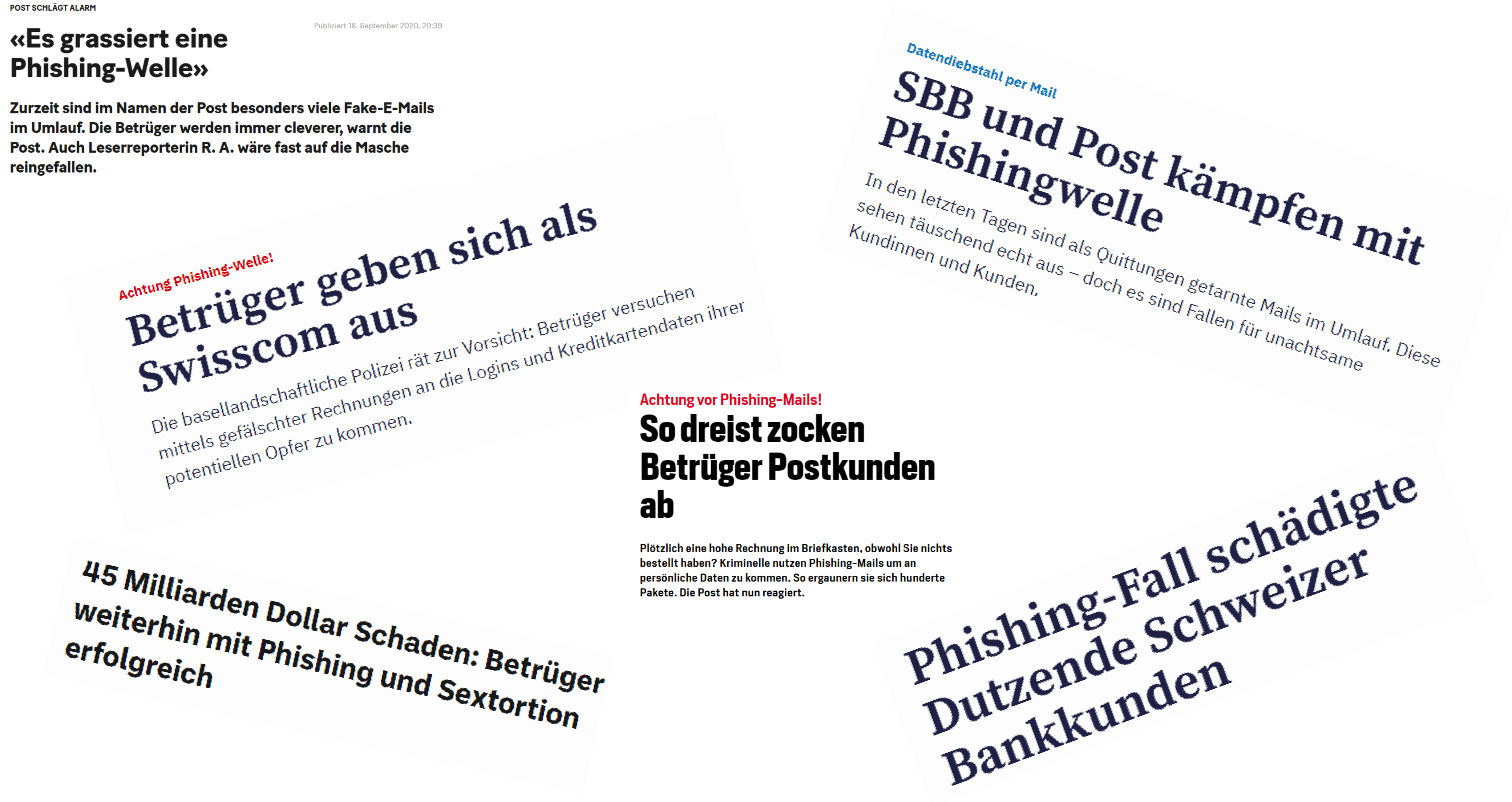
FIDO2 – No more Phishing

Online Beer-Talk

25th March 2021, 17:00

Yves Bieri – IT Security Analyst – yves.bieri@compass-security.com



POST SCHLÄGT ALARM

Publiziert 18. September 2020, 20:39

«Es grassiert eine Phishing-Welle»

Zurzeit sind im Namen der Post besonders viele Fake-E-Mails im Umlauf. Die Betrüger werden immer cleverer, warnt die Post. Auch Leserreporterin R. A. wäre fast auf die Masche reingefallen.

Datendiebstahl per Mail

SBB und Post kämpfen mit Phishingwelle

In den letzten Tagen sind als Quittungen getarnte Mails im Umlauf. Diese sehen täuschend echt aus – doch es sind Fallen für unachtsame Kundinnen und Kunden.

Achtung Phishing-Welle!

Betrüger geben sich als Swisscom aus

Die basellandschaftliche Polizei rät zur Vorsicht: Betrüger versuchen mittels gefälschter Rechnungen an die Logins und Kreditkartendaten ihrer potentiellen Opfer zu kommen.

Achtung vor Phishing-Mails!

So dreist zocken Betrüger Postkunden ab

Plötzlich eine hohe Rechnung im Briefkasten, obwohl Sie nichts bestellt haben? Kriminelle nutzen Phishing-Mails um an persönliche Daten zu kommen. So ergaunern sie sich hunderte Pakete. Die Post hat nun reagiert.

45 Milliarden Dollar Schaden: Betrüger weiterhin mit Phishing und Sextortion erfolgreich

Phishing-Fall schädigte Dutzende Schweizer Bankkunden

FIDO2

🍺 “Traditional” 2FA 🍺

Authentication Factors

Authentication may involve different factors:

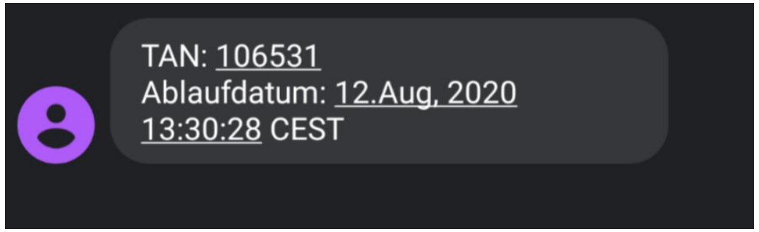
- To ***KNOW*** something
  - Password, PIN
- To ***OWN*** something
  - Smartcard, SecurId, Safeword, Vasco, OTP, Yubikey
- To ***BE*** something
  - Fingerprint, Iris, Voice, Face

Multi-Factor Authentication

- Combination of at least 2 ***DIFFERENT*** factors

Possession Factor Examples

RSA SecurID



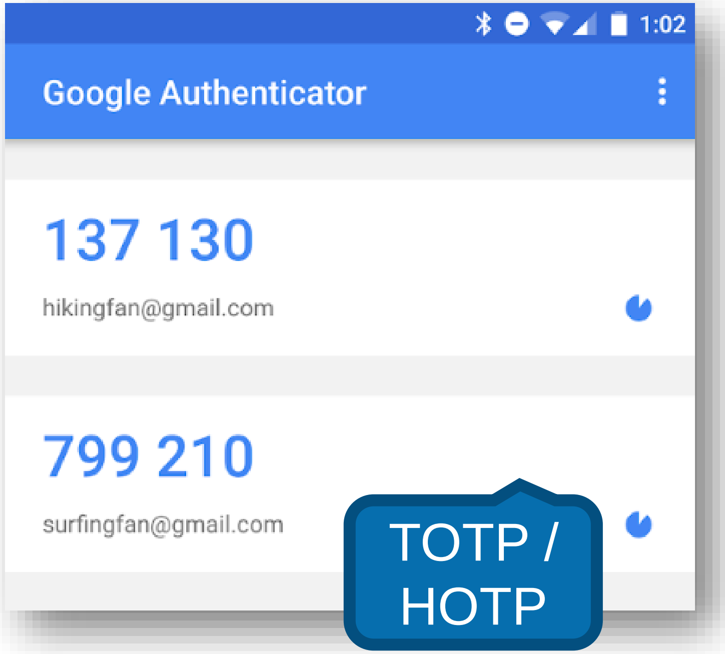
TAN: 106531
Ablaufdatum: 12.Aug, 2020
13:30:28 CEST

SmartCard

PhotoTAN / Cronto

MobileID

mTAN / SMS



1:02

Google Authenticator

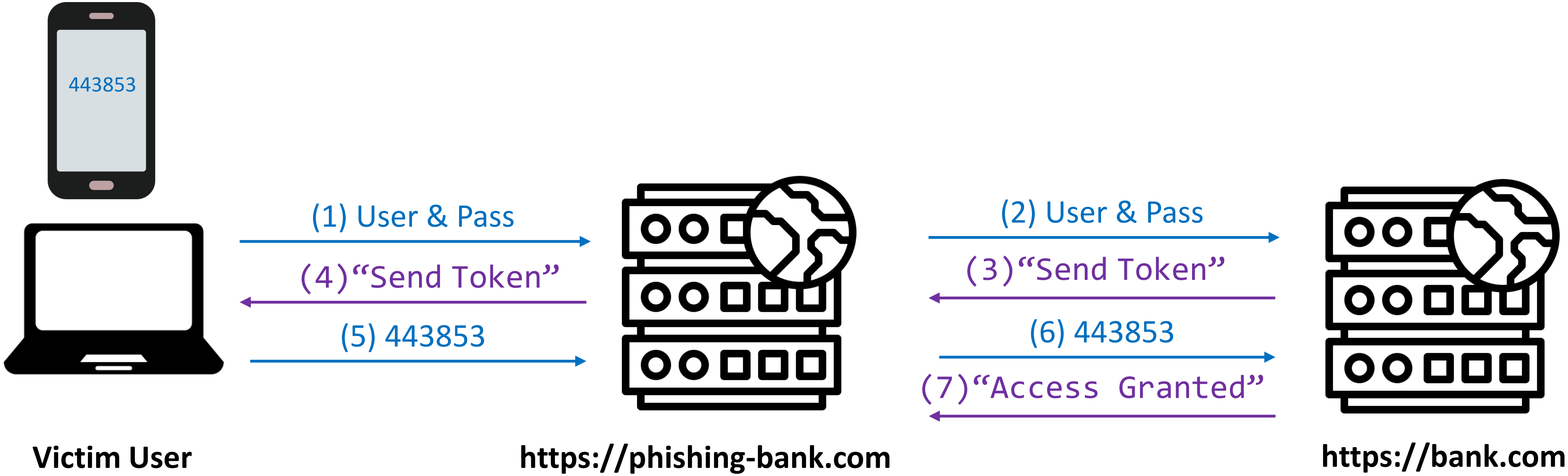
137 130
hikingfan@gmail.com

799 210
surfingfan@gmail.com

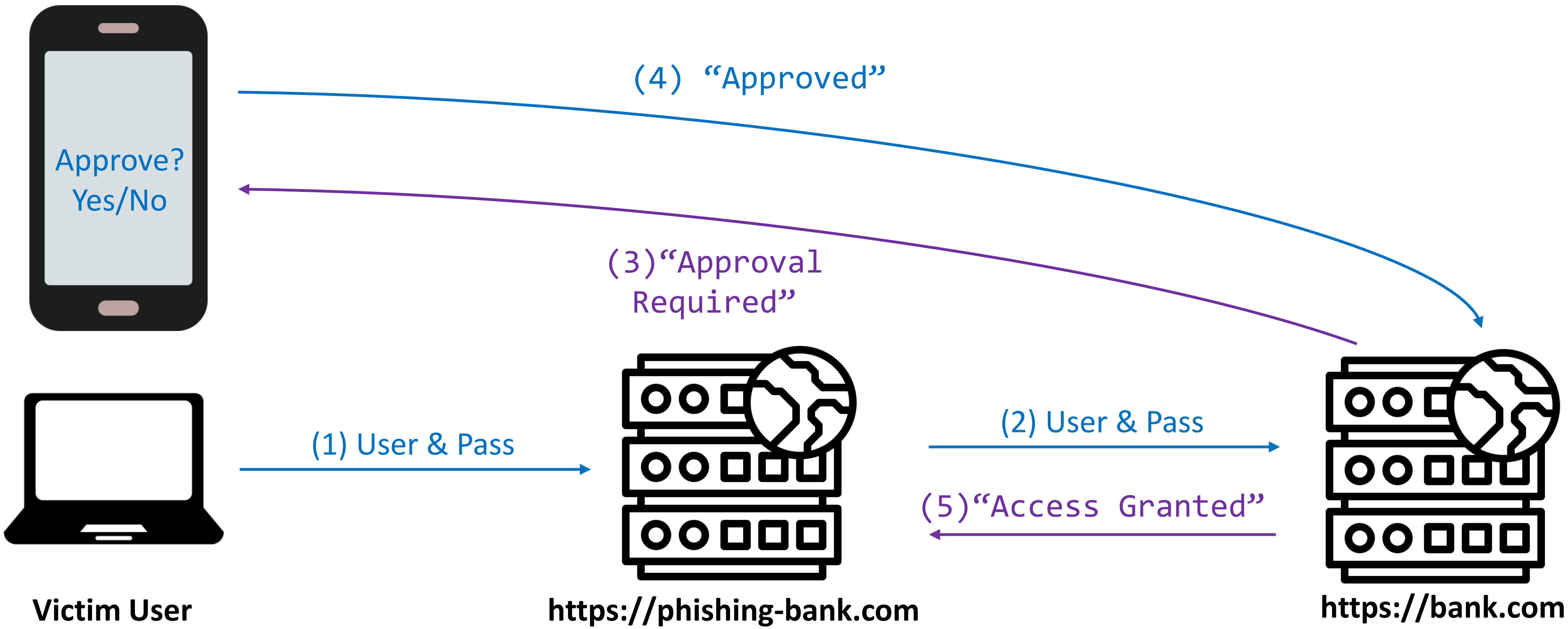
TOTP / HOTP

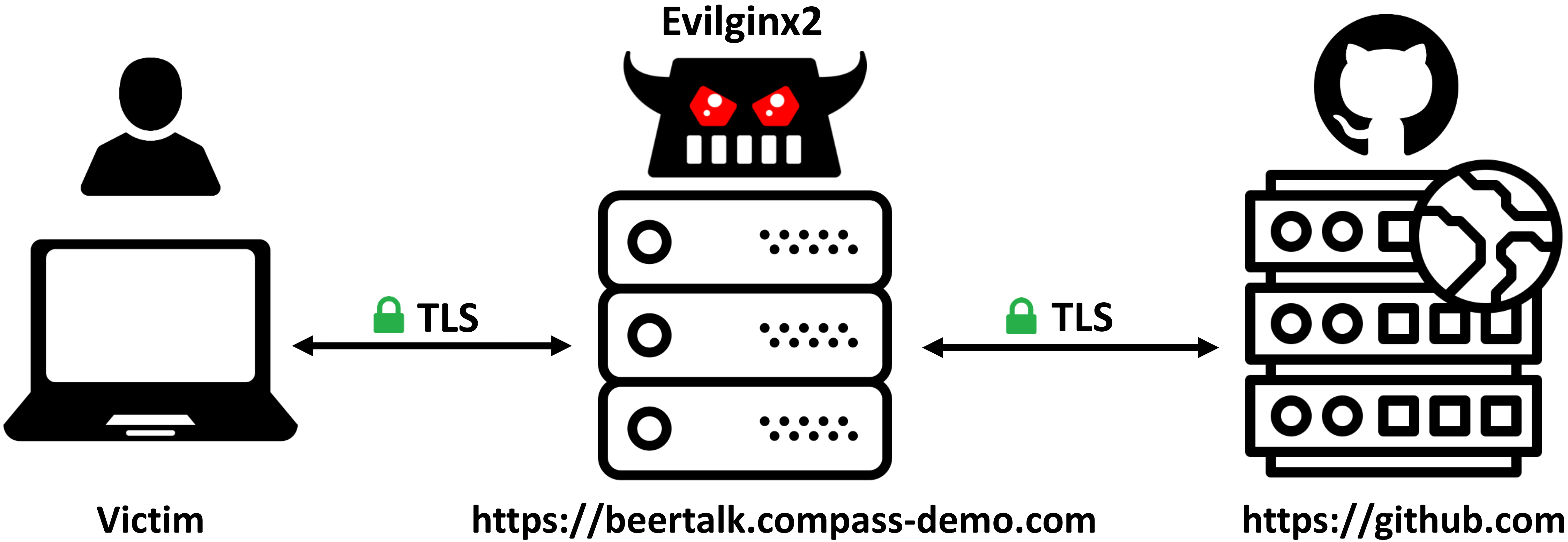
Most second factor mechanisms do not protect against credential phishing

2FA Phishing



HOTP / TOTP Phishing with Push Notification





- gitzhub.com
- githujb.com
- githuв.com
- githụb.com

DEMO

Phishing Solutions

User Awareness Campaigns

- Costly, time intensive, and ineffective after a while

Traditional 2FA

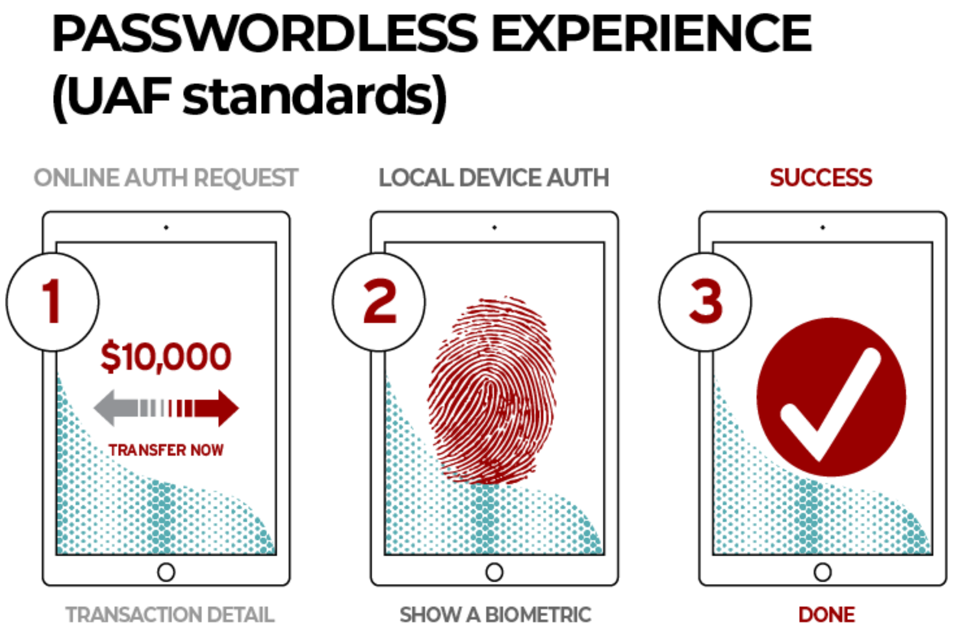
- Useful but attackers can bypass it

FIDO / FIDO2 Specifications

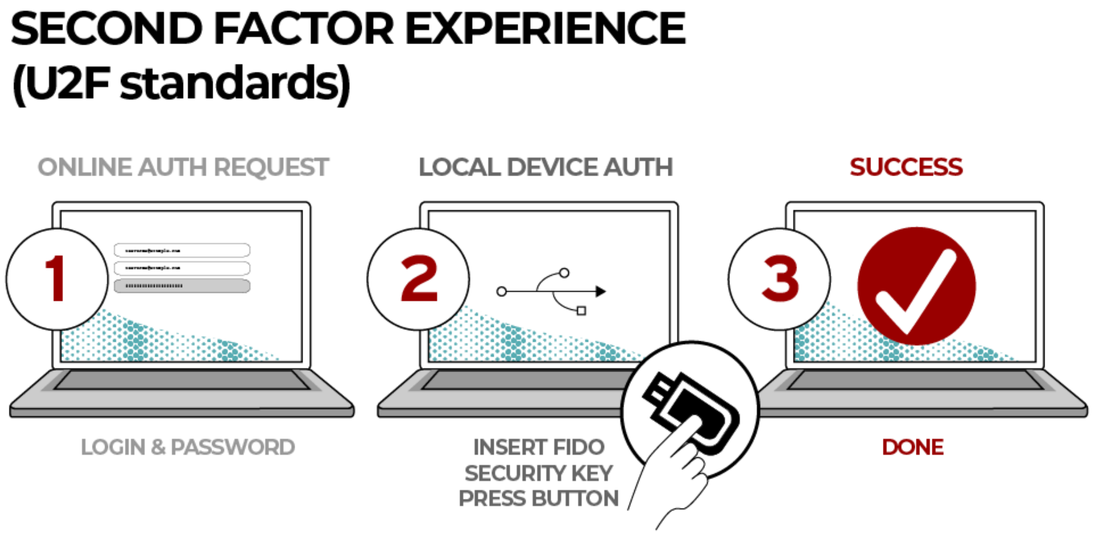
- A new set of specifications that define ***phishing-resistant*** authentication mechanisms

🍺 U2F, UAF, CTAP, WebAuthn, FIDO, FIDO2 🍺 oh my…

FIDO (Fast Identity Online)



PASSWORDLESS EXPERIENCE
(UAF standards)

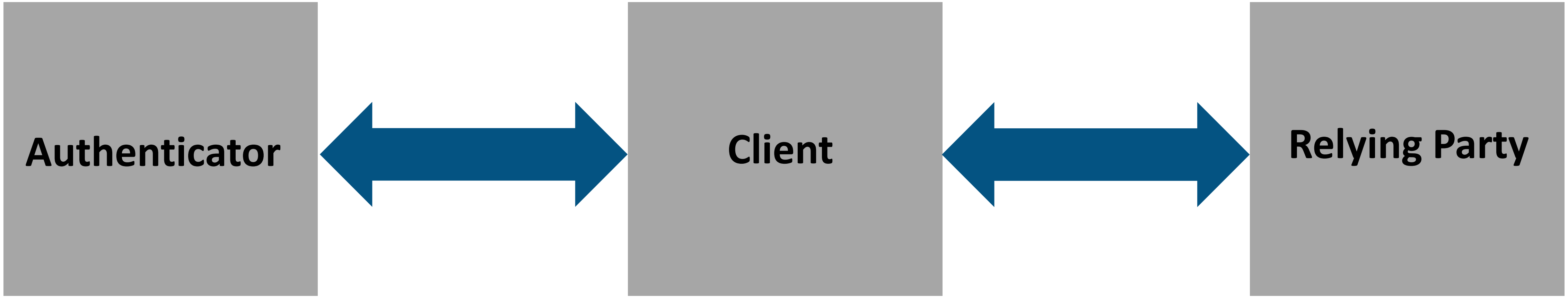


SECOND FACTOR EXPERIENCE
(U2F standards)

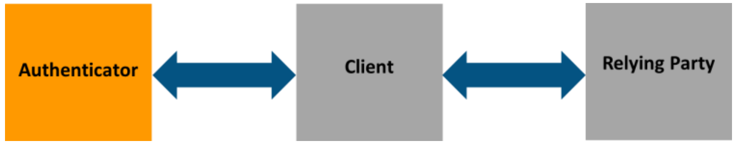
The FIDO2 specification replaces FIDO U2F and FIDO UAF

Source: https://fidoalliance.org/specifications/

FIDO2 Building Blocks



FIDO2 Authenticators



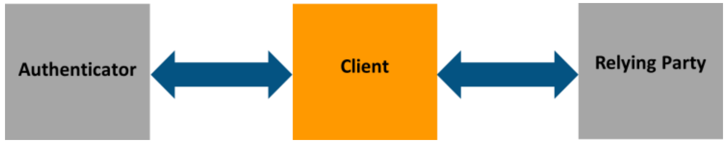
https://www.yubico.com/

https://cloud.google.com/titan-security-key/

https://onlykey.io/

https://solokeys.com/

FIDO2 Clients



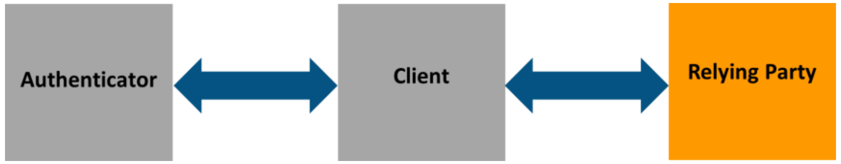
Authenticator

Client

Relying Party

Source: https://fidoalliance.org/fido2/)

FIDO2 Relying Parties


Authenticator
Client
Relying Party

Google

Microsoft

GitHub

PingIdentity®

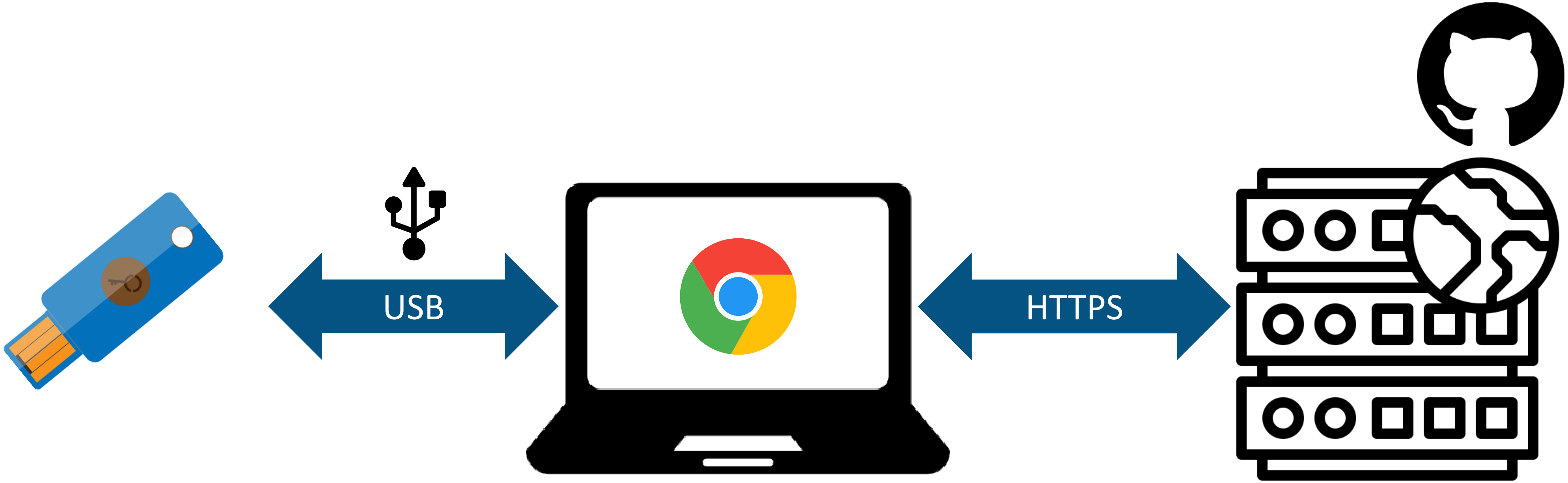
amazon

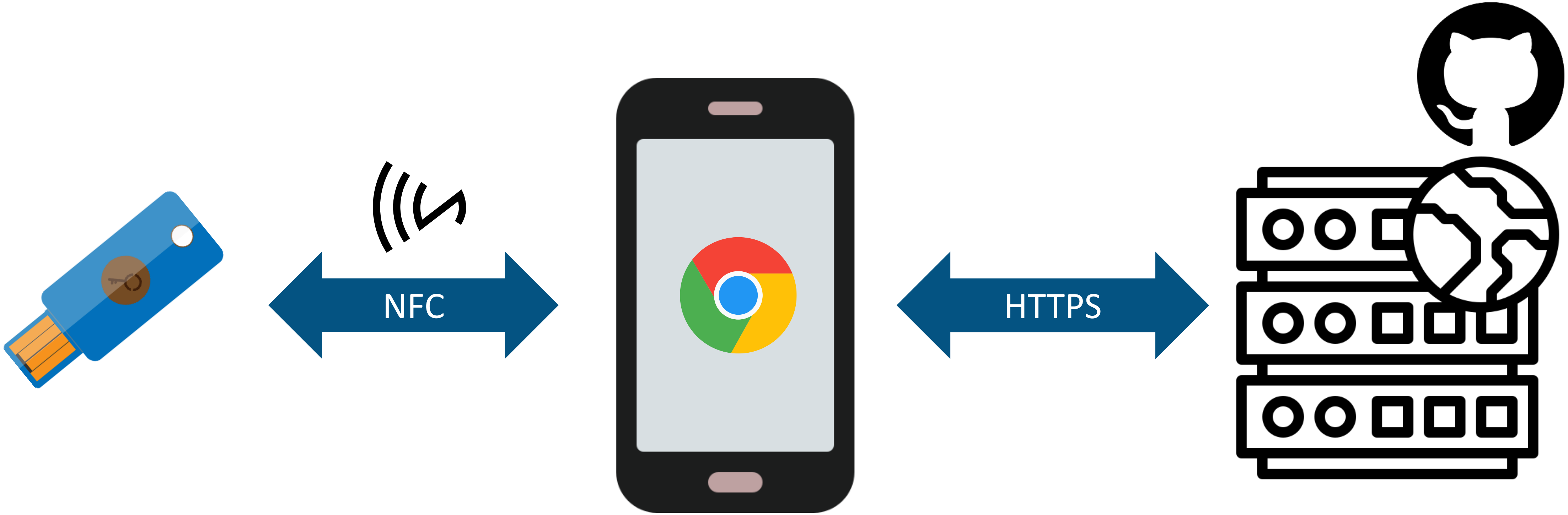
ebay

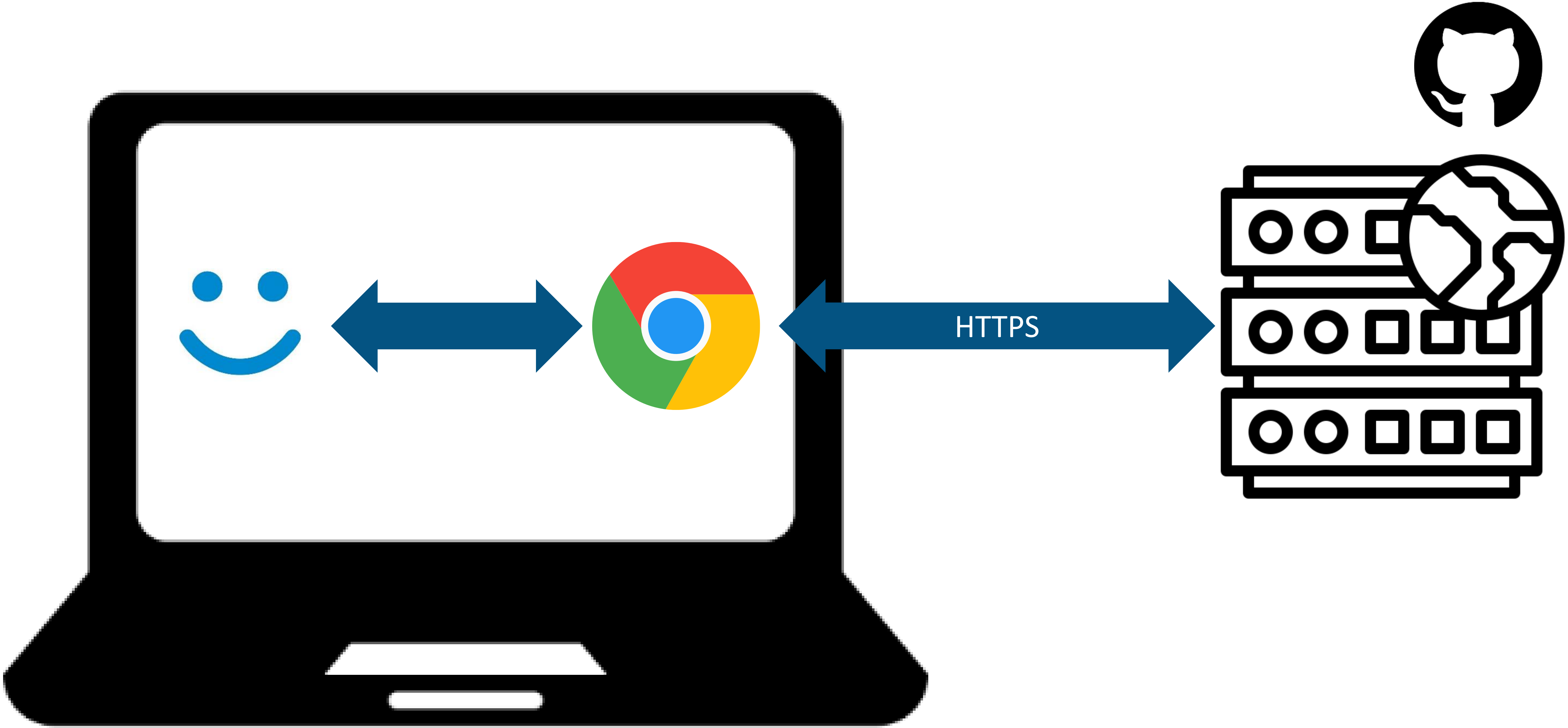
PayPal

Dropbox

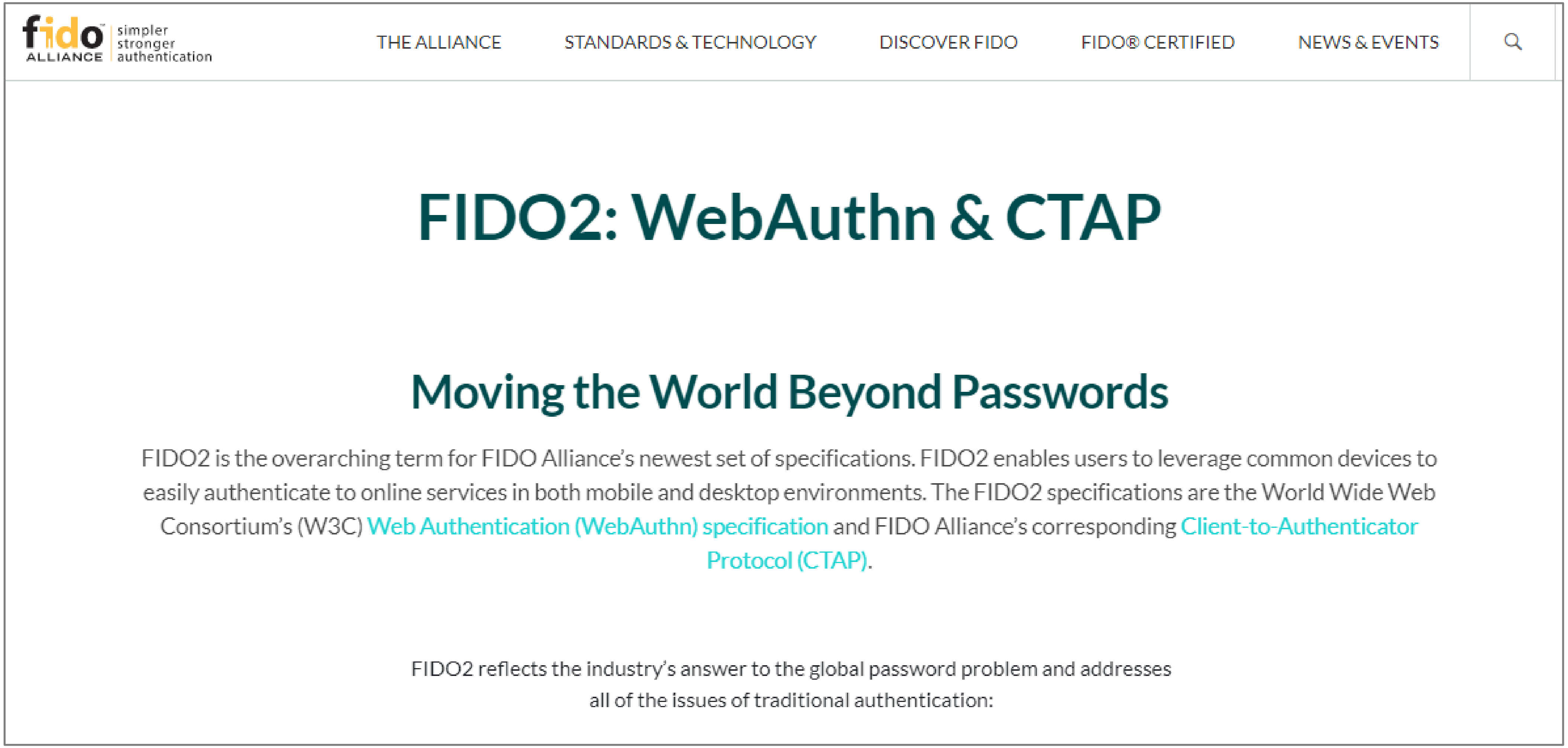
{okta}


USB
HTTPS


NFC
HTTPS


HTTPS

FIDO2



FIDO2: WebAuthn & CTAP

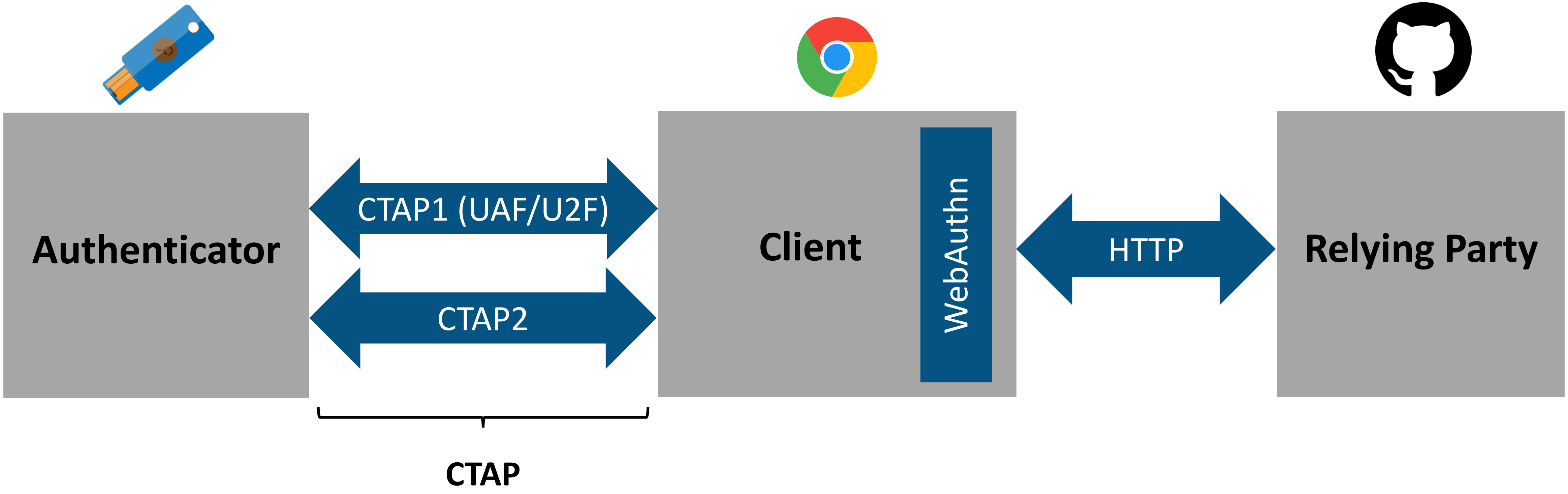
Moving the World Beyond Passwords

FIDO2 is the overarching term for FIDO Alliance's newest set of specifications. FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments. The FIDO2 specifications are the World Wide Web Consortium's (W3C) Web Authentication (WebAuthn) specification and FIDO Alliance's corresponding Client-to-Authenticator Protocol (CTAP).

FIDO2 reflects the industry's answer to the global password problem and addresses all of the issues of traditional authentication:

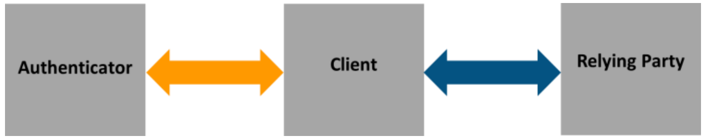
Souce: https://fidoalliance.org/fido2/

FIDO2 Building Blocks



🍺 Client to Authenticator Protocol (CTAP) 🍺

Client To Authenticator Protocol - CTAP



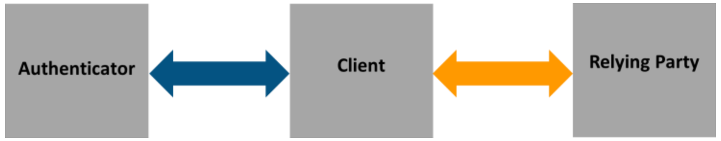
The communication from client to a *roaming* authenticator can use any of the following transport bindings:

- USB Human Interface Device (USB HID)
- Near Field Communication (NFC)
- Bluetooth Smart / Bluetooth Low Energy Technology

Application developers usually need not be concerned with CTAP

🍺 WebAuthn 🍺

WebAuthentication (WebAuthn)



- Standardized JavaScript Web API for FIDO2 Authentication
- Official web standard since March 2019
- Implemented by browsers and related web platform infrastructure

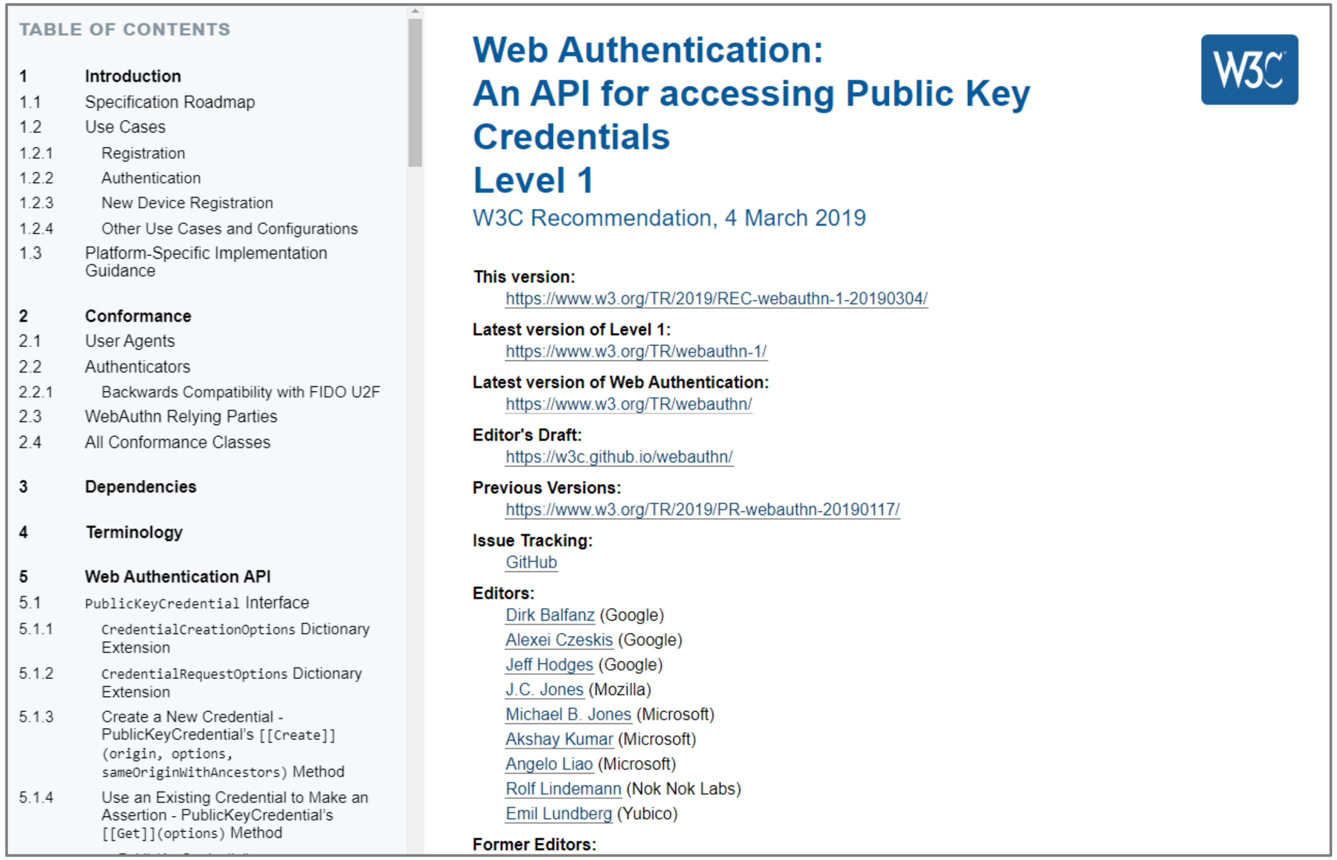


TABLE OF CONTENTS

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

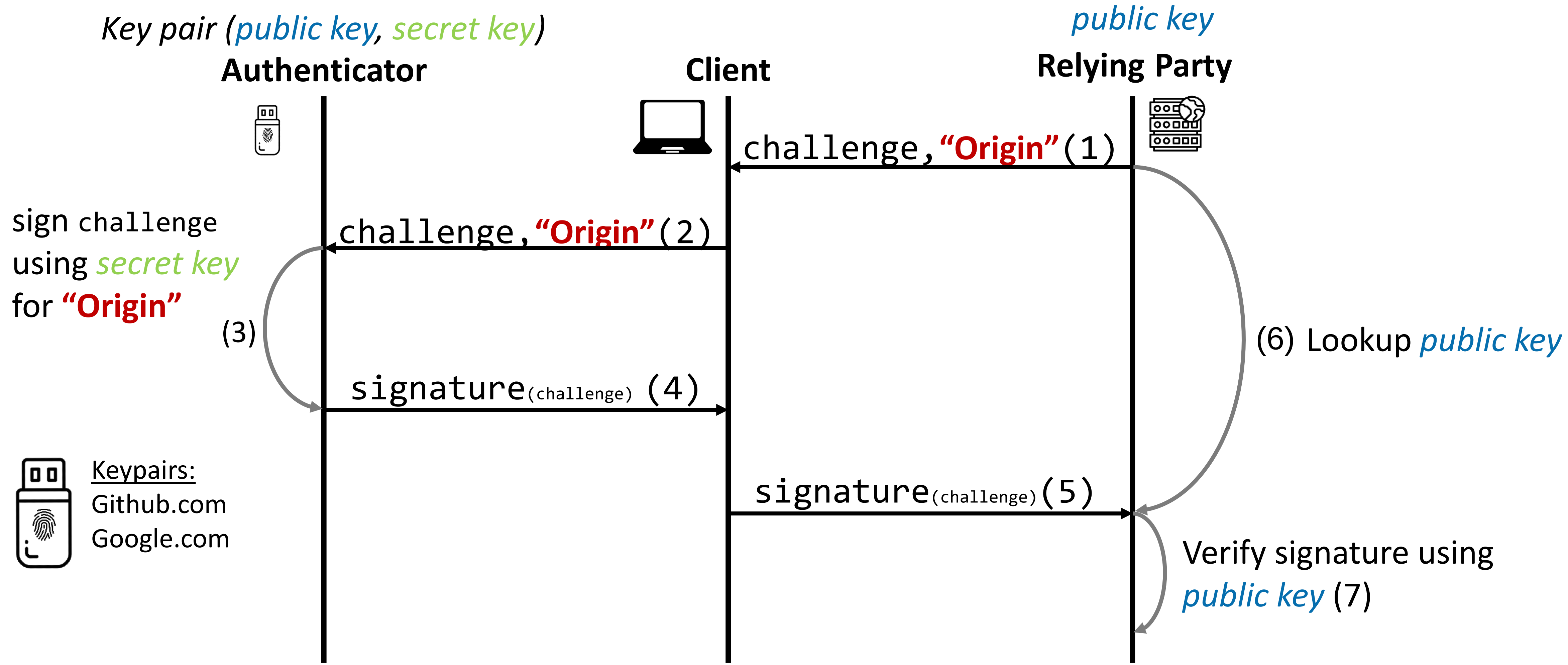
Editors:
Dirk Balfanz (Google)
Alexei Czeskis (Google)
Jeff Hodges (Google)
J.C. Jones (Mozilla)
Michael B. Jones (Microsoft)
Akshay Kumar (Microsoft)
Angelo Liao (Microsoft)
Rolf Lindemann (Nok Nok Labs)
Emil Lundberg (Yubico)

Former Editors:

Source: https://www.w3.org/TR/webauthn/

🍺 Authentication Protocol 🍺

FIDO2 Challenge Response Protocol



Key pair (public key, secret key)

Authenticator

Client

public key

Relying Party

challenge, **"Origin"** (1)

challenge, **"Origin"** (2)

sign challenge using *secret key* for **"Origin"**

(3)

signature(challenge) (4)

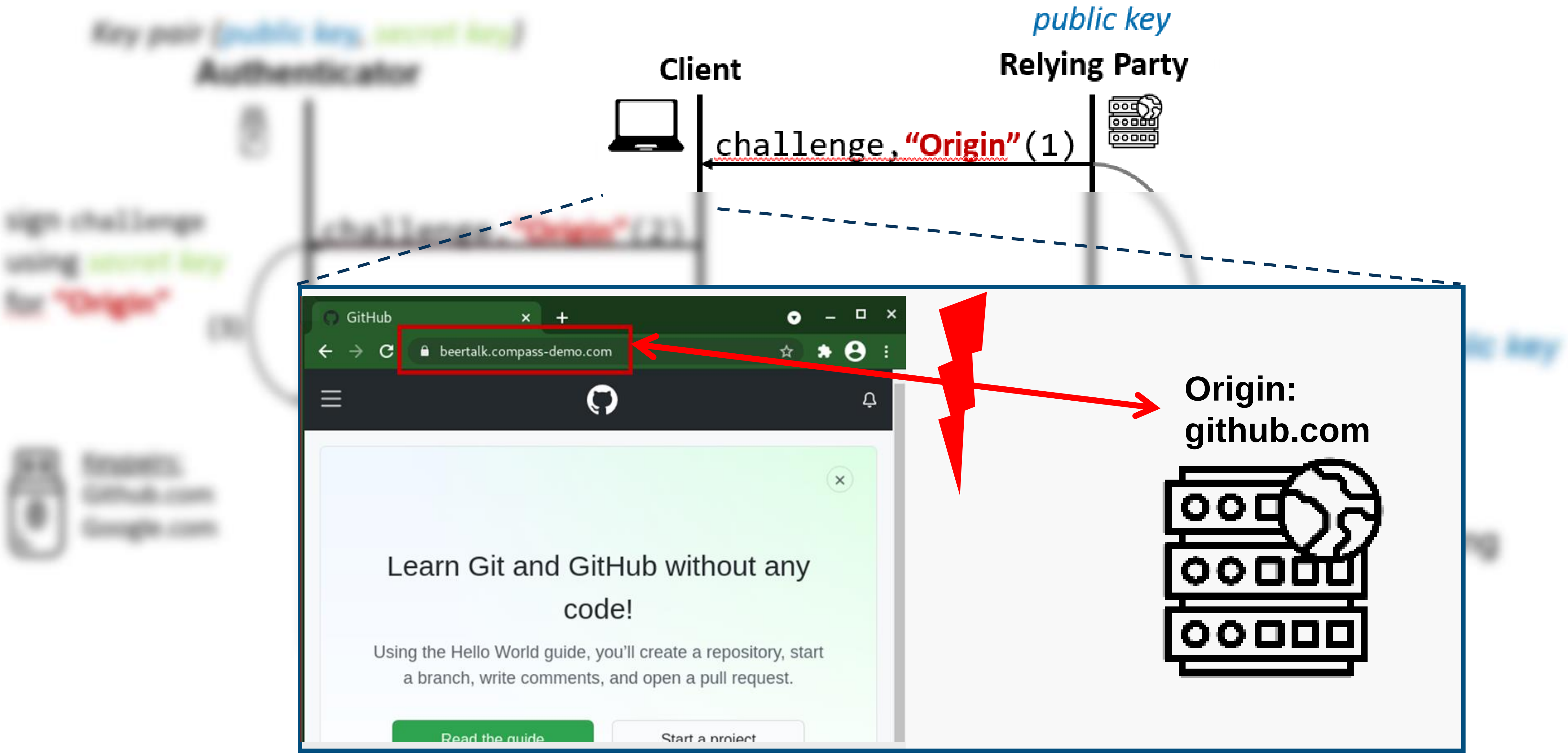
signature(challenge) (5)

(6) Lookup *public key*

Verify signature using *public key* (7)

Keypairs:
Github.com
Google.com

Phishing Protection (1) - Github



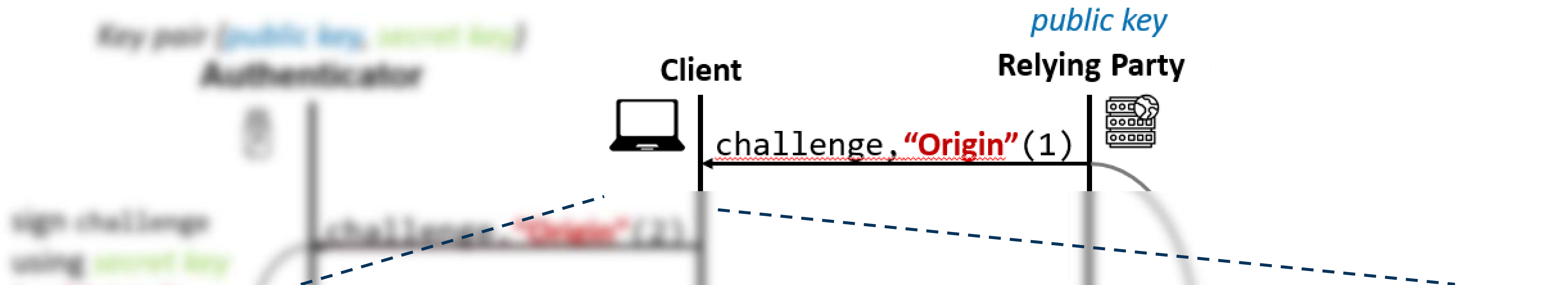
Learn Git and GitHub without any code!

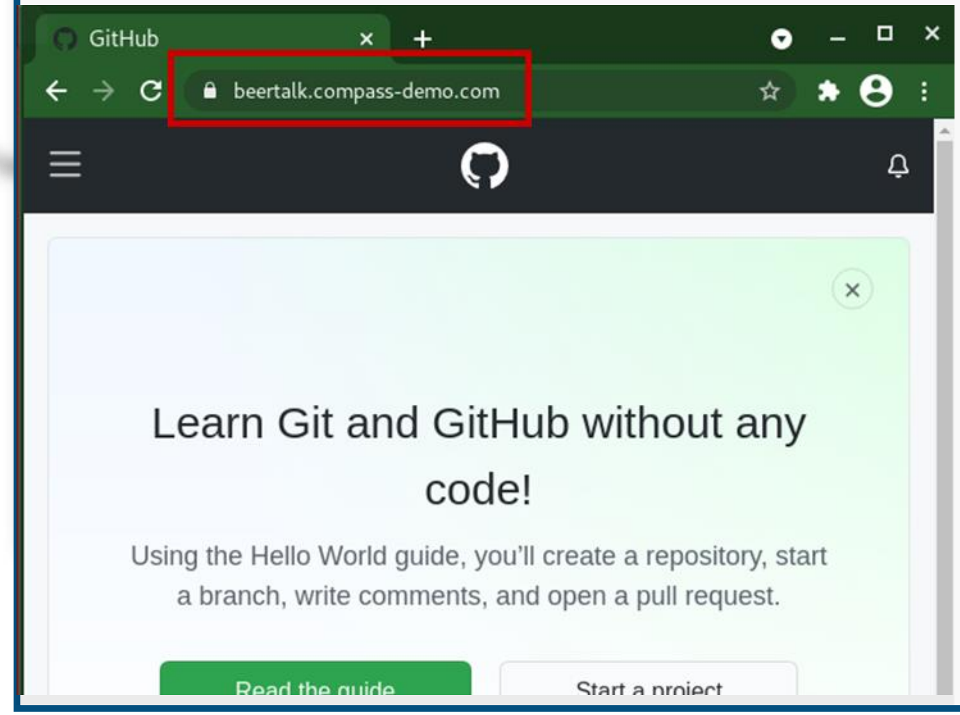
Using the Hello World guide, you'll create a repository, start a branch, write comments, and open a pull request.

Read the guide

Start a project

Phishing Protection (2) - Github



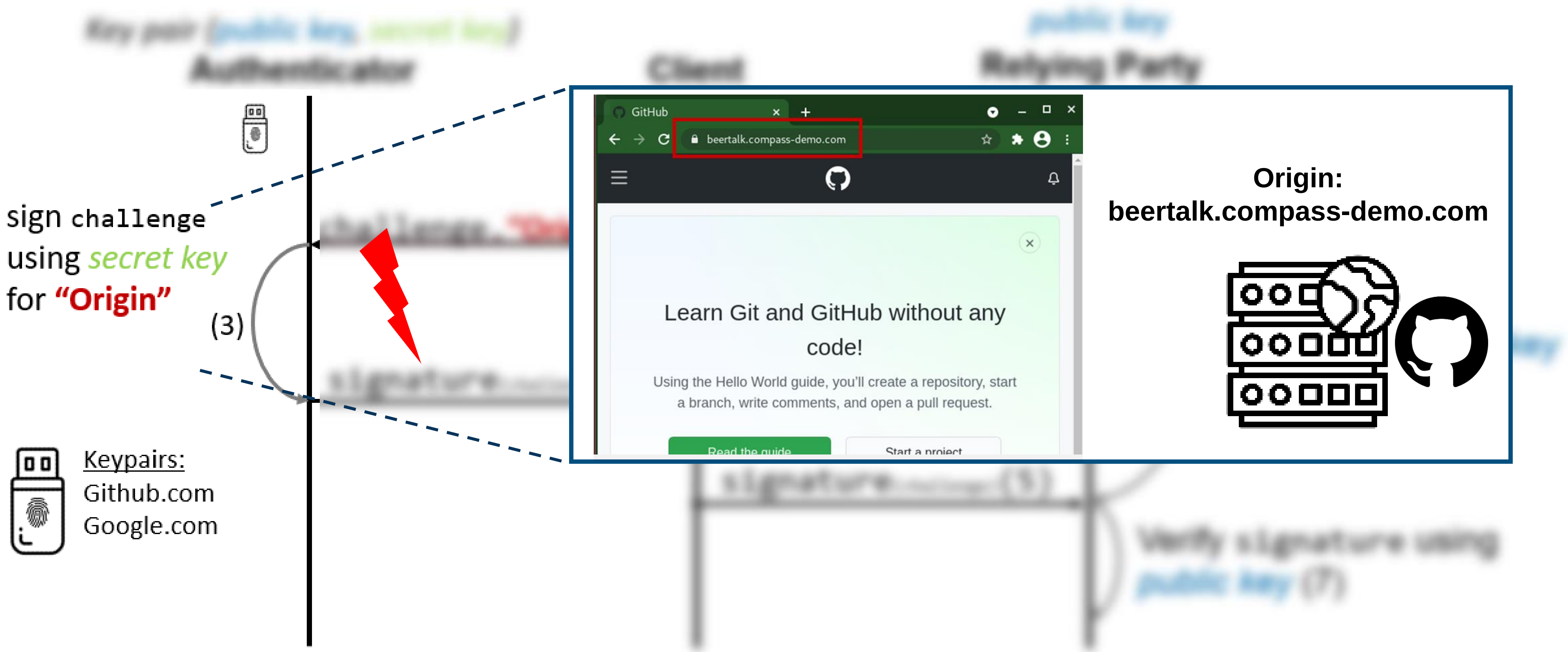


Learn Git and GitHub without any code!

Using the Hello World guide, you'll create a repository, start a branch, write comments, and open a pull request.

Origin: beertalk.compass-demo.com

Phishing Protection (2) - Github



Learn Git and GitHub without any code!

Using the Hello World guide, you'll create a repository, start a branch, write comments, and open a pull request.

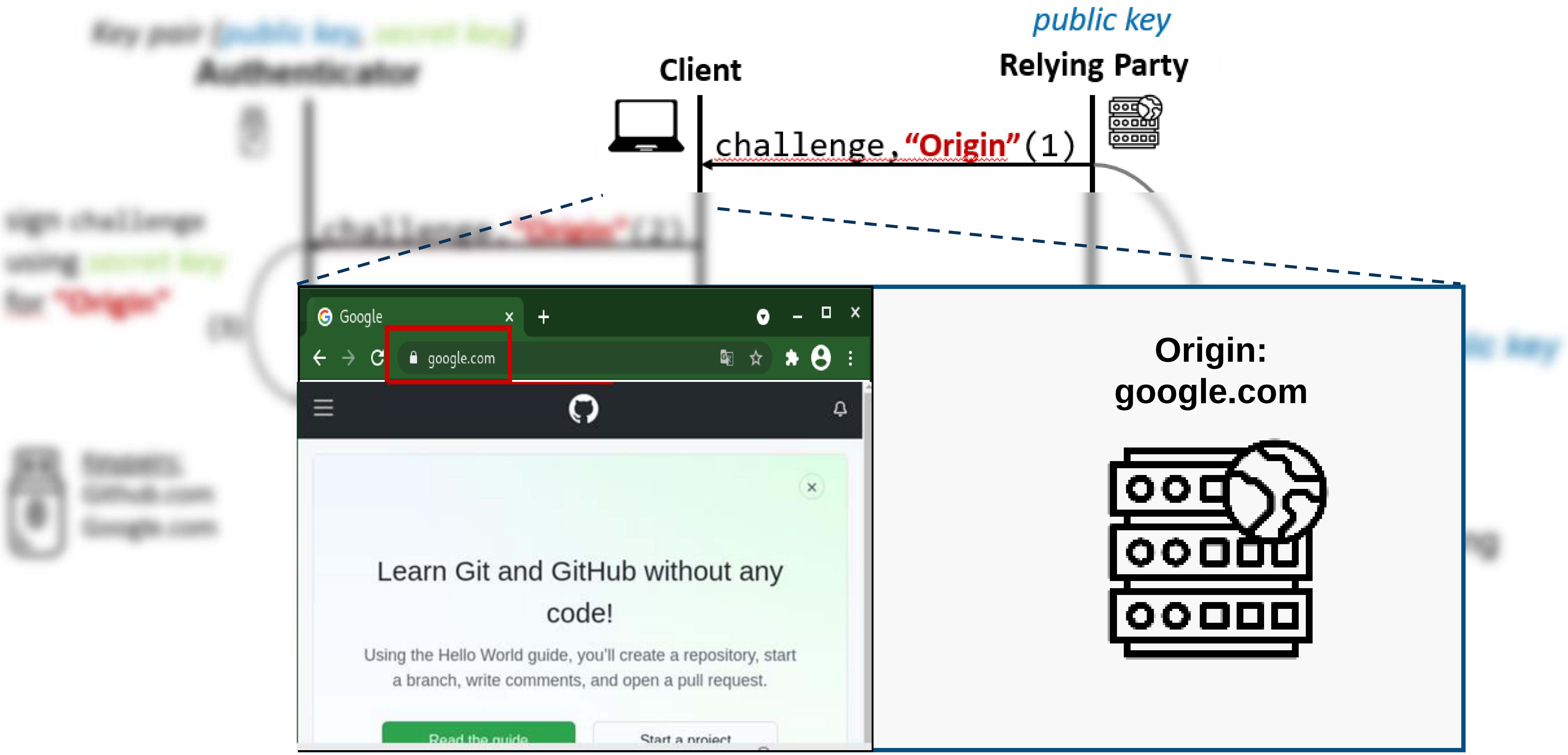
Origin: beertalk.compass-demo.com

sign challenge using *secret key* for **"Origin"**

(3)

Keypairs:
Github.com
Google.com

Phishing Protection (3) - Github



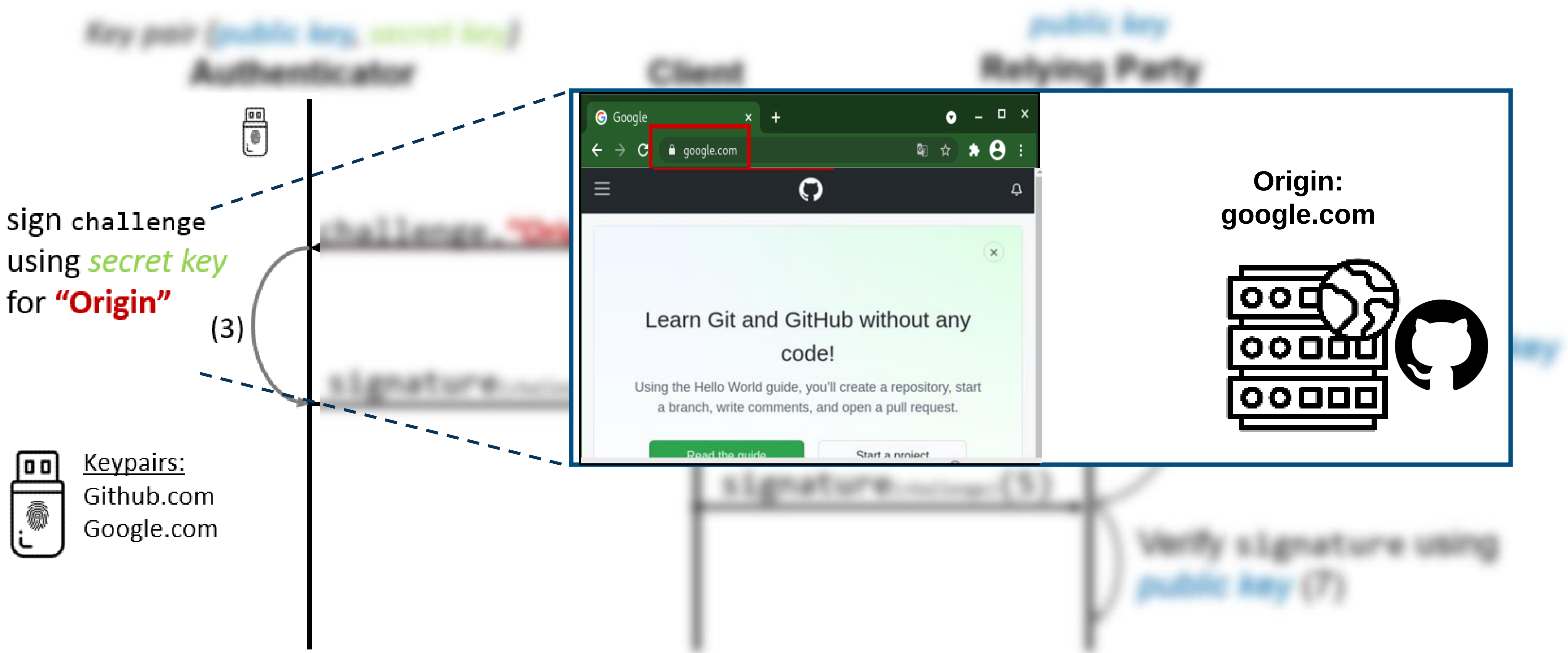
Learn Git and GitHub without any code!

Using the Hello World guide, you'll create a repository, start a branch, write comments, and open a pull request.

Read the guide

Start a project

Phishing Protection (3) - Github



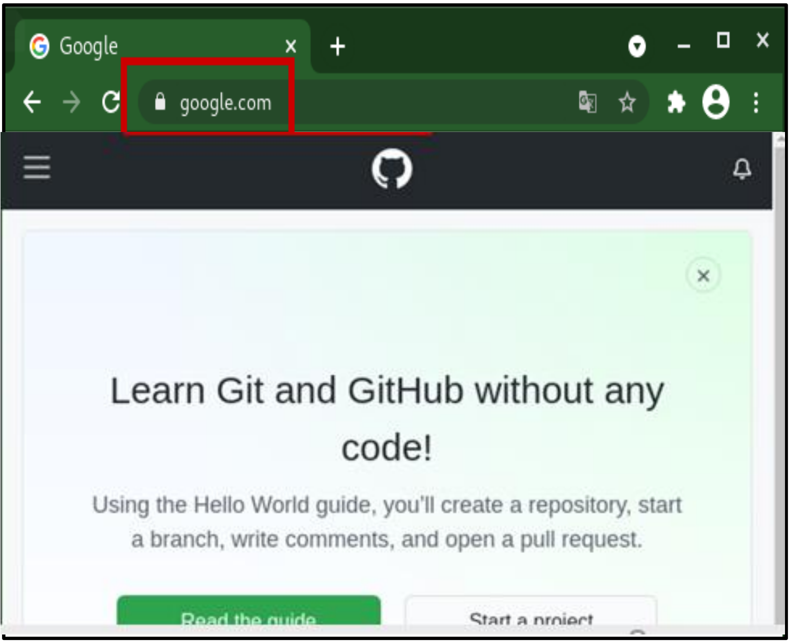
sign challenge using *secret key* for **"Origin"**

Learn Git and GitHub without any code!

Using the Hello World guide, you'll create a repository, start a branch, write comments, and open a pull request.

Keypairs:
Github.com
Google.com

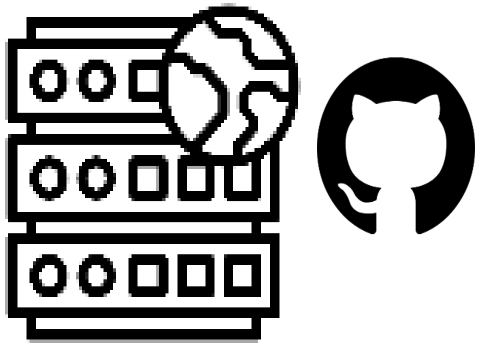
Phishing Protection (3) - Github

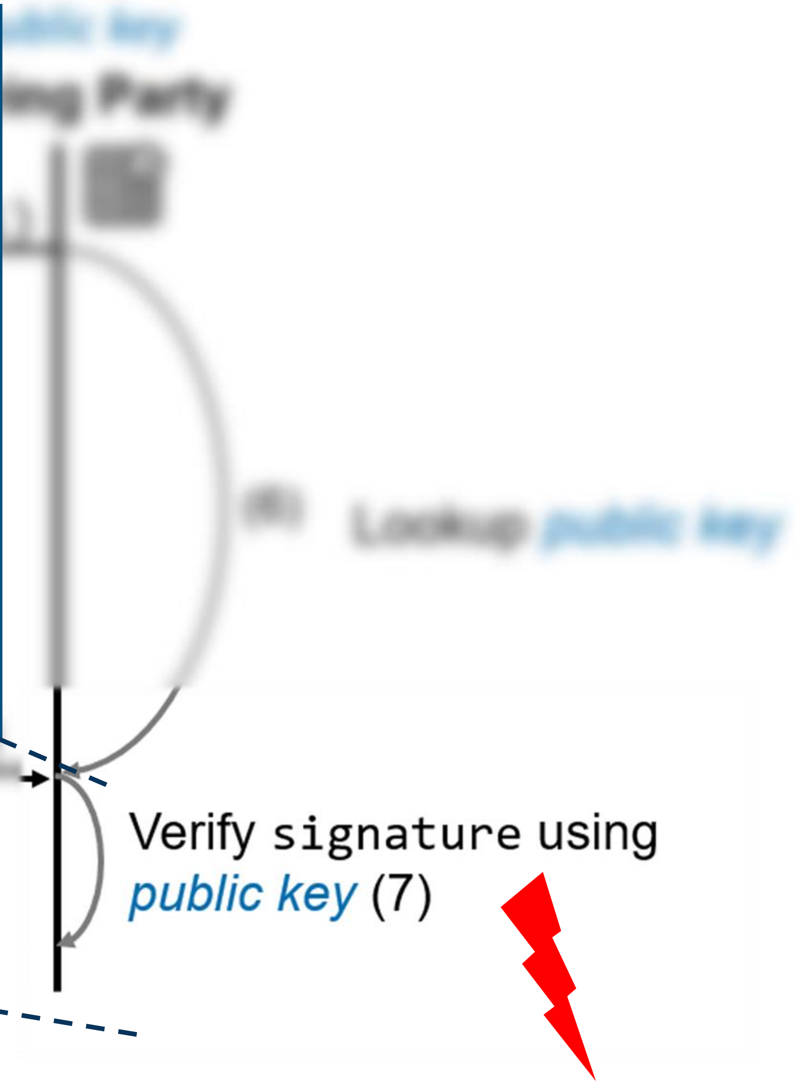


Learn Git and GitHub without any code!

Using the Hello World guide, you'll create a repository, start a branch, write comments, and open a pull request.

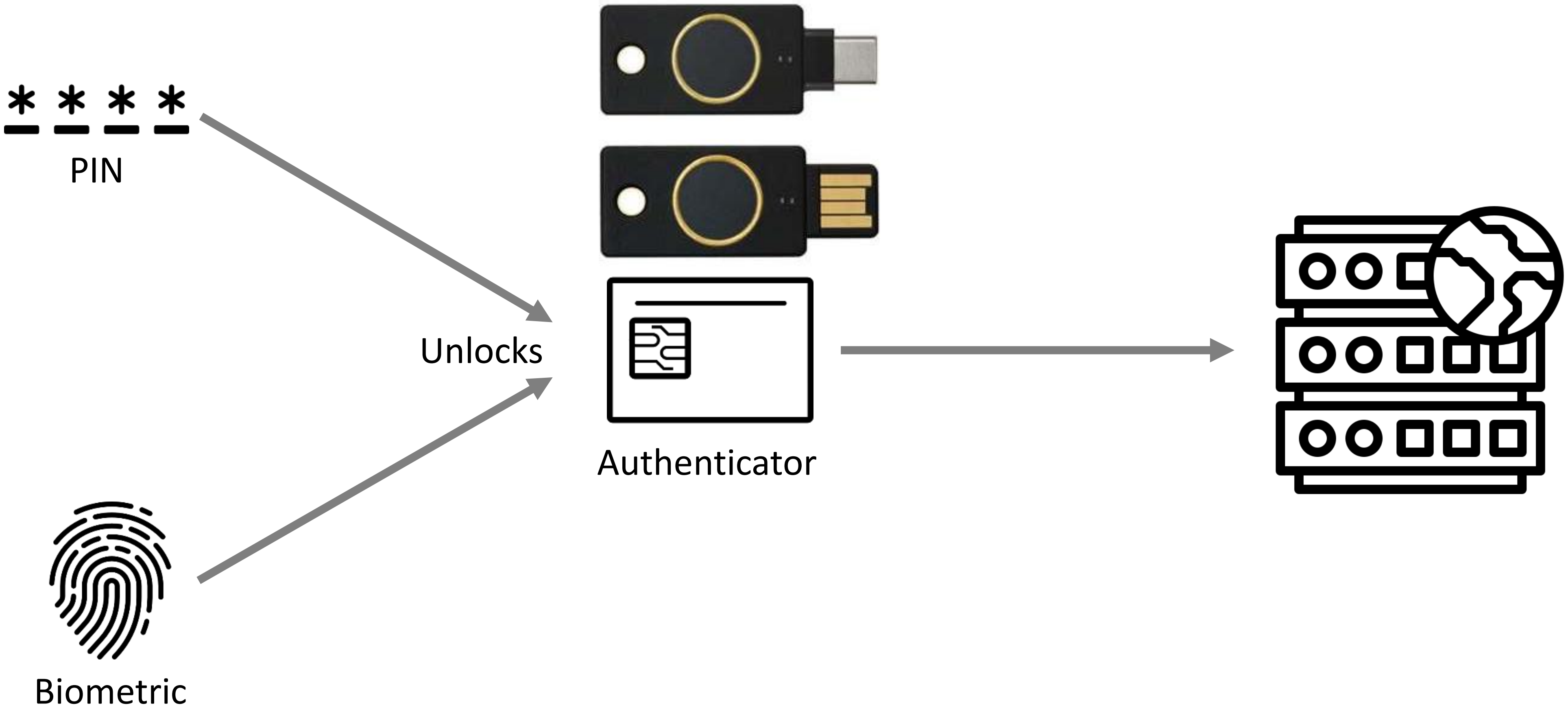
Origin: google.com





🍺 Password-Less Authentication 🍺

Password-Less Authentication



Source: https://pages.yubico.com/YubiKey-Bio-Updates-de.html

🍺 Conclusion 🍺

Conclusion

Traditional authentication mechanisms are not sufficient anymore

- Inconvenient
- Not resistant to phishing

FIDO2

- is a phishing-resistant authentication protocol
- is simple to use (also for non-technical people)
- has strong platform & industry support

COMPASS® SECURITY
OFFENSIVE DEFENSE