



Suppliers! Resist Phishing, Implement FIDO2

Swiss Cyber Storm

12th October 2021 11:20

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

«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.

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.

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

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 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.

Phishing-Fall schädigte Dutzende Schweizer Bankkunden









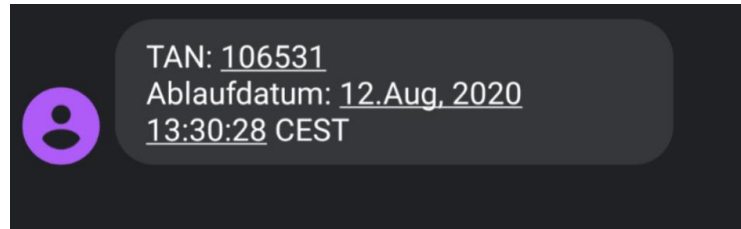
“Traditional” 2FA



Possession Factor Examples



RSA SecurID



SmartCard

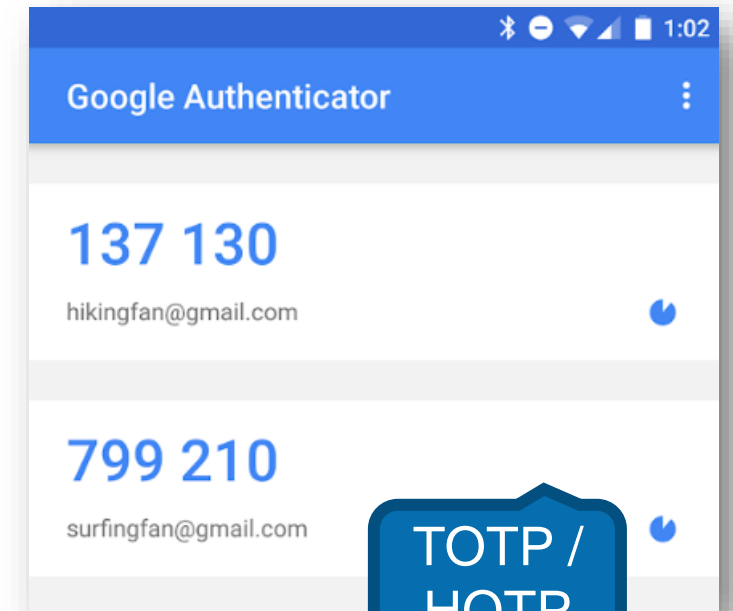


PhotoTAN / Cronto



MobileID

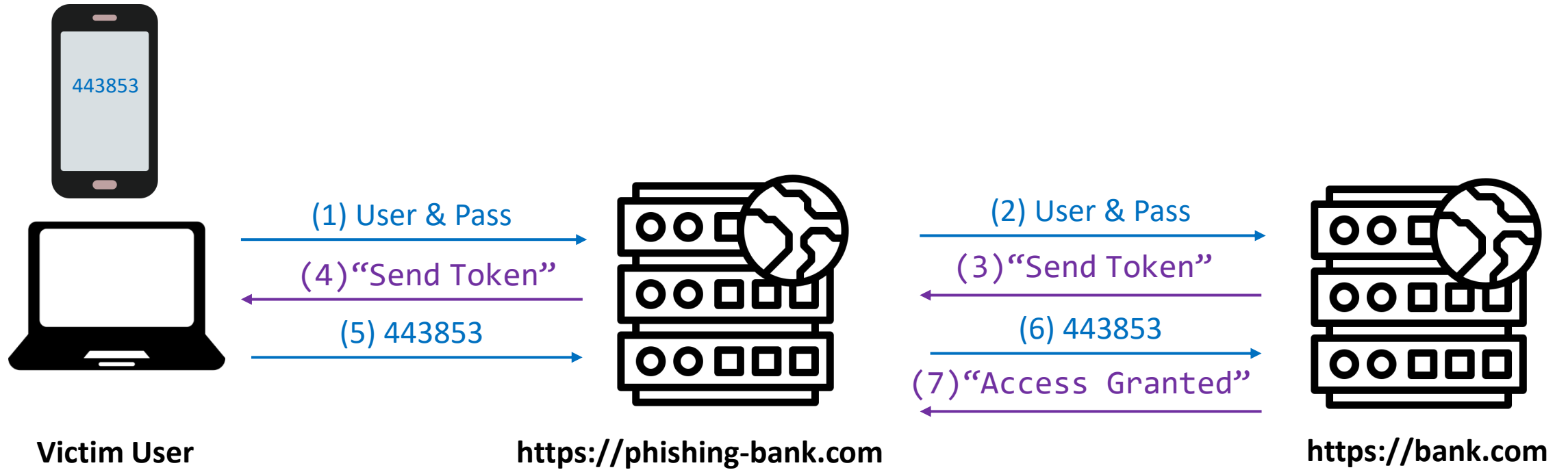
mTAN / SMS



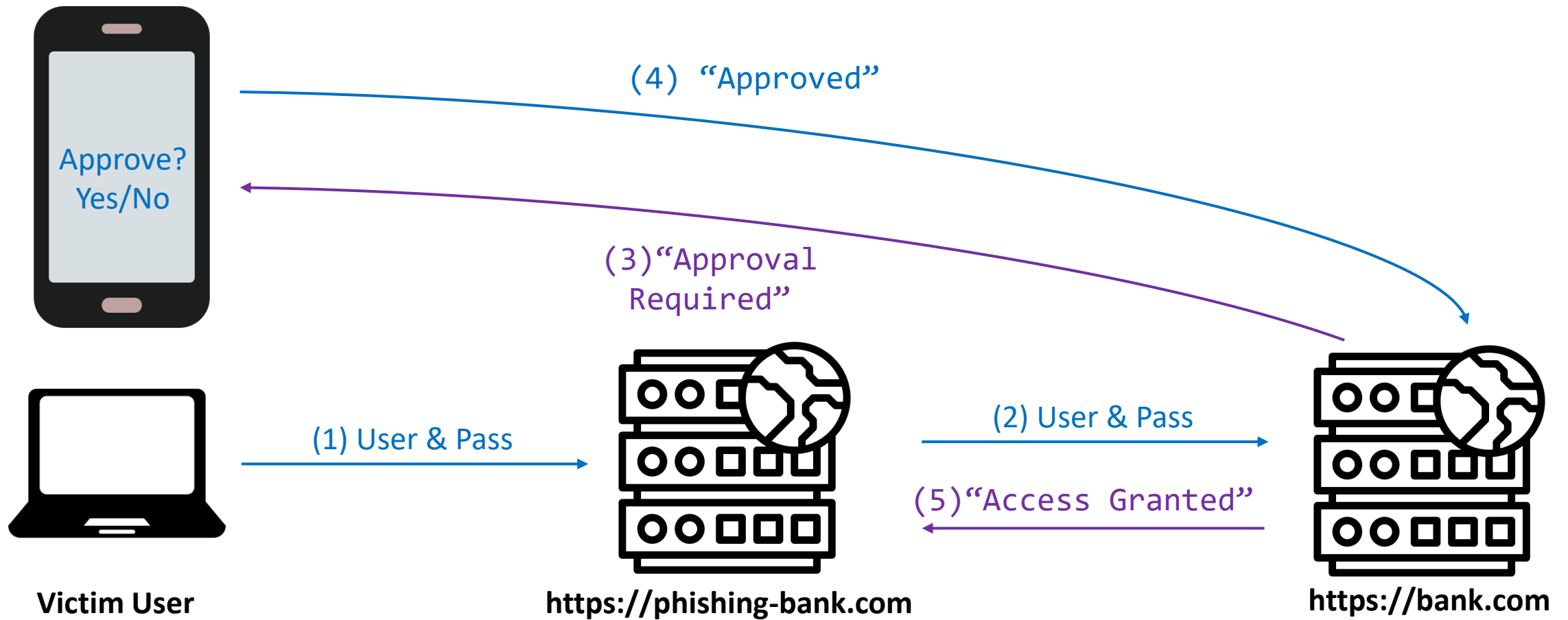
TOTP / HOTP

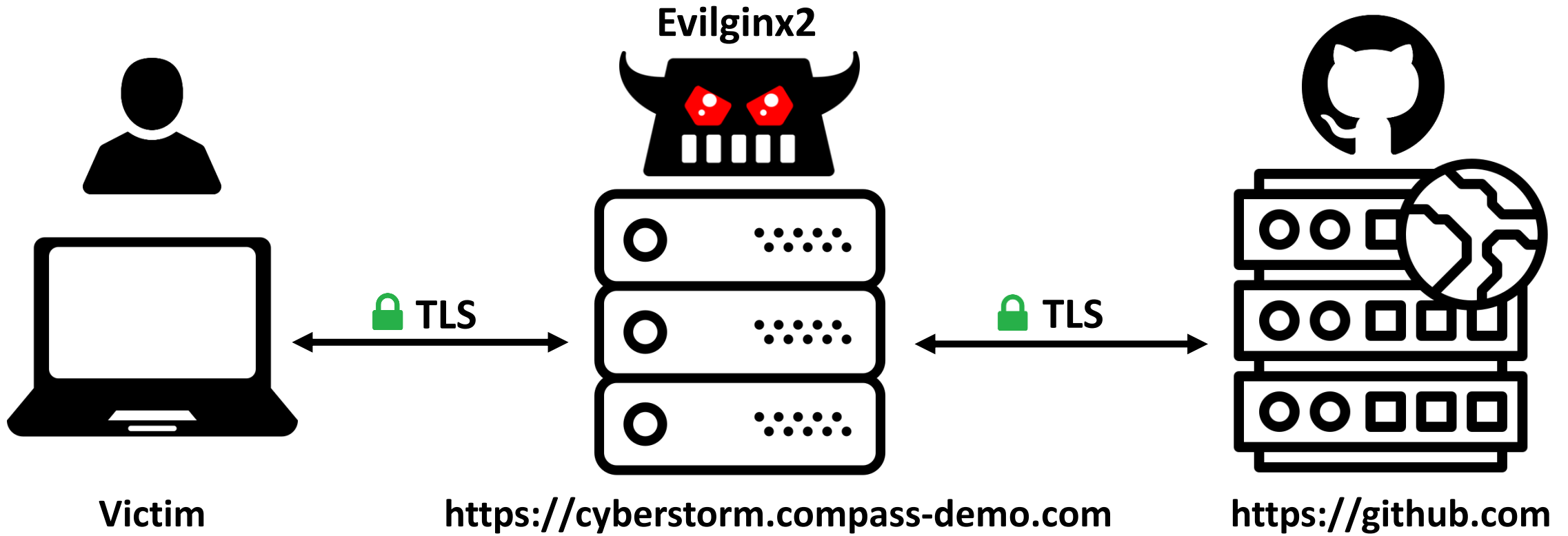
Most second factor mechanisms do **not** protect against credential phishing

2FA Phishing



HOTP / TOTP Phishing with Push Notification





- gitzhub.com
- githujb.com
- githuB.com
- githұb.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

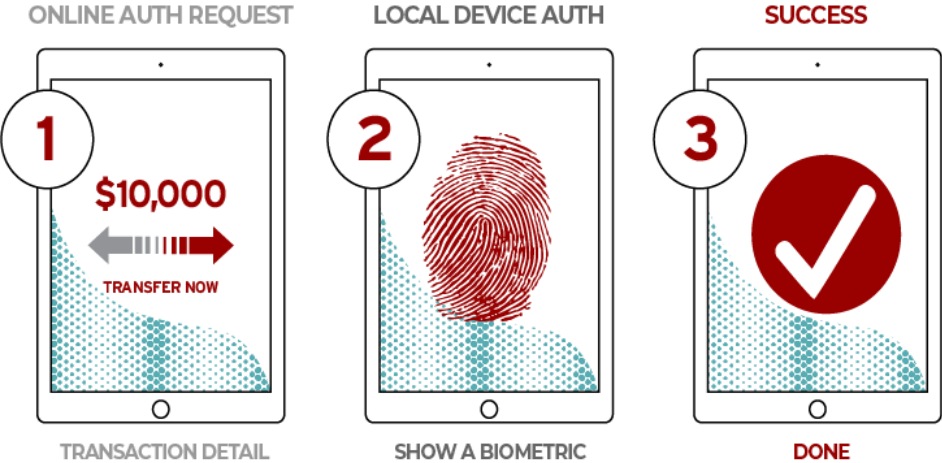


**U2F, UAF, CTAP, WebAuthn, FIDO, FIDO2
oh my...**

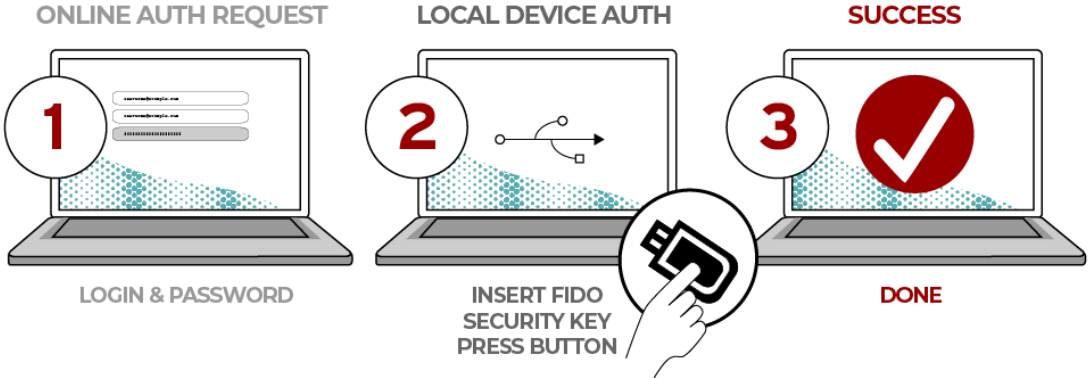


FIDO (Fast Identity Online)

PASSWORDLESS EXPERIENCE (UAF standards)



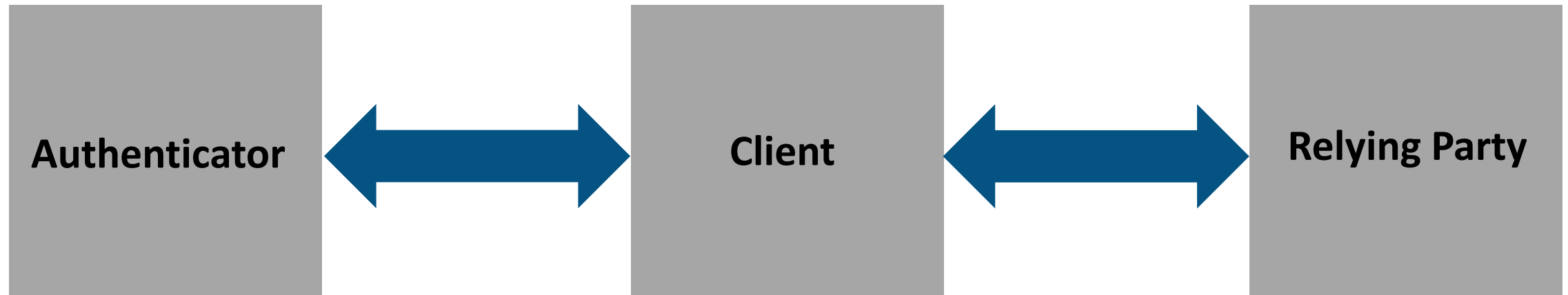
SECOND FACTOR EXPERIENCE (U2F standards)



The FIDO2 specification replaces FIDO U2F and FIDO UAF

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

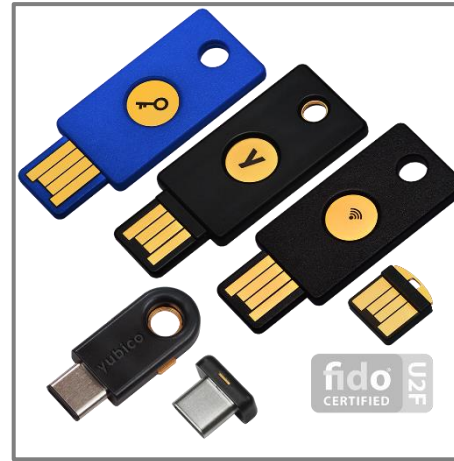
FIDO2 Building Blocks



FIDO2 Authenticators



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



<https://www.yubico.com/>



<https://onlykey.io/>



<https://solokeys.com/>

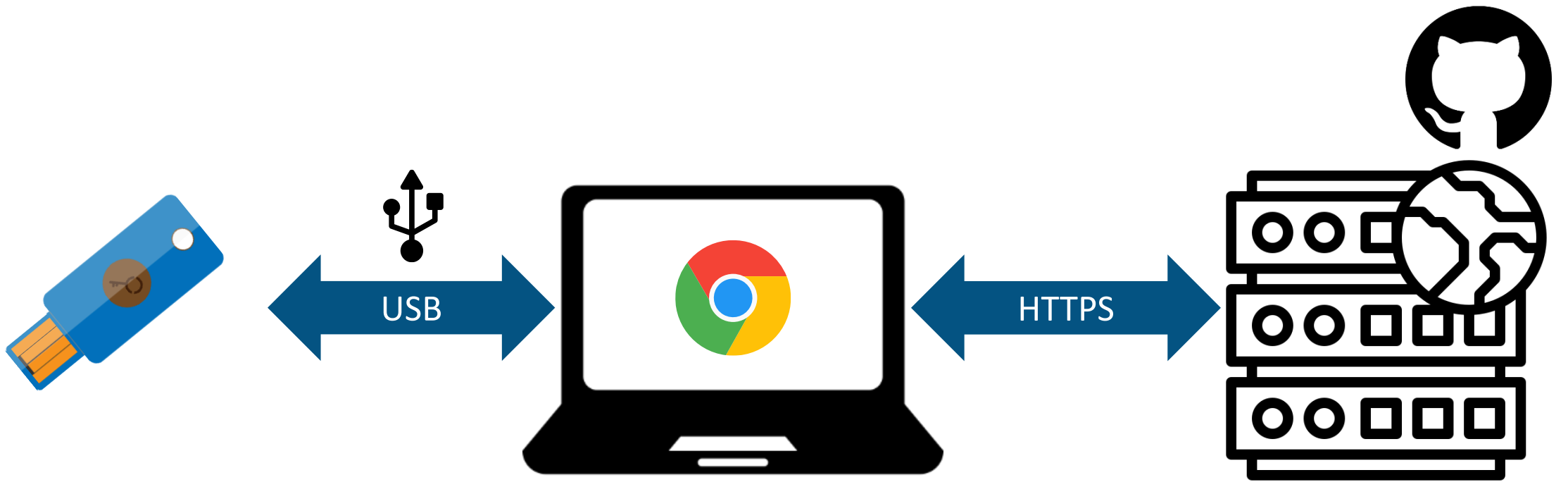
FIDO2 Clients

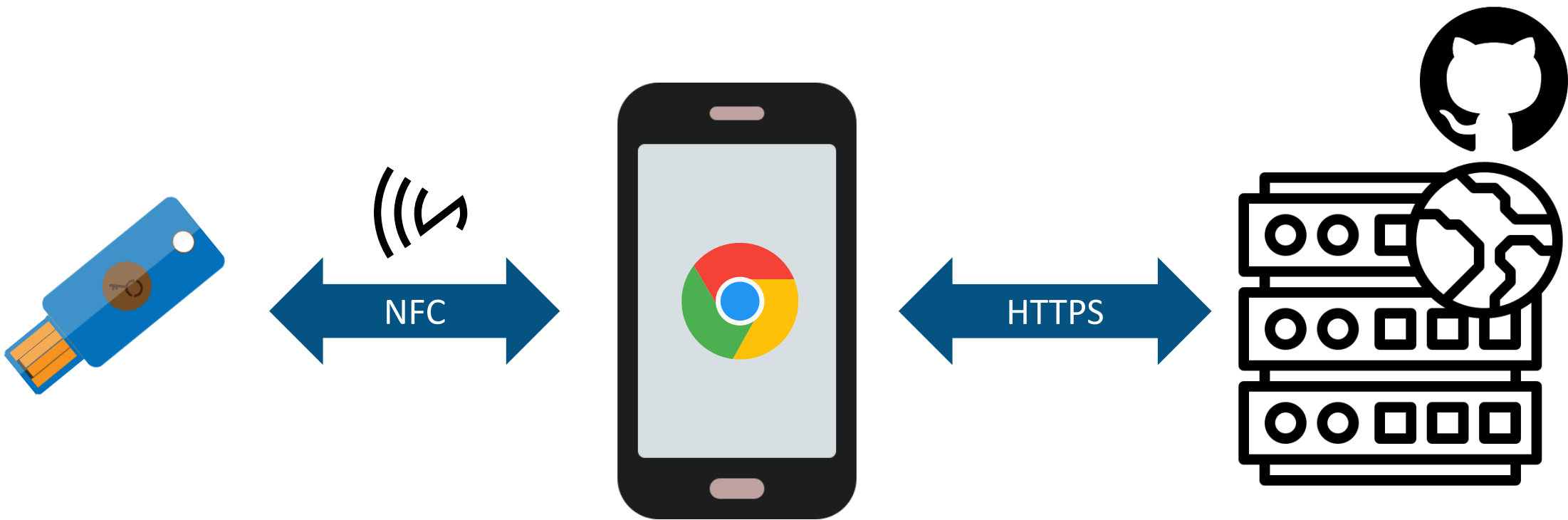


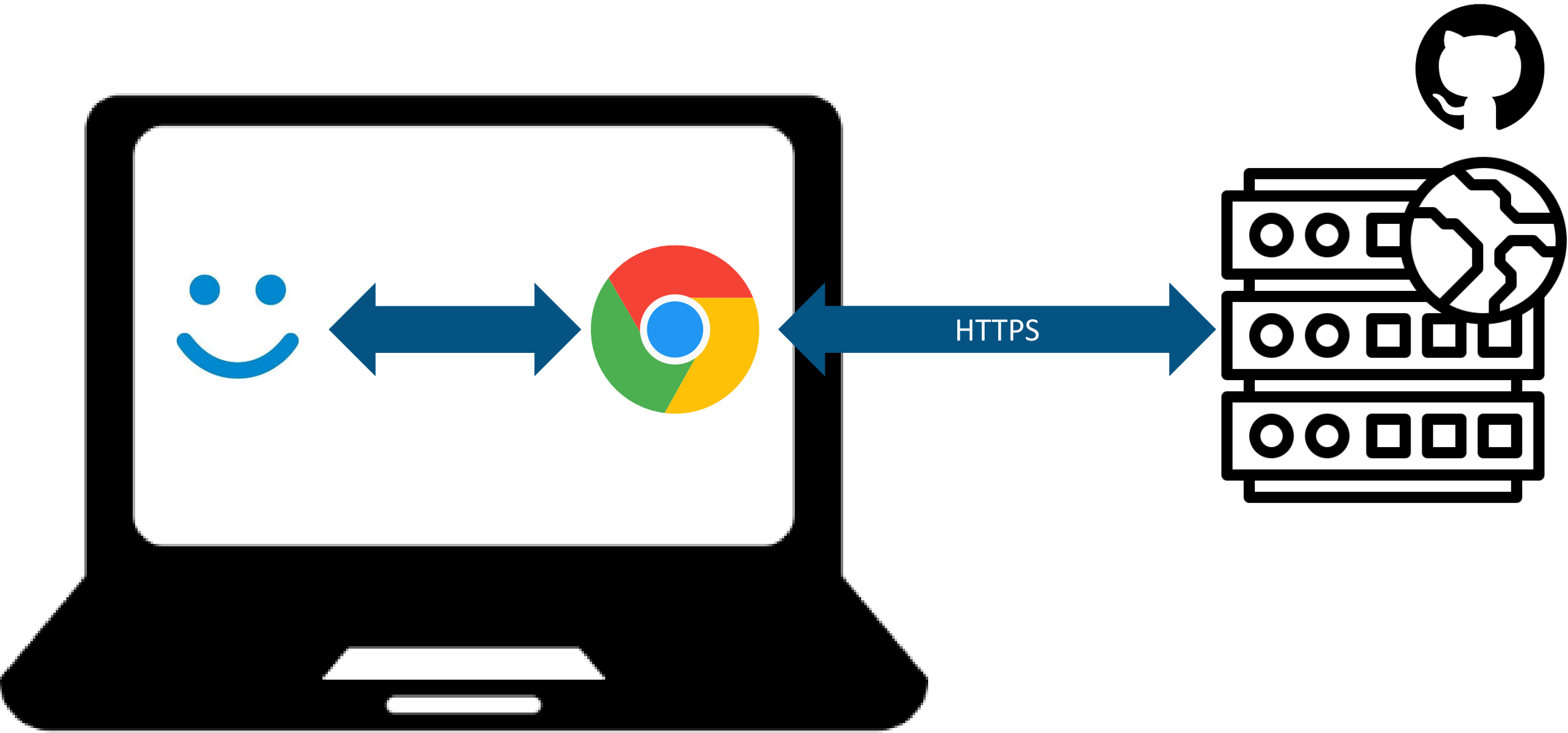
Source: <https://fidoalliance.org/fido2/>

FIDO2 Relying Parties









FIDO2



The screenshot shows the top navigation bar of the FIDO Alliance website. The logo on the left reads "fido ALLIANCE" with the tagline "simpler stronger authentication". The navigation menu includes "THE ALLIANCE", "STANDARDS & TECHNOLOGY", "DISCOVER FIDO", "FIDO® CERTIFIED", and "NEWS & EVENTS", followed by a search icon. The main content area features a large teal heading "FIDO2: WebAuthn & CTAP" and a sub-heading "Moving the World Beyond Passwords". Below this is a paragraph explaining that FIDO2 is the overarching term for the Alliance's newest specifications, enabling users to use common devices for authentication. It mentions the W3C's "Web Authentication (WebAuthn) specification" and the Alliance's "Client-to-Authenticator Protocol (CTAP)". At the bottom, it states that FIDO2 addresses the global password problem.

fido ALLIANCE simpler stronger authentication

THE ALLIANCE STANDARDS & TECHNOLOGY DISCOVER FIDO FIDO® CERTIFIED NEWS & EVENTS 🔍

FIDO2: WebAuthn & CTAP

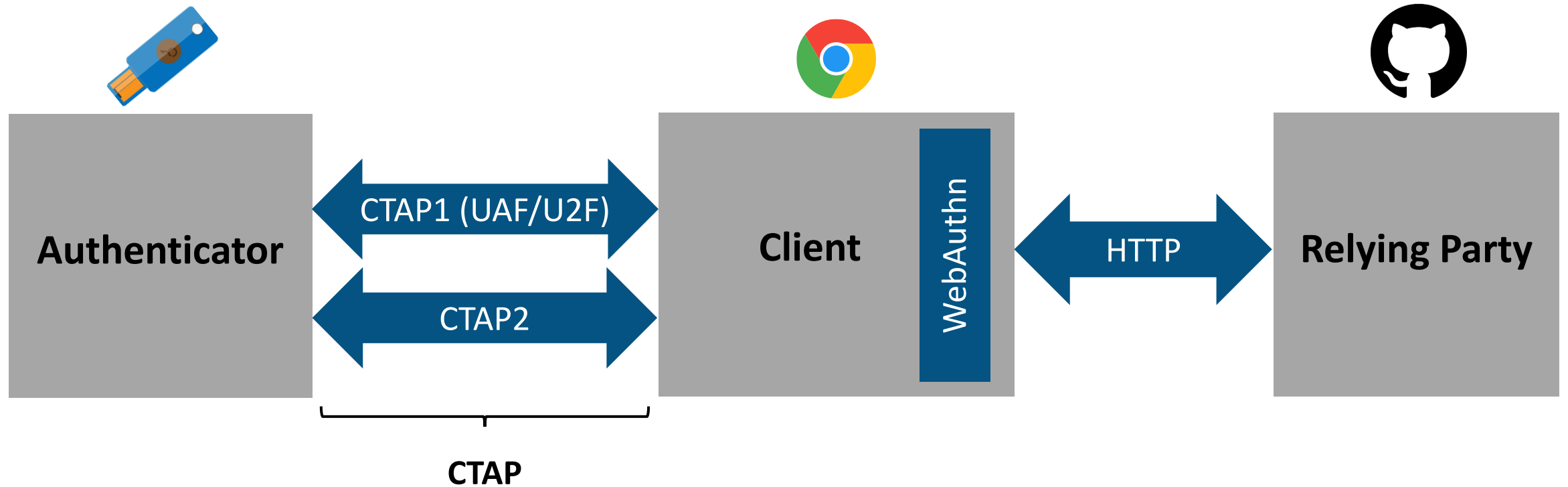
Moving the World Beyond Passwords

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:

Source: <https://fidoalliance.org/fido2/>

FIDO2 Building Blocks





Client to Authenticator Protocol (CTAP)

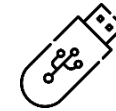


Client To Authenticator Protocol - CTAP



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



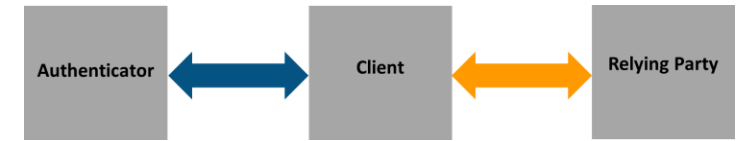
Application developers usually need not be concerned with CTAP



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

- 1 Introduction
 - 1.1 Specification Roadmap
 - 1.2 Use Cases
 - 1.2.1 Registration
 - 1.2.2 Authentication
 - 1.2.3 New Device Registration
 - 1.2.4 Other Use Cases and Configurations
 - 1.3 Platform-Specific Implementation Guidance
- 2 Conformance
 - 2.1 User Agents
 - 2.2 Authenticators
 - 2.2.1 Backwards Compatibility with FIDO U2F
 - 2.3 WebAuthn Relying Parties
 - 2.4 All Conformance Classes
- 3 Dependencies
- 4 Terminology
- 5 Web Authentication API
 - 5.1 PublicKeyCredential Interface
 - 5.1.1 CredentialCreationOptions Dictionary Extension
 - 5.1.2 CredentialRequestOptions Dictionary Extension
 - 5.1.3 Create a New Credential - PublicKeyCredential's [[Create]] (origin, options, sameOriginWithAncestors) Method
 - 5.1.4 Use an Existing Credential to Make an Assertion - PublicKeyCredential's [[Get]](options) Method

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:

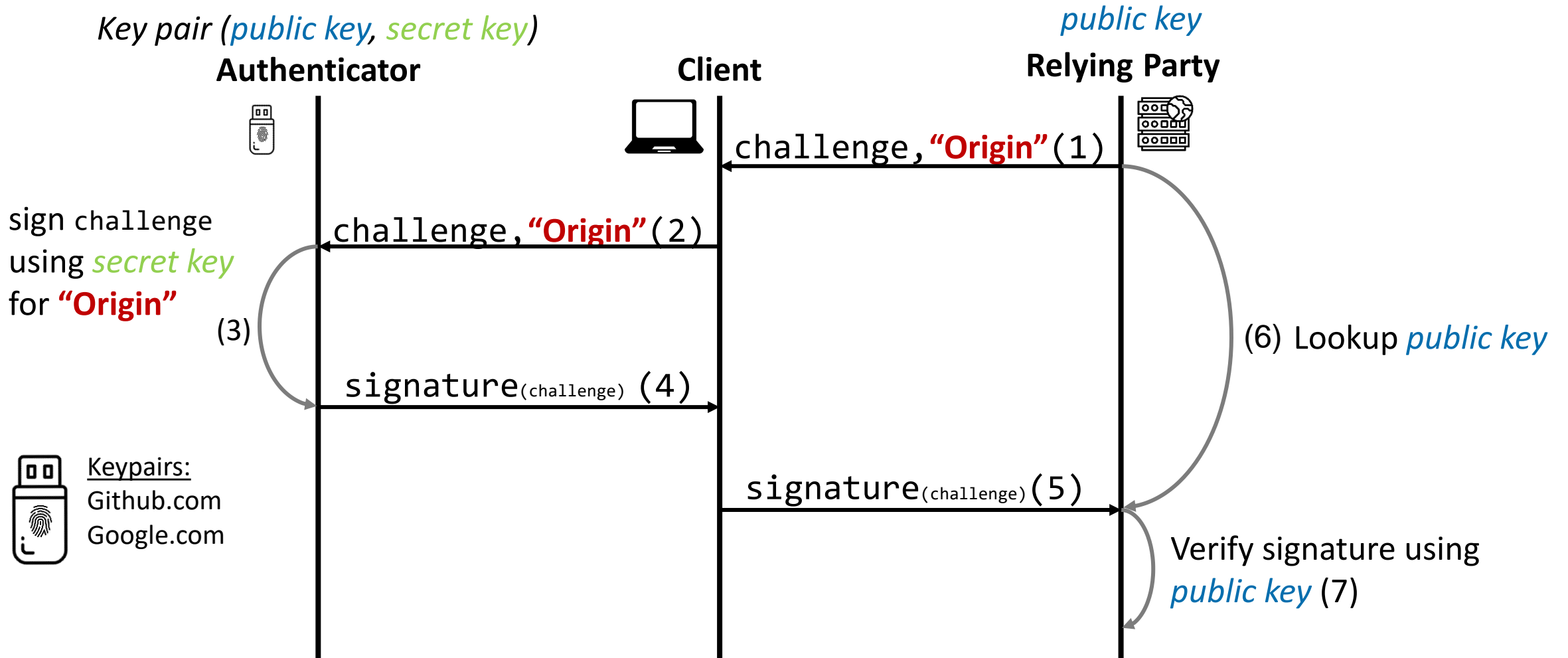
Source: <https://www.w3.org/TR/webauthn/>



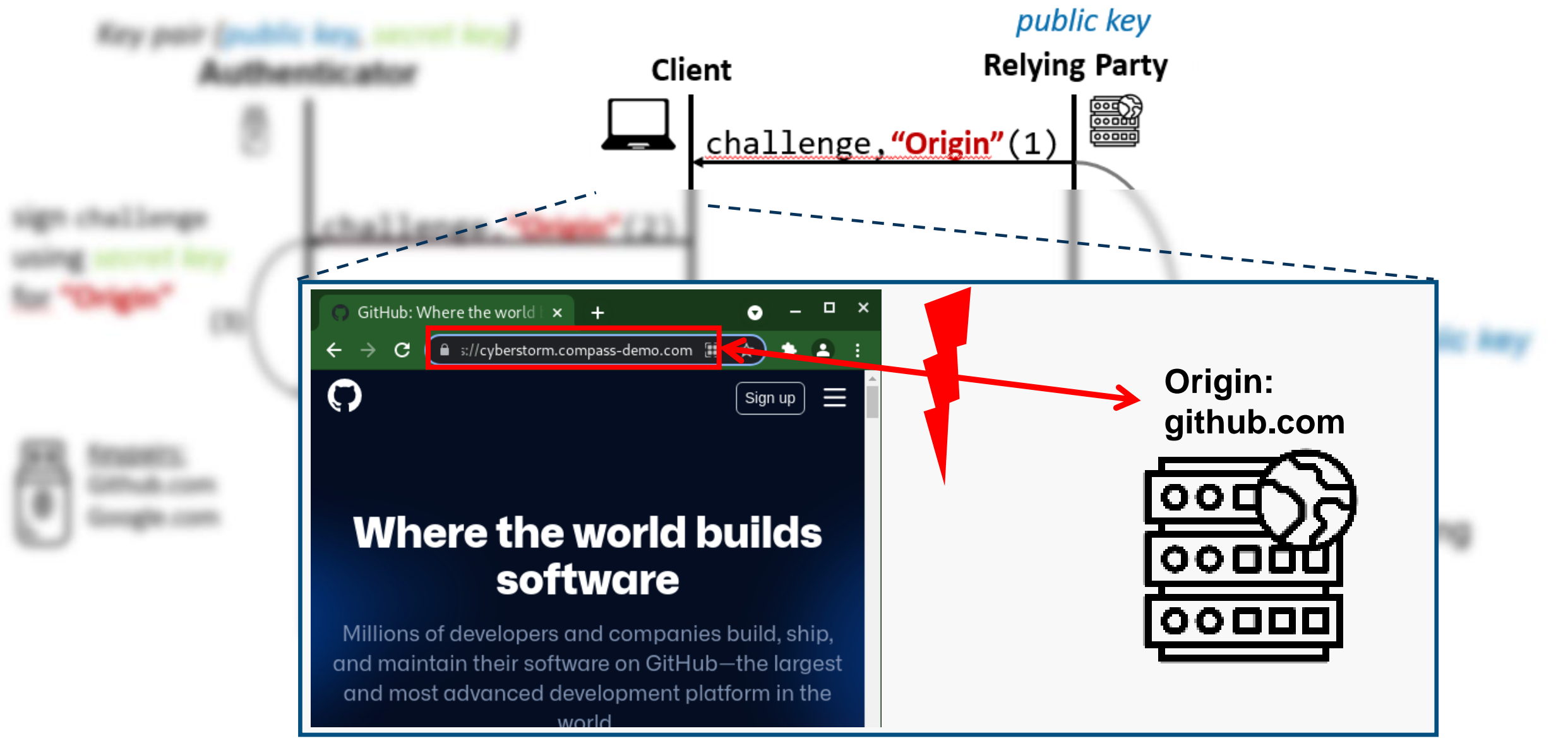
Authentication Protocol



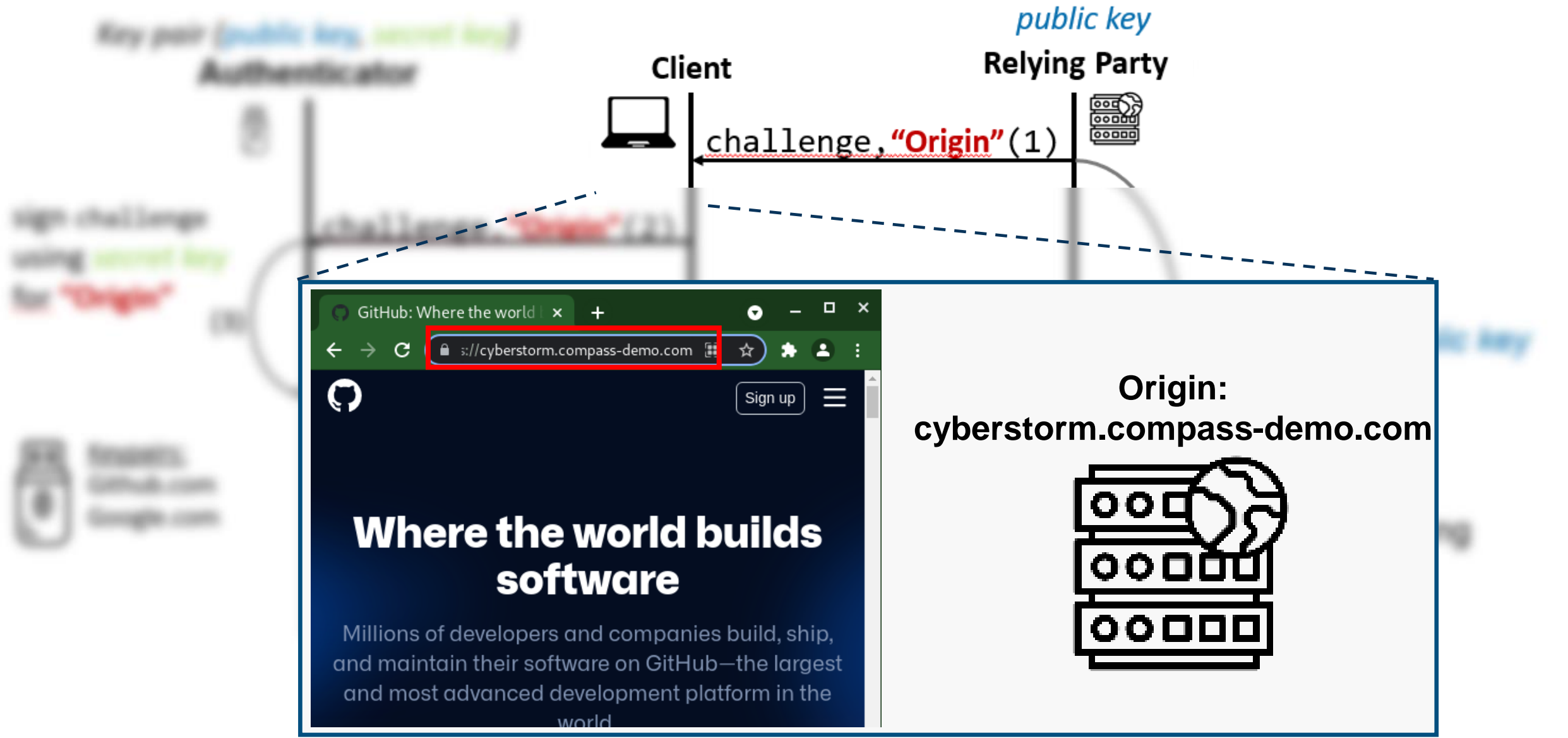
FIDO2 Challenge Response Protocol



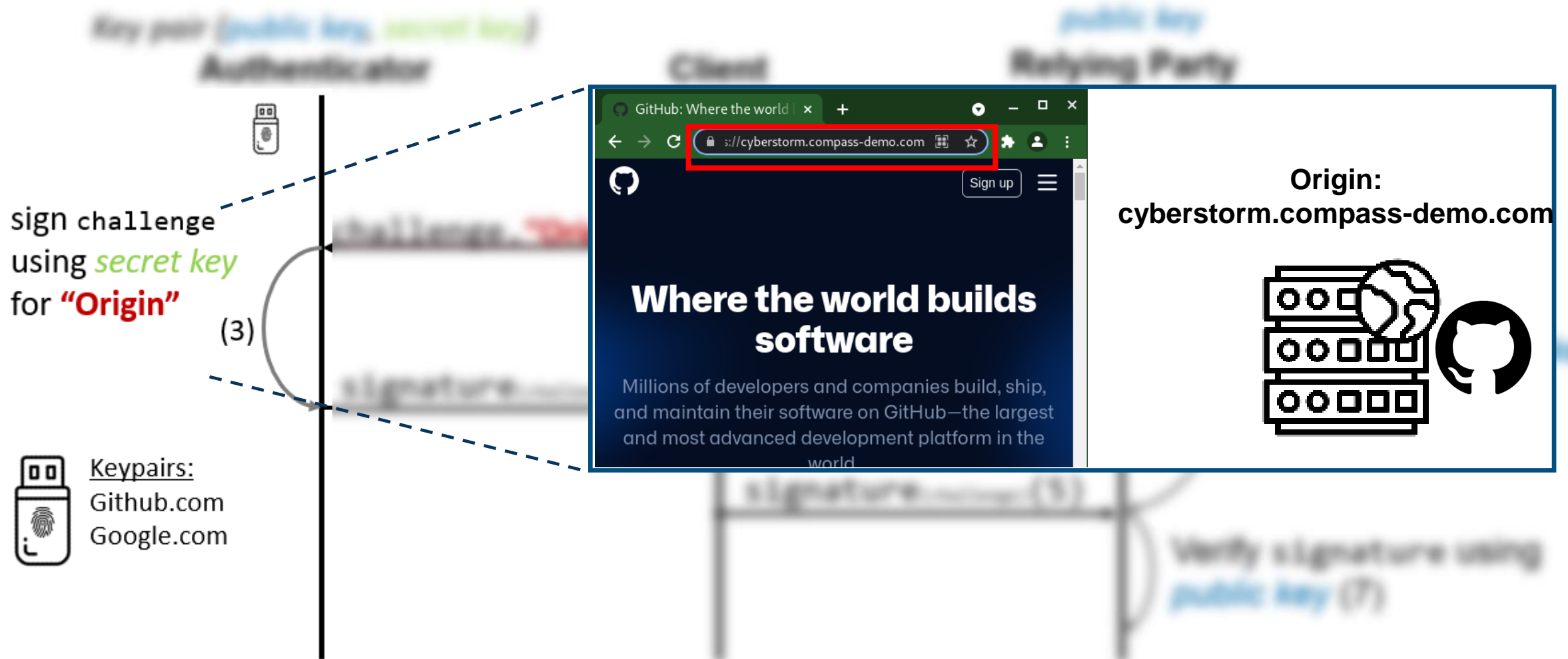
Phishing Protection (1) - Github



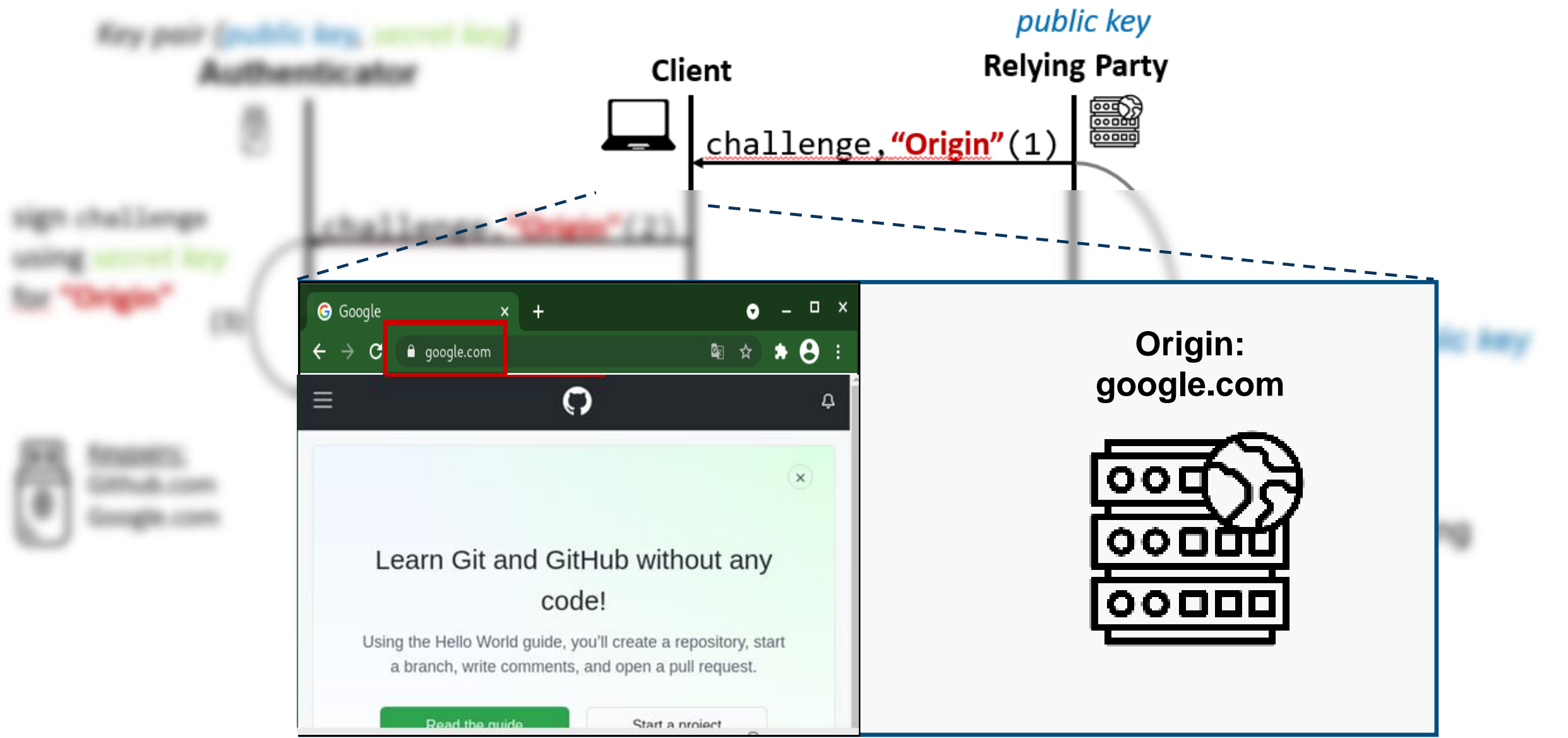
Phishing Protection (2) - Github



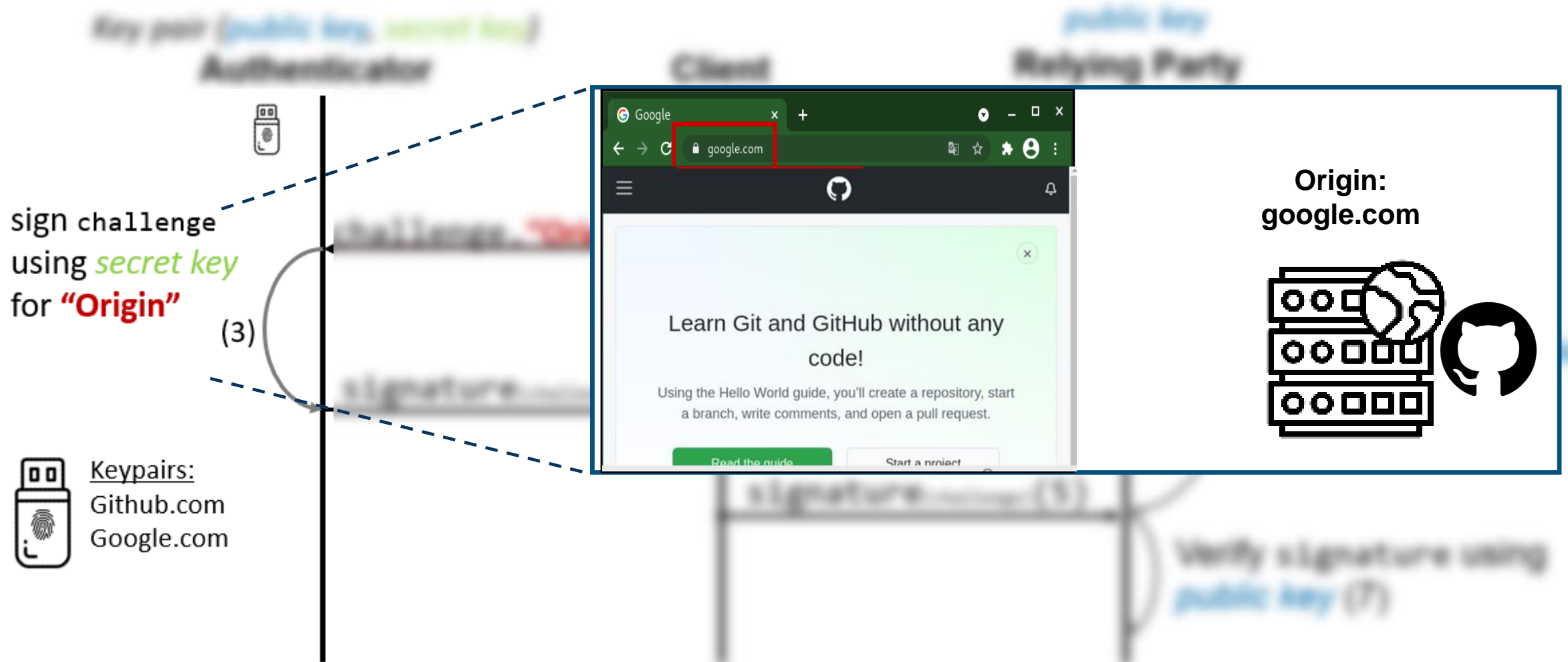
Phishing Protection (2) - Github



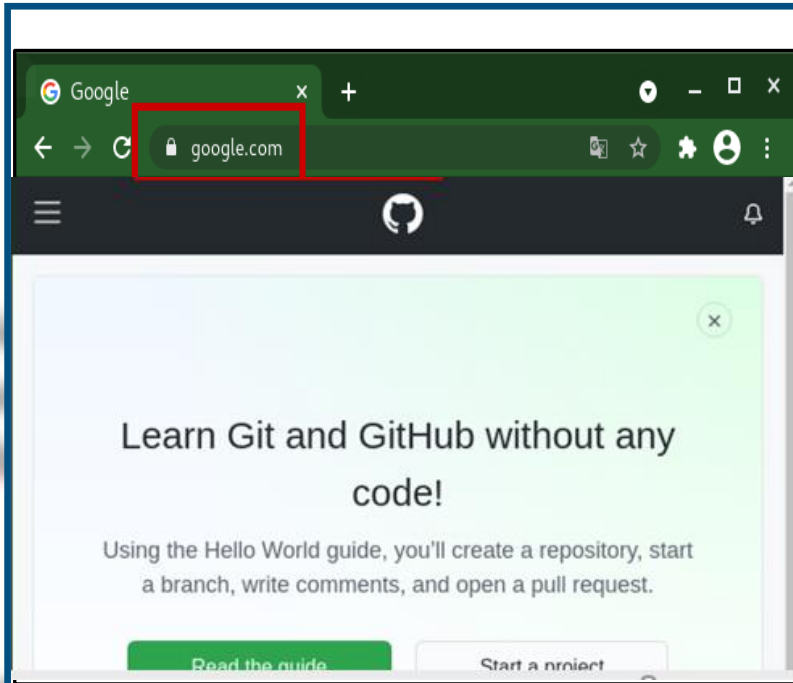
Phishing Protection (3) - Github



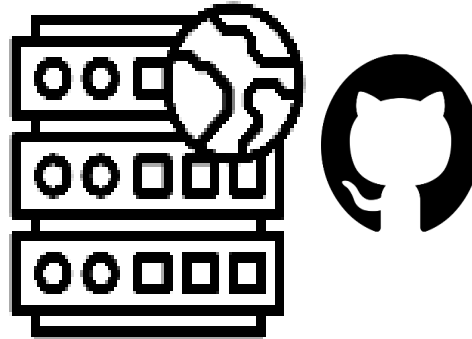
Phishing Protection (3) - Github



Phishing Protection (3) - Github



Origin: google.com



Verify signature using *public key* (7)





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