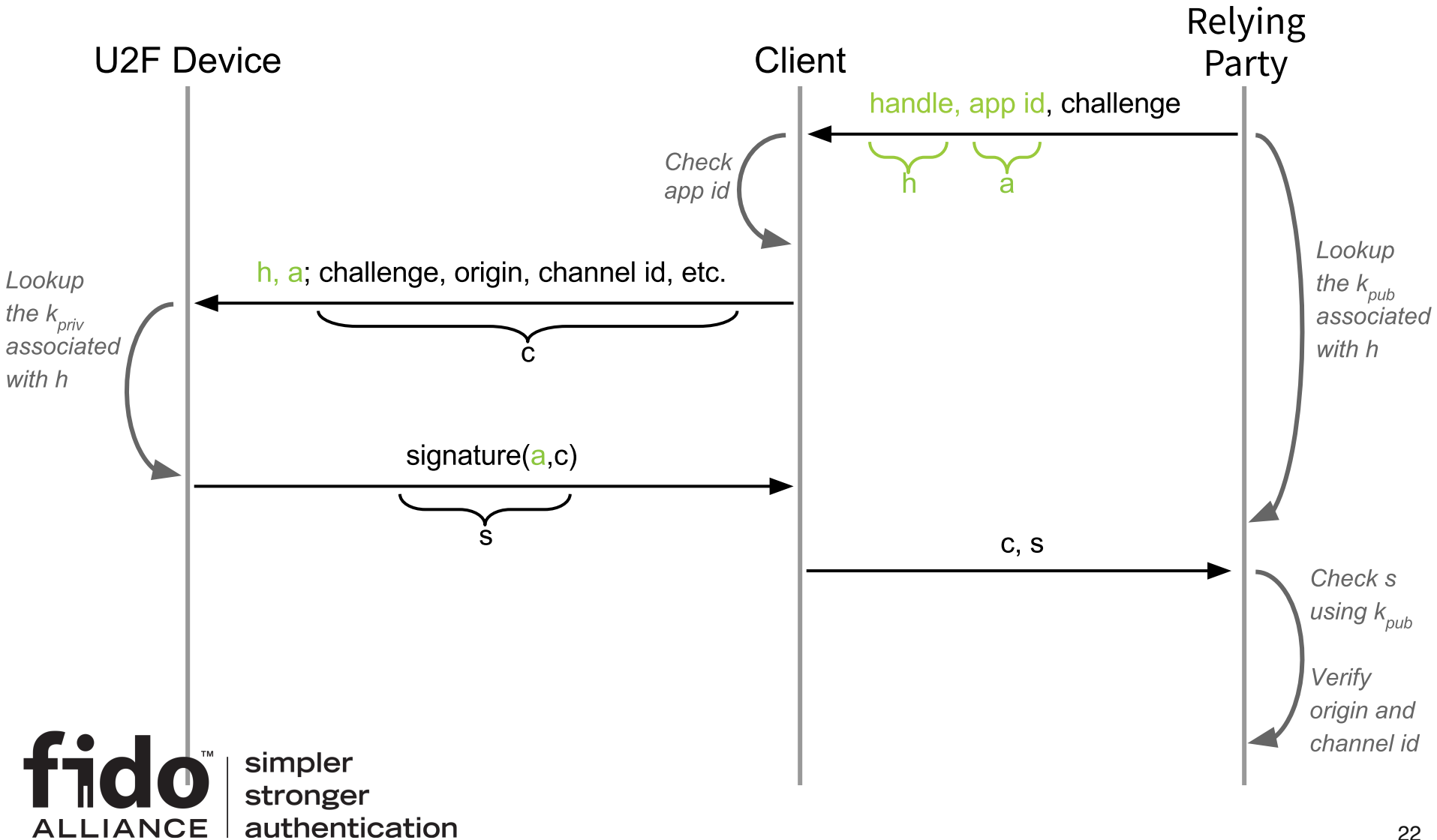
Step one: Challenge-Response



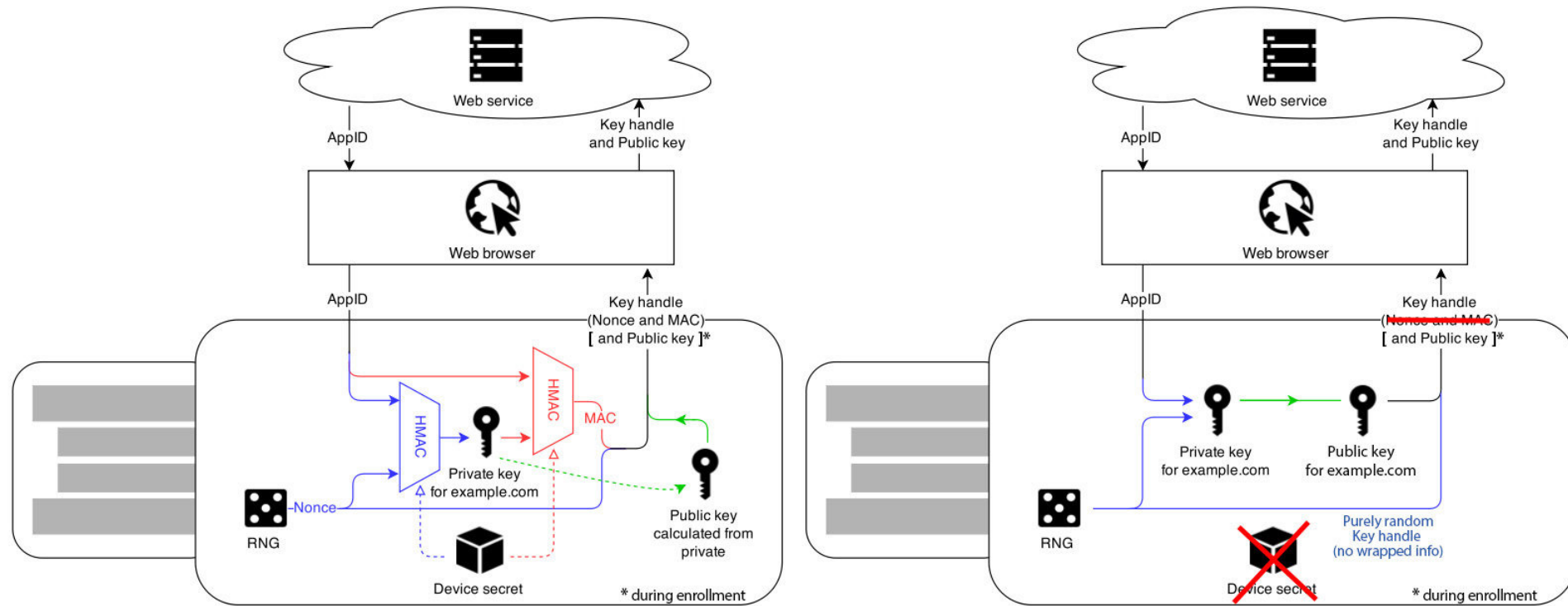
Step two: Phishing protection



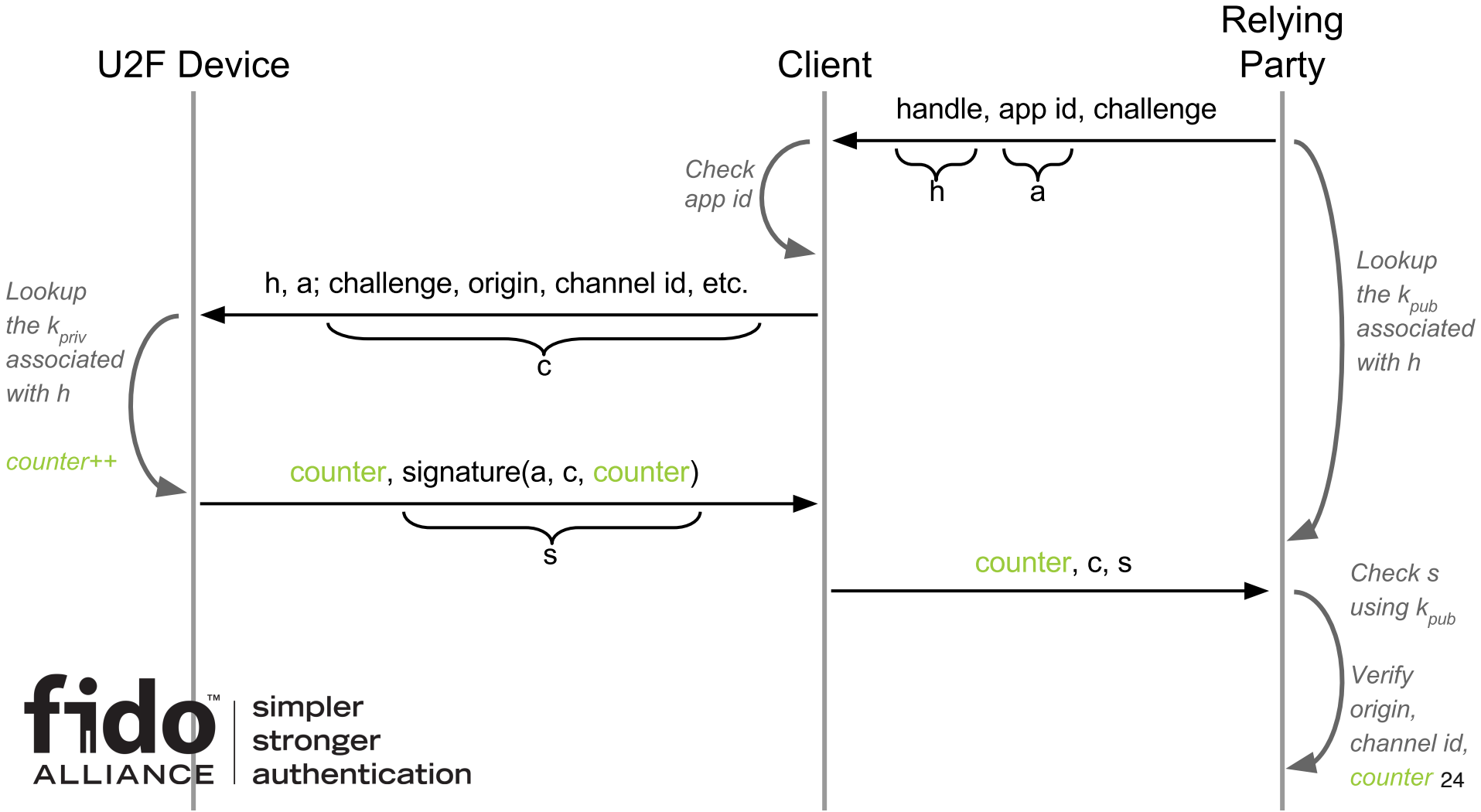
Step three: Application-specific key-pair



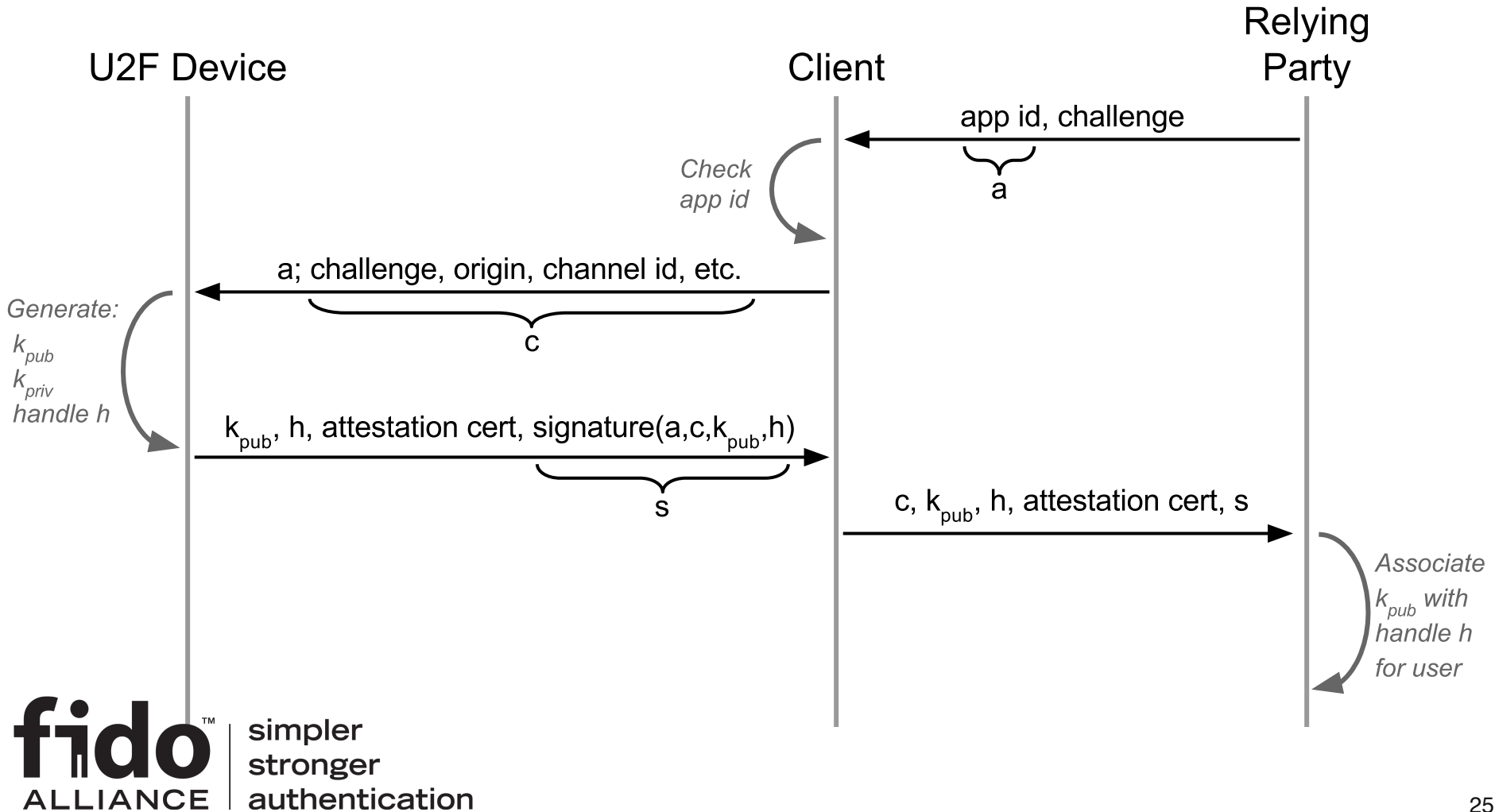
To Wrap, or not to Wrap?



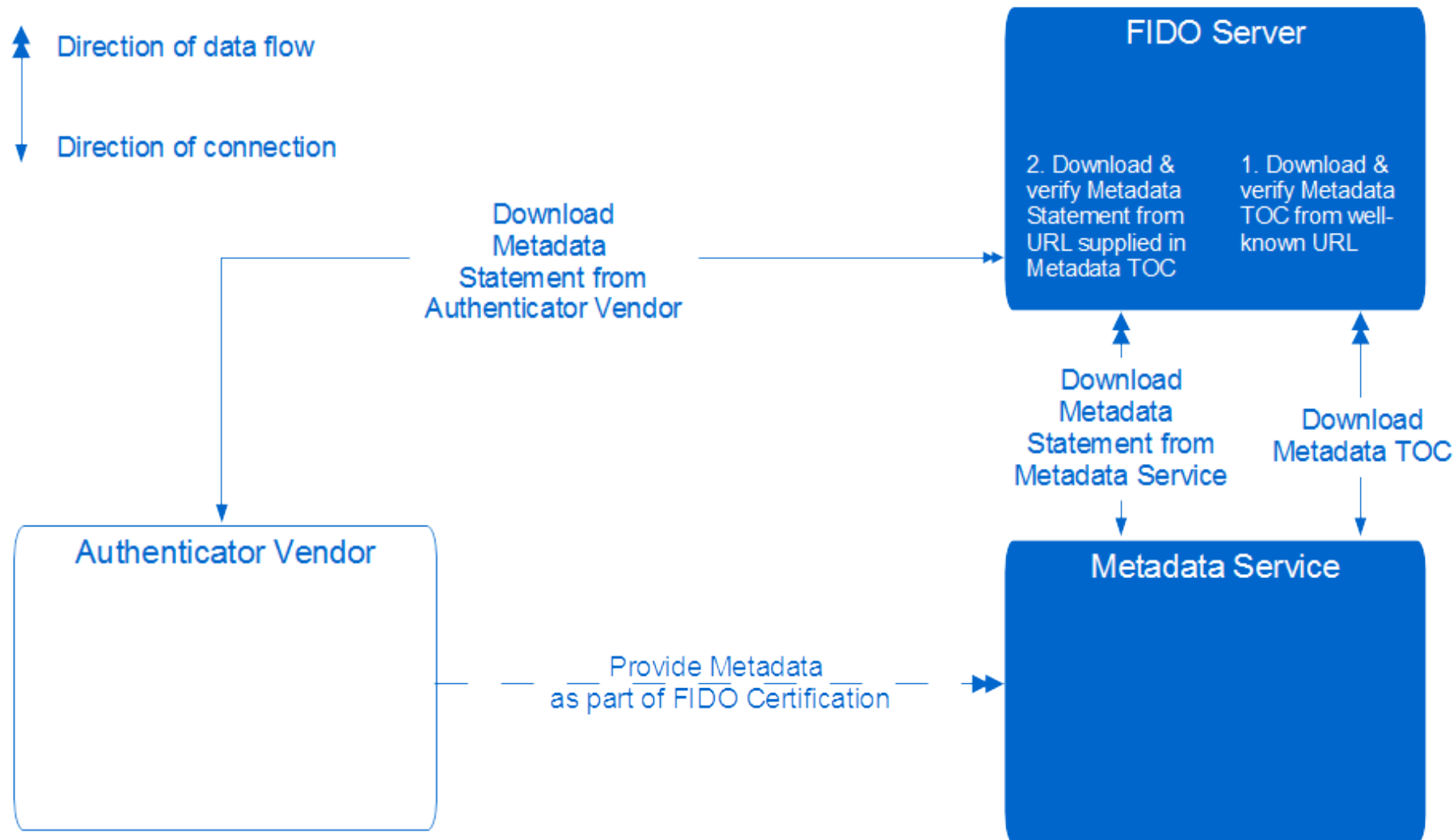
Step four: Replay Attack Protection



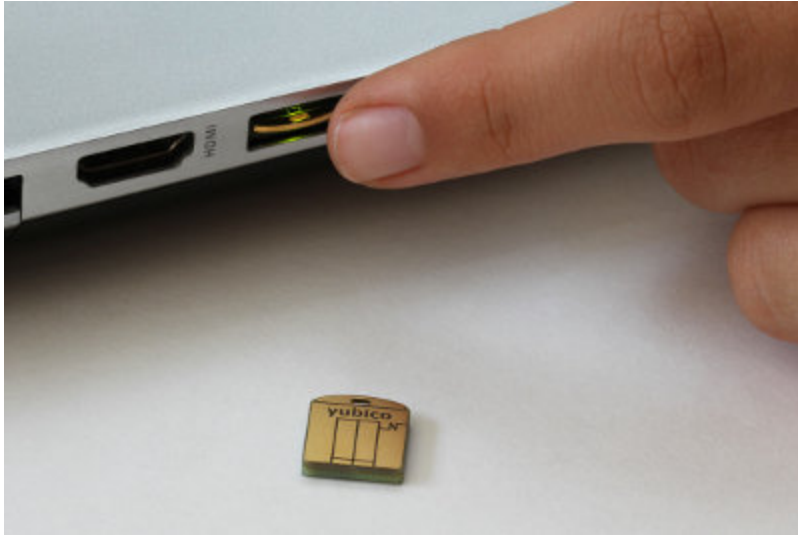
Step five: Device attestation



Metadata service



Step five and a half: Key exercise protection



User must confirm their decision to perform 2FA, by performing user gesture

e.g.

Pressing button

Fingerprint

Retina scan

Pincode

Solving Rubikscube

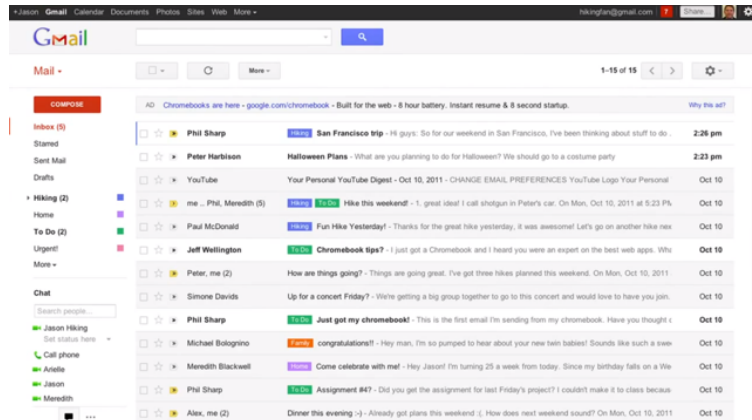
Remembering your wife's birthday.

...anything you want.

Multiple identifiers

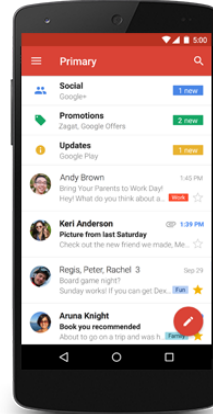
GMail

Web



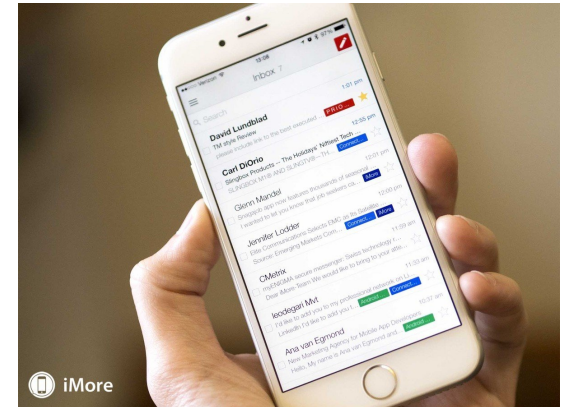
mail.google.com

Android



apk-key-
hash:FD18FA

iOS



com.google.SecurityKe
y.dogfood

How do we deal with it?

fidoTM
ALLIANCE

simpler
stronger
authentication

Application Facets

```
{
  "trustedFacets": [{
    "version": { "major": 1, "minor" : 0 },
    "ids": [
      "https://accounts.google.com",
      "https://myaccount.google.com",
      "https://security.google.com",

      "android:apk-key-hash:FD18FA800DD00C0D9D7724328B6D...",
      "android:apk-key-hash:/Rj6gA3QDA2ddyQyi21JXly6gw9D...",

      "ios:bundle-id:com.google.SecurityKey.dogfood"
    ]
  }]
}
```

MUST be served over VALID HTTPS!

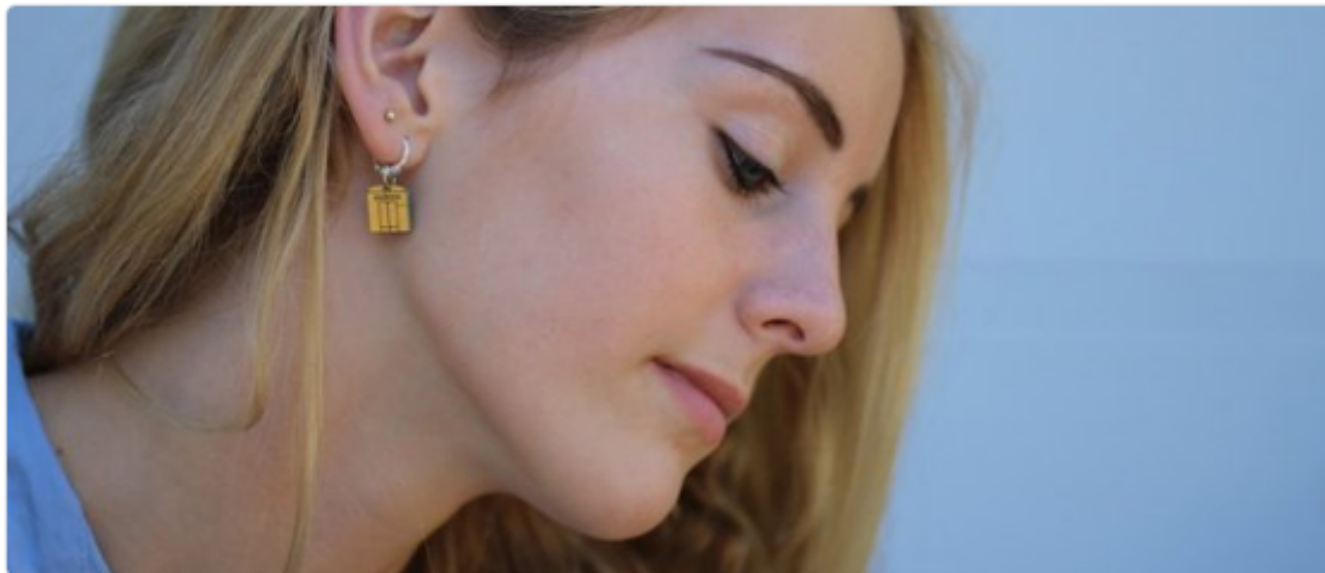
...no self signed certs.

Implementations



@NotThatNiemand @jessysaurusrex -
YubiKeys make nice earrings as well. :)

 Показать перевод



ОТМЕТКИ «НРАВИТСЯ»

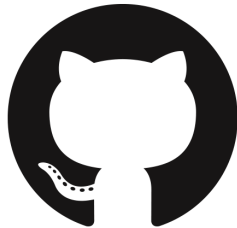
2



11:55 - 4 марта 2016 г.



Current users



Browser support



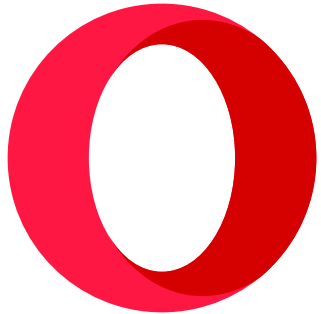
Yes



Yes*
(Nightly)



No*
(Soon...)



Yes



Maybe?

WebAuthN

A W3C standard for PublicKey credential authentication

<https://www.w3.org/Webauthn/>

Today we learned

- Passwords are hard
- 2FA is wubalubadubdub, and we need to do something about it.
- FIDO U2F is sweet.
 - Protocol is cute
 - You can have multiple identities
 - There are existing solutions...
 - ...and people do use it

DEMO

Security considerations

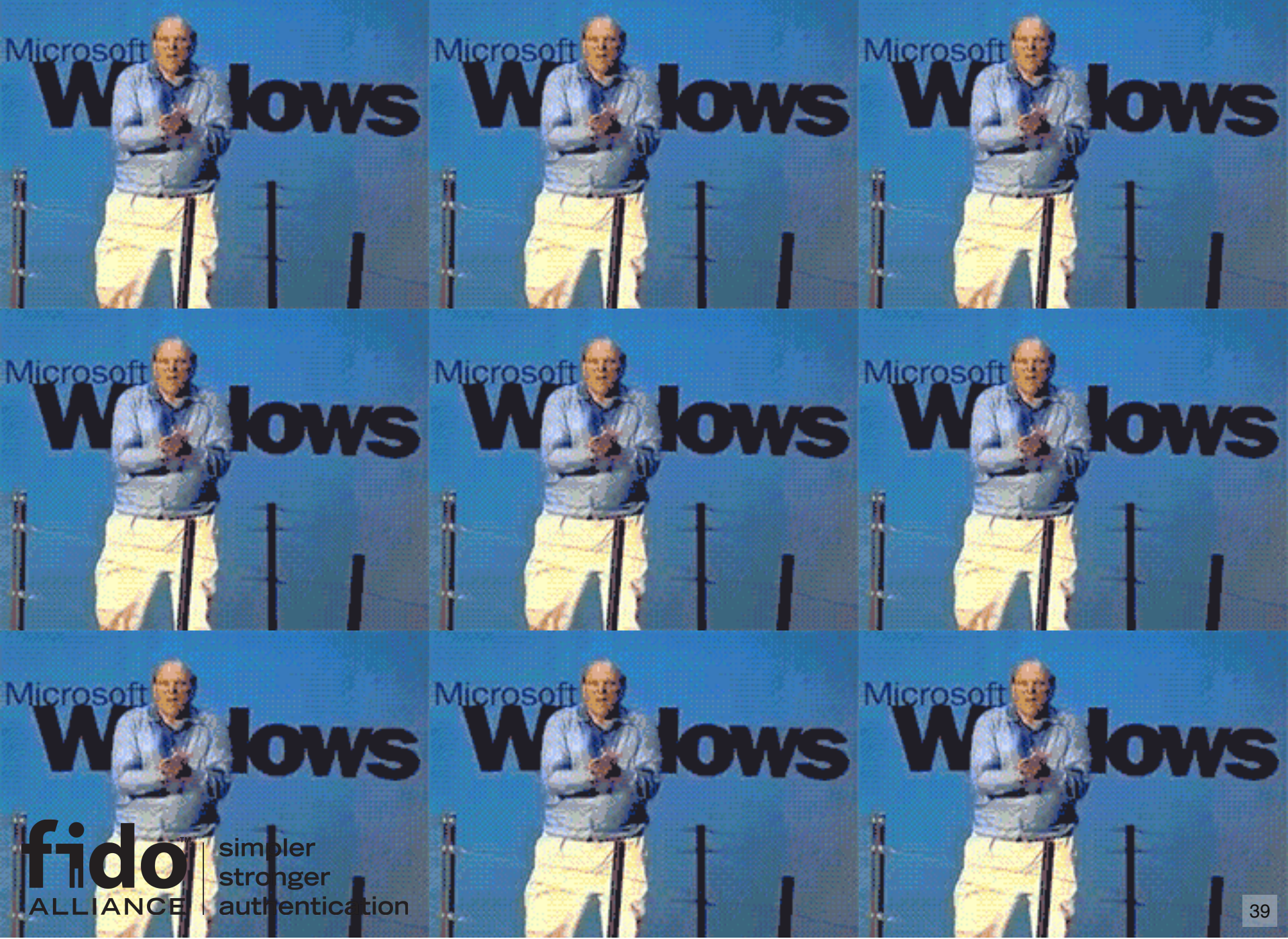
- You must use HTTPS
- Start using TLS Channel ID's
- U2F is just 2FA. Don't use as primary factor.

Things to play with

- <https://github.com/Yubico/pam-u2f>
- <https://github.com/Yubico/python-u2flib-server>
- <https://github.com/Yubico/python-u2flib-host>
- <https://github.com/herrjemand/flask-fido-u2f>
- <https://github.com/gavinwahl/django-u2f>
- <https://github.com/google/u2f-ref-code>
- <https://github.com/conorpp/u2f-zero>

Specs and data

- <https://developers.yubico.com/U2F/>
- <https://fidoalliance.org/specifications/download/>
- <https://github.com/LedgerHQ> <- JavaCard
- FIDO Dev (fido-dev) mailing list



fido | simpler
ALLIANCE | stronger
authentication

Questions?

twitter/github: @herrjemand

Quick thanks to
Feitian and Yubico
for swag!



Thank you
OWASP!