ИСПОЛЬЗУЕМ USB-ТОКЕНЫ ДЛЯ АУТЕНТИФИКАЦИИ В БРАУЗЕРЕ

Алексей Авдеев, Mish.Design

👨‍💻 О себе

1. 👨 Алексей Авдеев (https://twitter.com/avdeev_alexey)
2. 👔 CTO, руковожу разработкой
3. 🌆 Из Нижнего Новгорода, работаю в Москве
4. 🌐 Mish.Design
5. 👴 Программирую с 2002 года

Вы ретвитнули

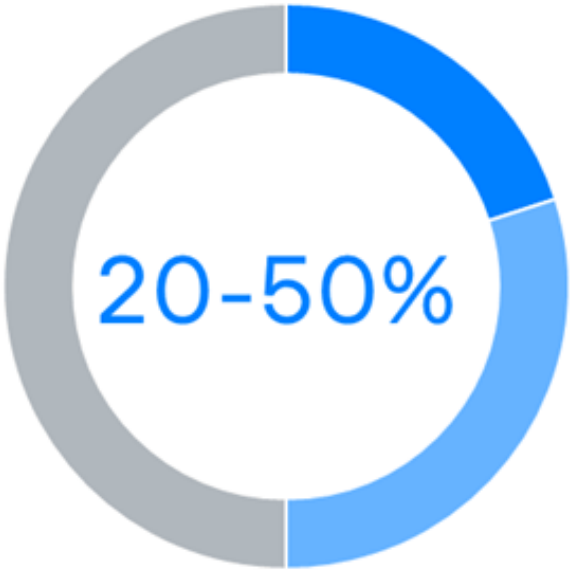
sadcore bitch
@ohkatewow

волки бэкендеров делают auth

5:34 PM · 9 авг. 2021 г. · Twitter Web App

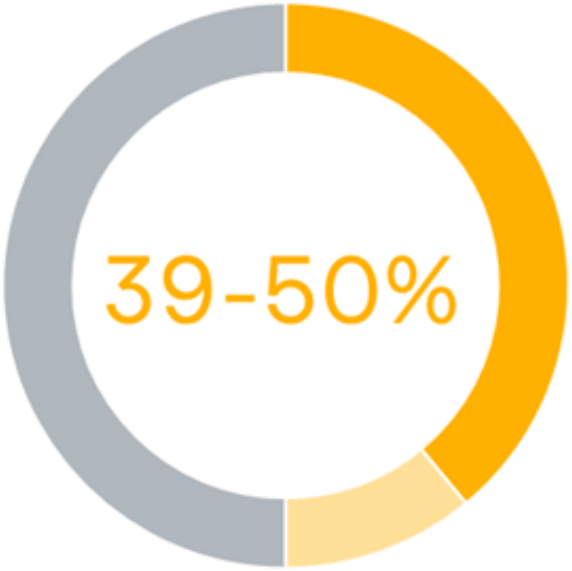
Пароли уязвимы

1960



of all help desk calls are related to password resets

Gartner Group



of people reuse personal or business passwords for workplace accounts

State of Password and Authentication Security Behaviors Report 2020

of breaches involved weak or stolen credentials

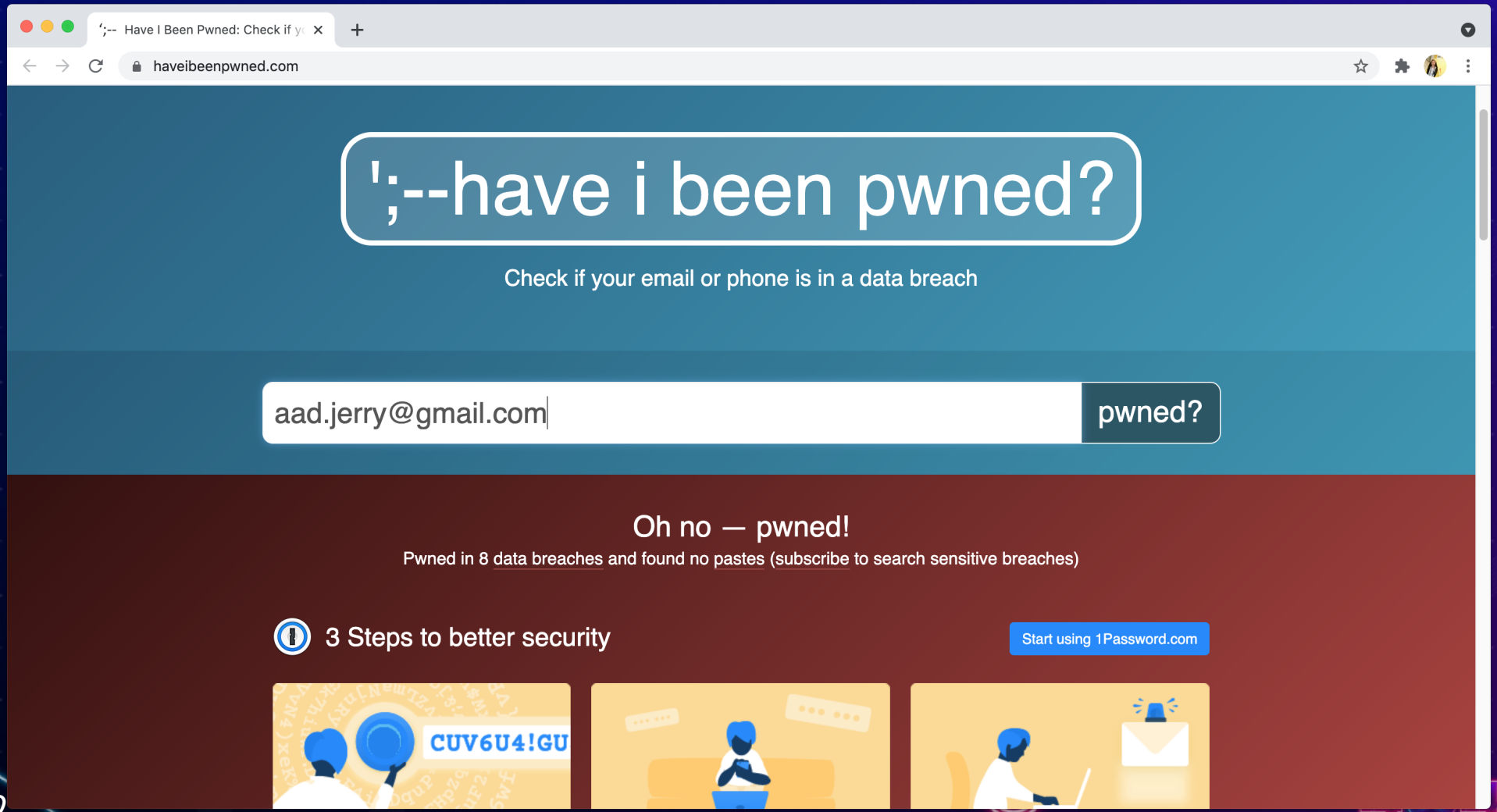
Verizon DBIR 2021

Простой пароль – слабая защита

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884

# of characters	Numerical [0-9]	Upper- and lowercase letters [a-Z]	Number, upper- and lowercase letters [0-9a-Z]	Numbers, upper- and lowercase letters and symbols [0-9a-Z%$]
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 secs
7	instantly	2 secs	6 secs	49 mins
8	instantly	1 min	6 mins	5 days
9	instantly	1 hour	6 hours	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 secs	20 years	162 years	8m years
13	16 secs	1k years	10k years	1bn years
14	3 mins	53k years	622k years	176bn years
15	26 mins	3m years	39m years	27tn years
16	4 hours	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

Сложный пароль — сложно запомнить

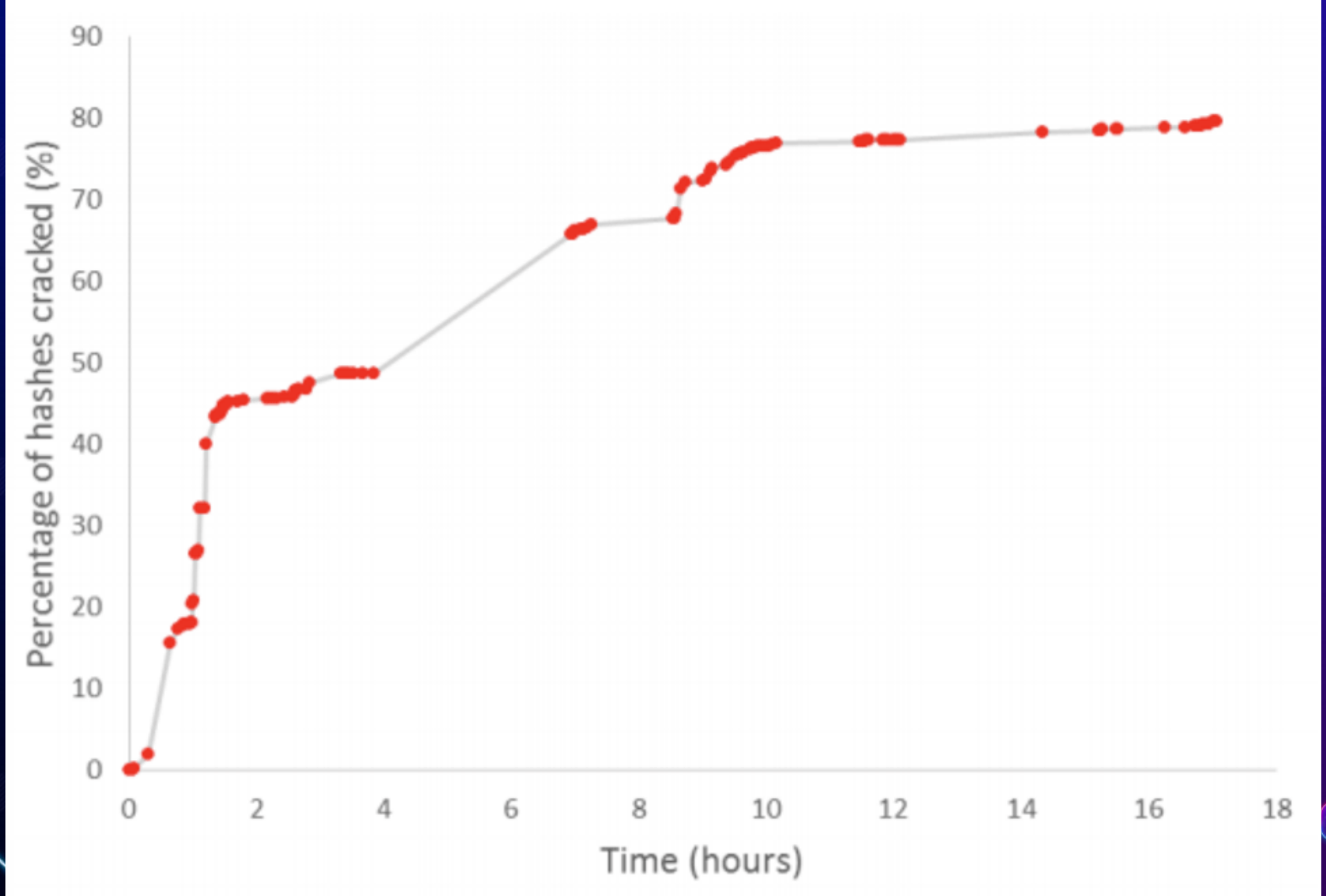

';-- Have I Been Pwned: Check if y
haveibeenpwned.com
';--have i been pwned?
Check if your email or phone is in a data breach
aad.jerry@gmail.com
pwned?
Oh no — pwned!
Pwned in 8 data breaches and found no pastes (subscribe to search sensitive breaches)
3 Steps to better security
Start using 1Password.com
CUV6U4!GU

Сбер
@sberbank

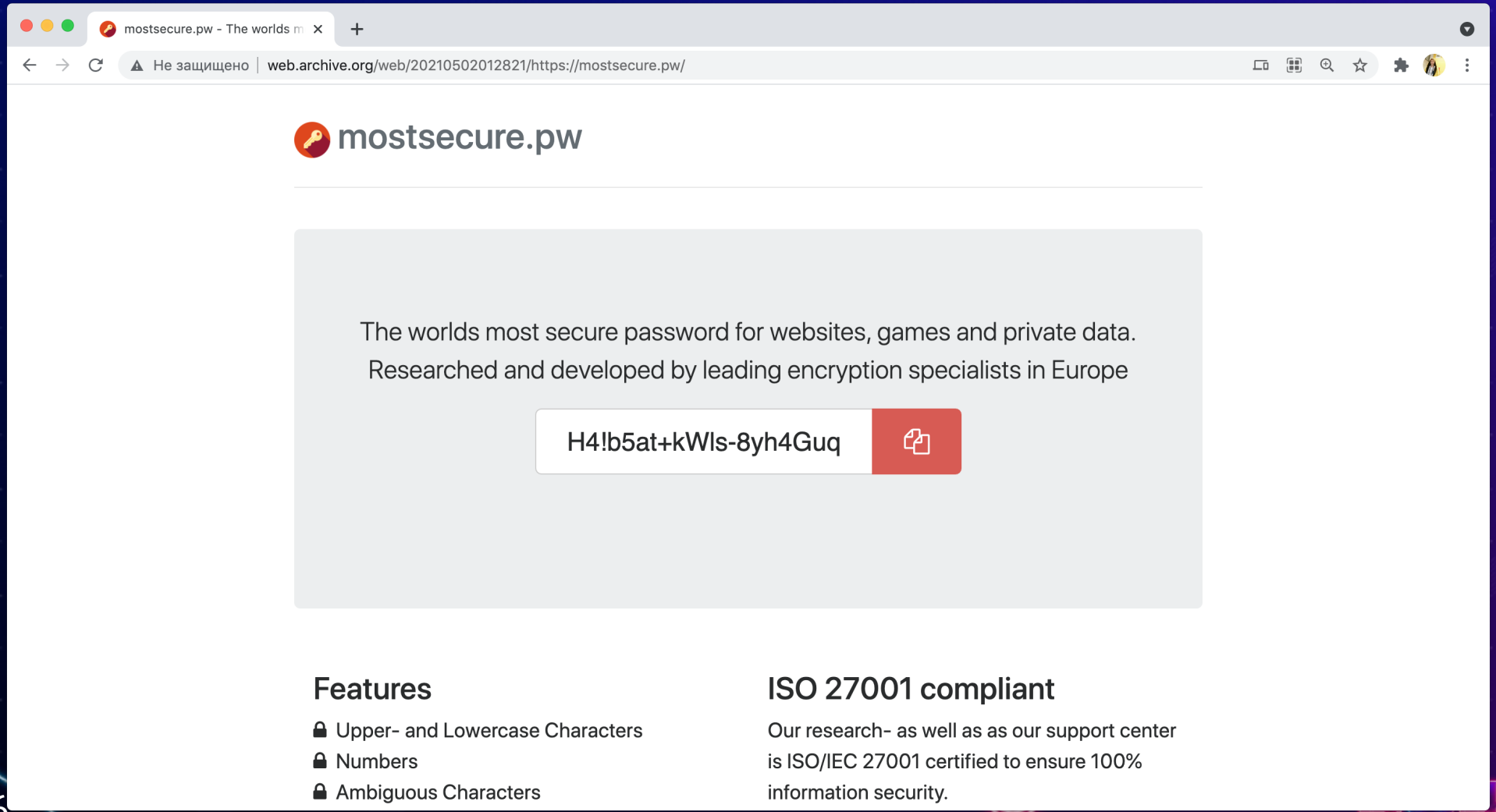
В ответ @a_okshus

Да, логин и пароль не чувствительны к регистру, чтобы пользователям было удобнее. Не переживайте, это безопасно.

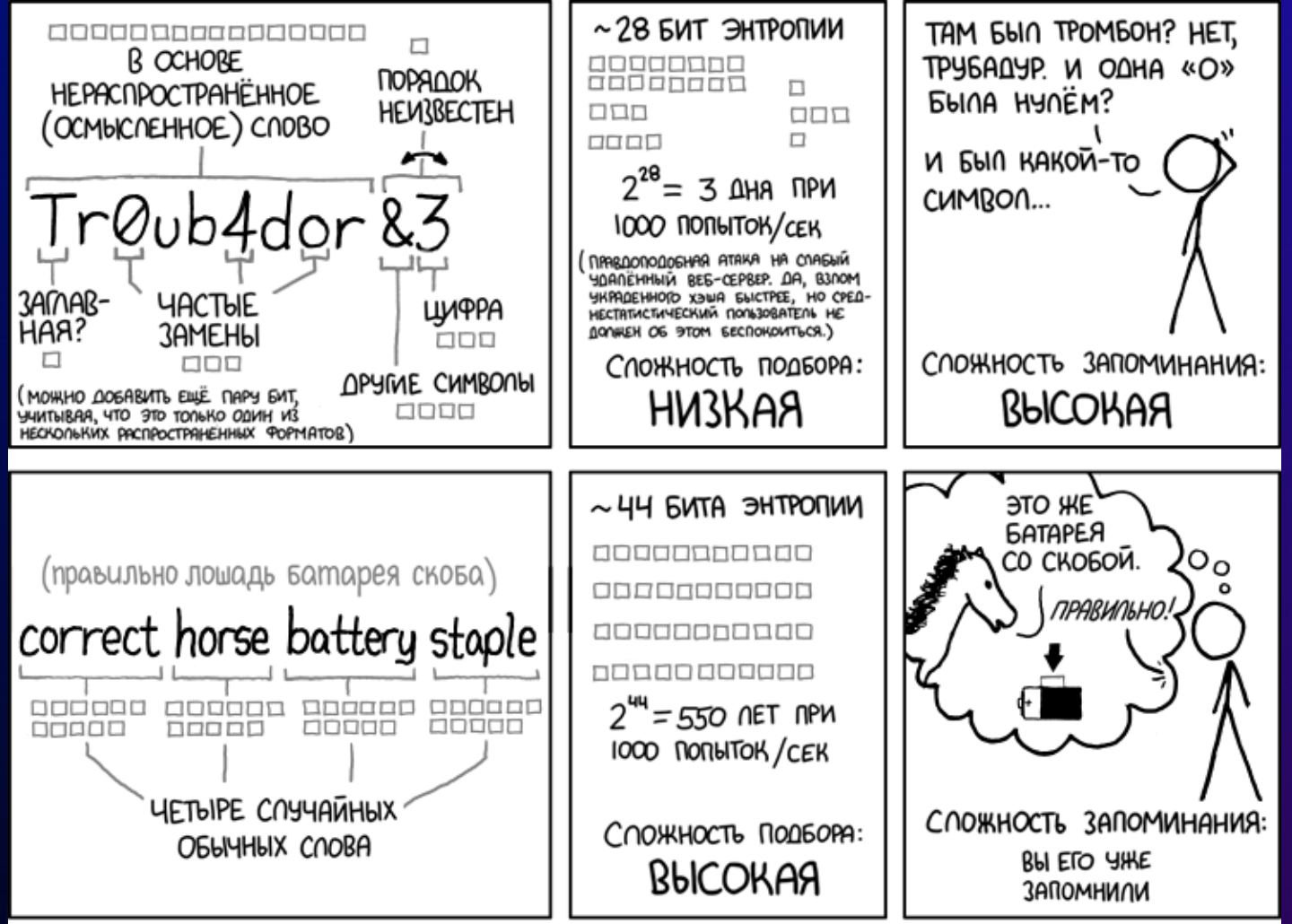
8:36 AM · 7 сент. 2020 г. · Angry.Space


Percentage of hashes cracked (%)
90
80
70
60
50
40
30
20
10
0
0
2
4
6
8
10
12
14
16
18
Time (hours)

Много паролей


mostsecure.pw - The worlds m
Не защищено | web.archive.org/web/20210502012821/https://mostsecure.pw/
mostsecure.pw
The worlds most secure password for websites, games and private data.
Researched and developed by leading encryption specialists in Europe
H4!b5at+kWls-8yh4Guq
Features
Upper- and Lowercase Characters
Numbers
Ambiguous Characters
ISO 27001 compliant
Our research- as well as as our support center is ISO/IEC 27001 certified to ensure 100% information security.

Парольные фразы


В ОСНОВЕ НЕРАСПРОСТРАНЁННОЕ (ОСМЫСЛЕННОЕ) СЛОВО
ПОРЯДОК НЕИЗВЕСТЕН
Tr0ub4dor&3
ЗАГЛАВ-НАЯ?
ЧАСТЫЕ ЗАМЕНЫ
ЦИФРА
ДРУГИЕ СИМВОЛЫ
(МОЖНО ДОБАВИТЬ ЕЩЁ ПАРУ БИТ, УЧИТЫВАЯ, ЧТО ЭТО ТОЛЬКО ОДИН ИЗ НЕСКОЛЬКИХ РАСПРОСТРАНЁННЫХ ФОРМАТОВ)
~28 БИТ ЭНТРОПИИ
2^{28} = 3 ДНЯ ПРИ 1000 ПОПЫТОК/СЕК
(ПРАВДОПОДОБНАЯ АТАКА НА СЛАБЫЙ УДАЛЁННЫЙ ВЕБ-СЕРВЕР. ДА, ВЗЛОМ УКРАДЕННОГО ХЭША БЫСТРЕЕ, НО СРЕДНЕСТАТИСТИЧЕСКИЙ ПОЛЬЗОВАТЕЛЬ НЕ ДОЛЖЕН ОБ ЭТОМ БЕСПОКОИТЬСЯ.)
СЛОЖНОСТЬ ПОДБОРА:
НИЗКАЯ
ТАМ БЫЛ ТРОМБОН? НЕТ, ТРУБАДУР. И ОДНА «О» БЫЛА НУЛЁМ?
И БЫЛ КАКОЙ-ТО СИМВОЛ...
СЛОЖНОСТЬ ЗАПОМИНАНИЯ:
ВЫСОКАЯ
(правильно лошадь батарея скоба)
correct horse battery staple
ЧЕТЫРЕ СЛУЧАЙНЫХ ОБЫЧНЫХ СЛОВА
~44 БИТА ЭНТРОПИИ
2^{44} = 550 ЛЕТ ПРИ 1000 ПОПЫТОК/СЕК
СЛОЖНОСТЬ ПОДБОРА:
ВЫСОКАЯ
ЭТО ЖЕ БАТАРЕЯ СО СКОБОЙ.
ПРАВИЛЬНО!
СЛОЖНОСТЬ ЗАПОМИНАНИЯ:
ВЫ ЕГО УЖЕ ЗАПОМНИЛИ
ЗА 20 ЛЕТ СТАРАНИЙ МЫ НАУЧИЛИ ВСЕХ ИСПОЛЬЗОВАТЬ ПАРОЛИ, КОТОРЫЕ ЧЕЛОВЕКУ ЗАПОМНИТЬ СЛОЖНО, А КОМПЬЮТЕРУ ПОДОБРАТЬ ЛЕГКО.

World Passw*rd Day 2021

Пароли мертвы
(с) Билл Гейтс, 2004

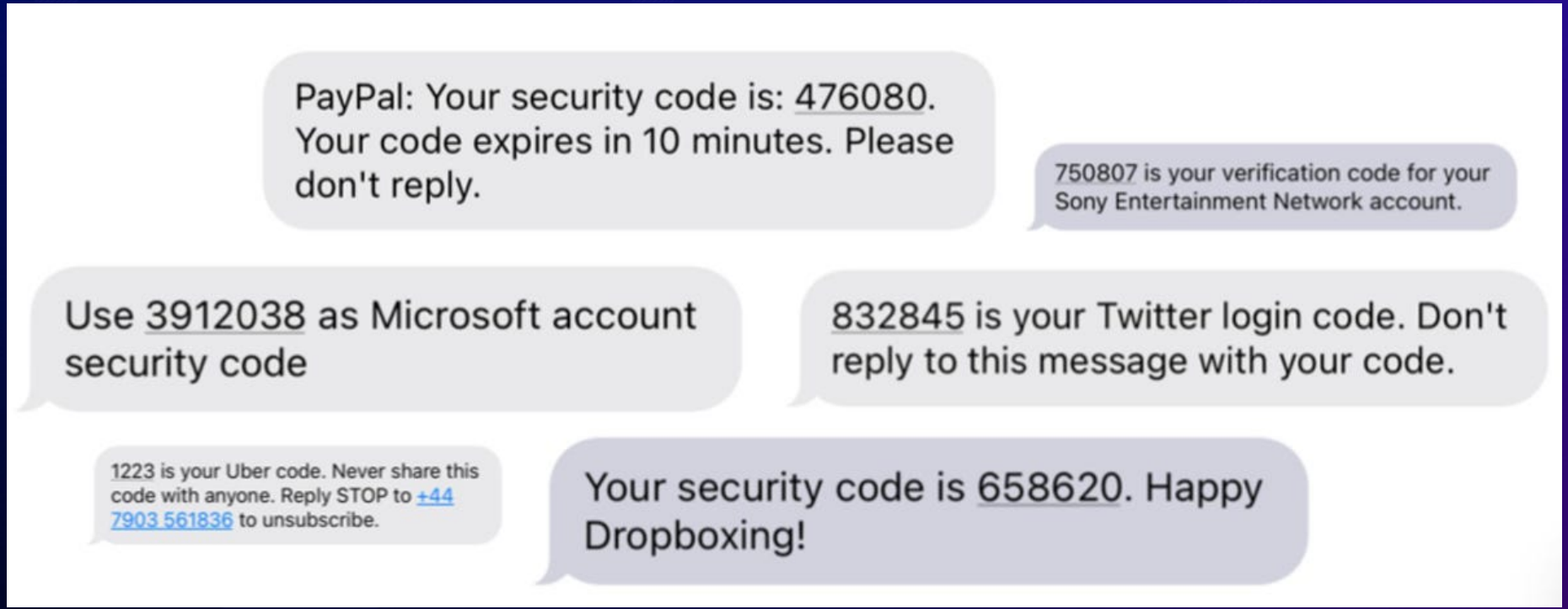
Многофакторная аутентификация (MFA)

Факторы аутентификации

- Фактор знания
- Фактор владения
- Фактор свойства
- Фактор местоположения

Одноразовый пароль

SMS


PayPal: Your security code is: 476080. Your code expires in 10 minutes. Please don't reply.
750807 is your verification code for your Sony Entertainment Network account.
Use 3912038 as Microsoft account security code
832845 is your Twitter login code. Don't reply to this message with your code.
1223 is your Uber code. Never share this code with anyone. Reply STOP to +44 7903 561836 to unsubscribe.
Your security code is 658620. Happy Dropboxing!

SMS

– Не приходят

SMS-подтверждение входа

На ваш мобильный телефон выслано SMS-сообщение с кодом подтверждения.
Телефон: **********
Сессия: 12919015

Внимание! У вас осталось 3 попытки запроса кода, после чего аккаунт будет заблокирован на 2 часа

Код подтверждения

(04:35) Выслать код повторно

Нет доступа к телефону?

Подтвердить

SMS

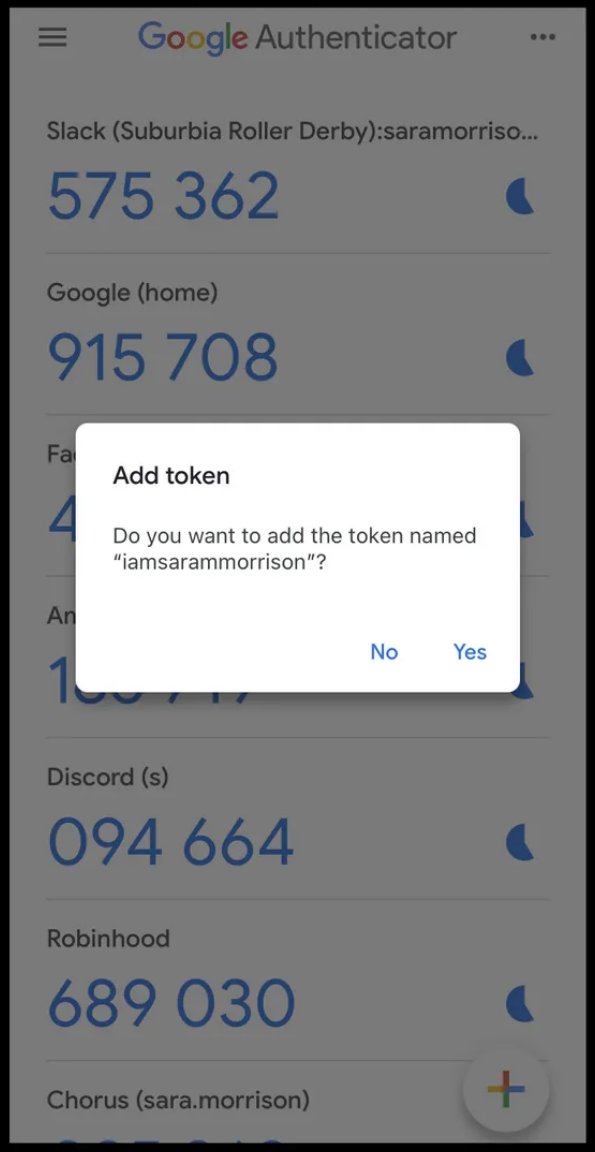
- Не приходят
- Стоят денег
- Можно подглядеть
- Можно подменить/перевыпустить SIM-карту
- Можно перехватить

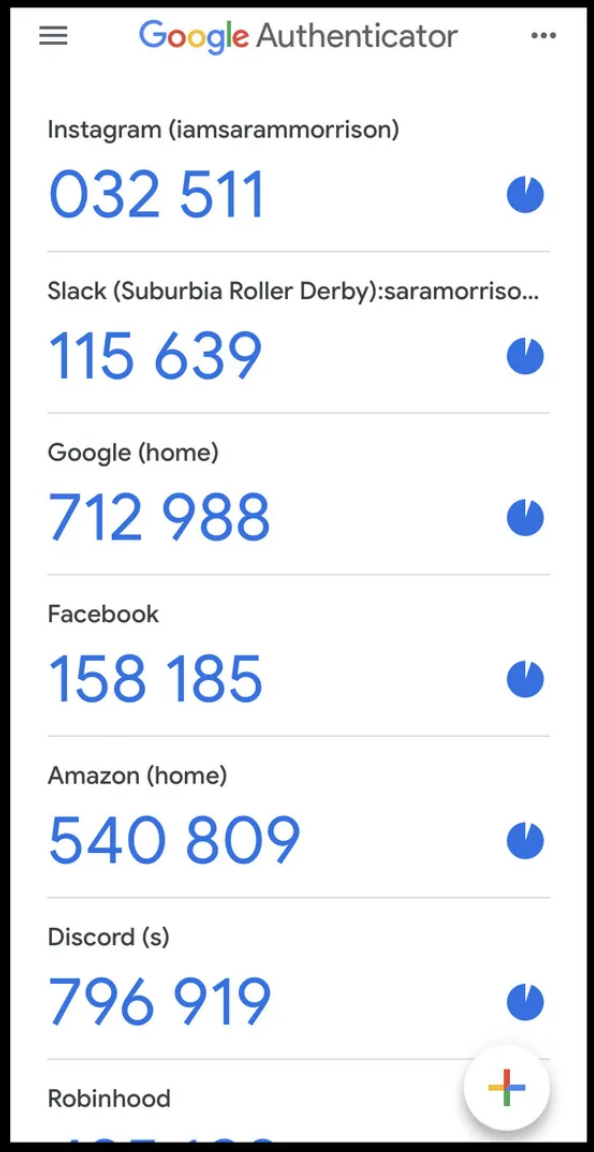
Push Notifications

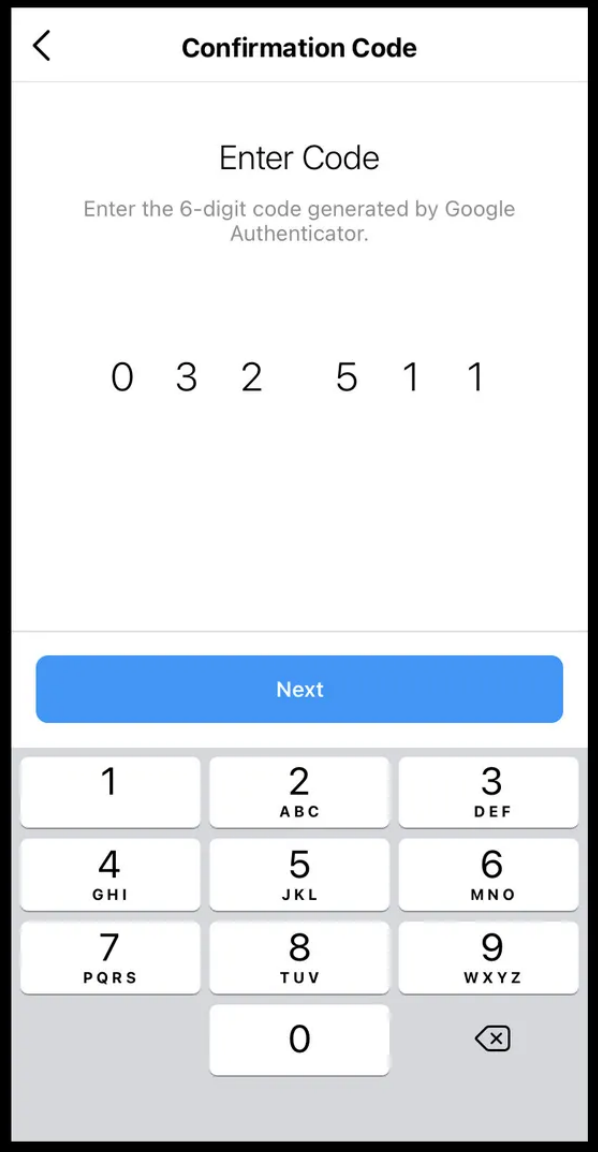
Push Notifications

- Не приходят
- Стоят денег (меньше)
- Можно подглядеть
- ~~Можно подменить/перевыпустить SIM-карту~~
- ~~Можно перехватить~~

Authenticator app

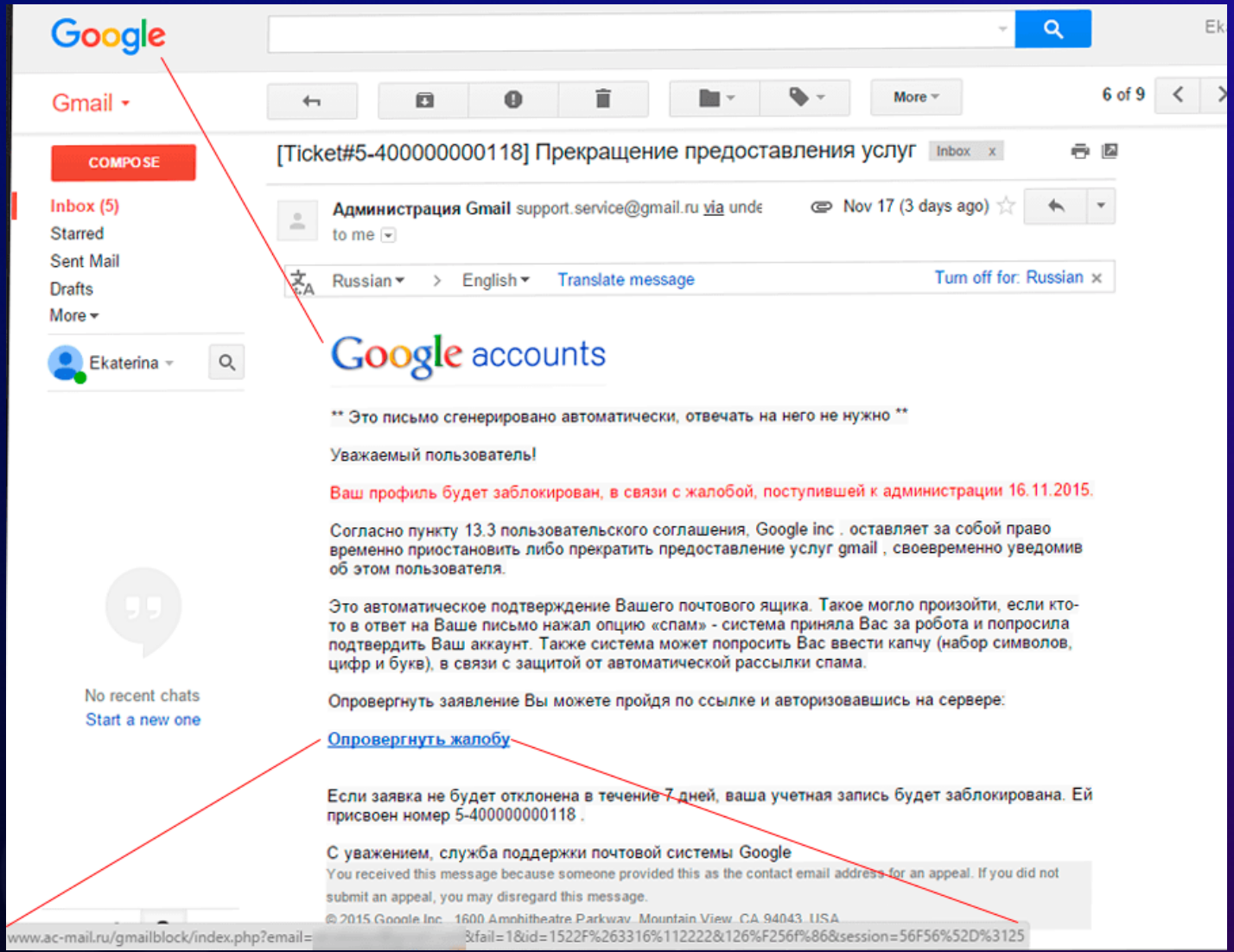

Google Authenticator
Slack (Suburbia Roller Derby):saramorriso...
575 362
Google (home)
915 708
Add token
Do you want to add the token named "iamsarammorrison"?
No
Yes
Discord (s)
094 664
Robinhood
689 030
Chorus (sara.morrison)


Google Authenticator
Instagram (iamsarammorrison)
032 511
Slack (Suburbia Roller Derby):saramorriso...
115 639
Google (home)
712 988
Facebook
158 185
Amazon (home)
540 809
Discord (s)
796 919
Robinhood


Confirmation Code
Enter Code
Enter the 6-digit code generated by Google Authenticator.
0 3 2 5 1 1
Next
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

Authenticator app

- Секреты хранятся программно
- Уязвимы для фишинга


Google
Gmail
COMPOSE
Inbox (5)
Starred
Sent Mail
Drafts
More
Ekaterina
No recent chats
Start a new one
More
6 of 9
[Ticket#5-400000000118] Прекращение предоставления услуг
Inbox x
Администрация Gmail support.service@gmail.ru via unde
Nov 17 (3 days ago)
to me
Russian
English
Translate message
Turn off for: Russian
Google accounts
** Это письмо сгенерировано автоматически, отвечать на него не нужно **
Уважаемый пользователь!
Ваш профиль будет заблокирован, в связи с жалобой, поступившей к администрации 16.11.2015.
Согласно пункту 13.3 пользовательского соглашения, Google inc , оставляет за собой право временно приостановить либо прекратить предоставление услуг gmail , своевременно уведомив об этом пользователя.
Это автоматическое подтверждение Вашего почтового ящика. Такое могло произойти, если кто-то в ответ на Ваше письмо нажал опцию «спам» - система приняла Вас за робота и попросила подтвердить Ваш аккаунт. Также система может попросить Вас ввести капчу (набор символов, цифр и букв), в связи с защитой от автоматической рассылки спама.
Опровергнуть заявление Вы можете пройдя по ссылке и авторизовавшись на сервере:
Опровергнуть жалобу
Если заявка не будет отклонена в течение 7 дней, ваша учетная запись будет заблокирована. Ей присвоен номер 5-400000000118 .
С уважением, служба поддержки почтовой системы Google
You received this message because someone provided this as the contact email address for an appeal. If you did not submit an appeal, you may disregard this message.
© 2015 Google Inc. 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
www.ac-mail.ru/gmailblock/index.php?email=
&fail=1&id=1522F%263316%112222&126%F256f%86&session=56F56%52D%3125

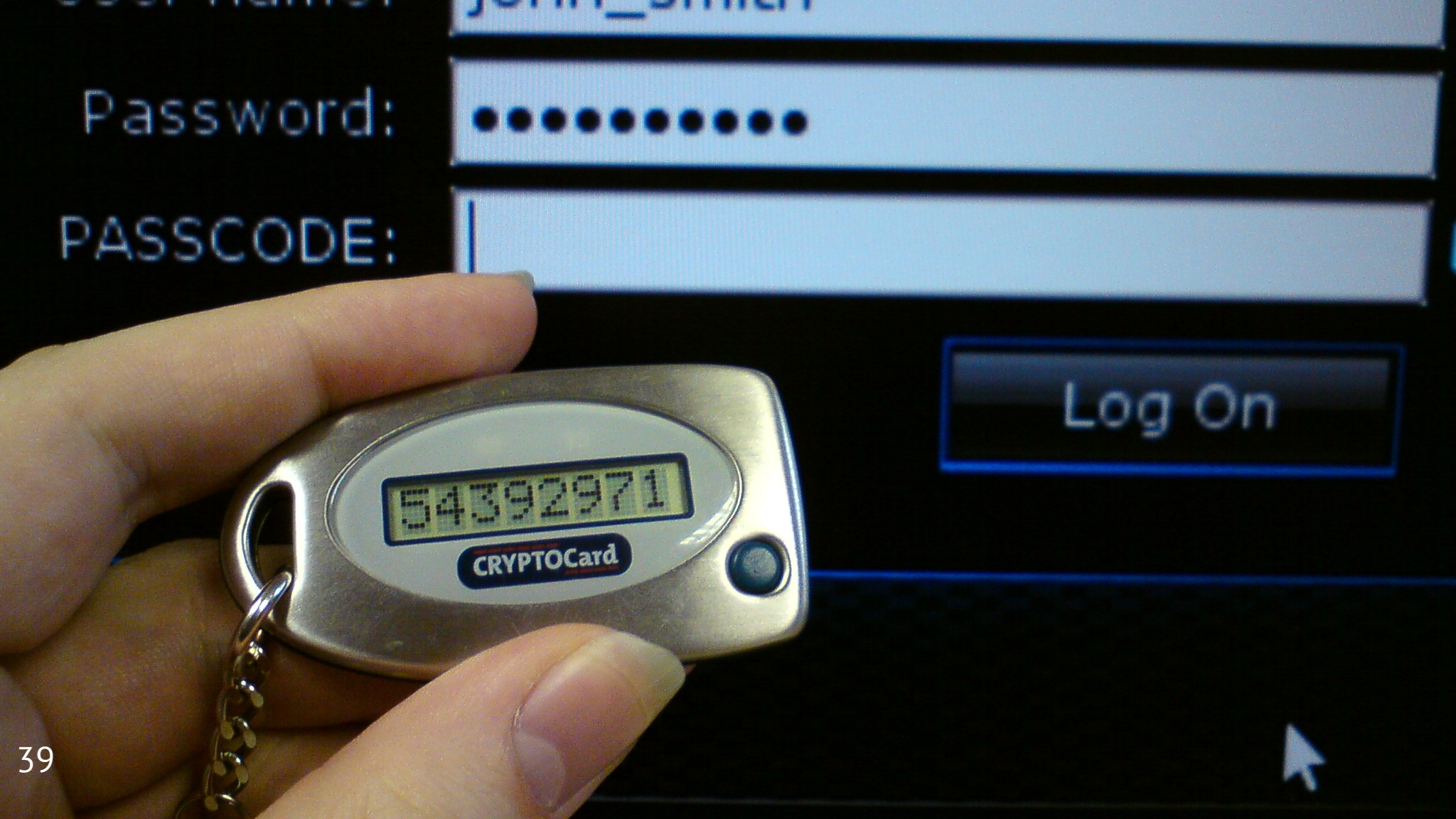
Токен


1 GB
eToken
NG-FLASH
523745
eToken
NG-OTP
eToken
PRO SmartCard
922627

Стандарты и сертификаты

- FIPS 140
- ГОСТ Р 34.10-2012
- ГОСТ Р 34.11-2012
- Сертификат ФСБ
- Сертификат ФСТЭК

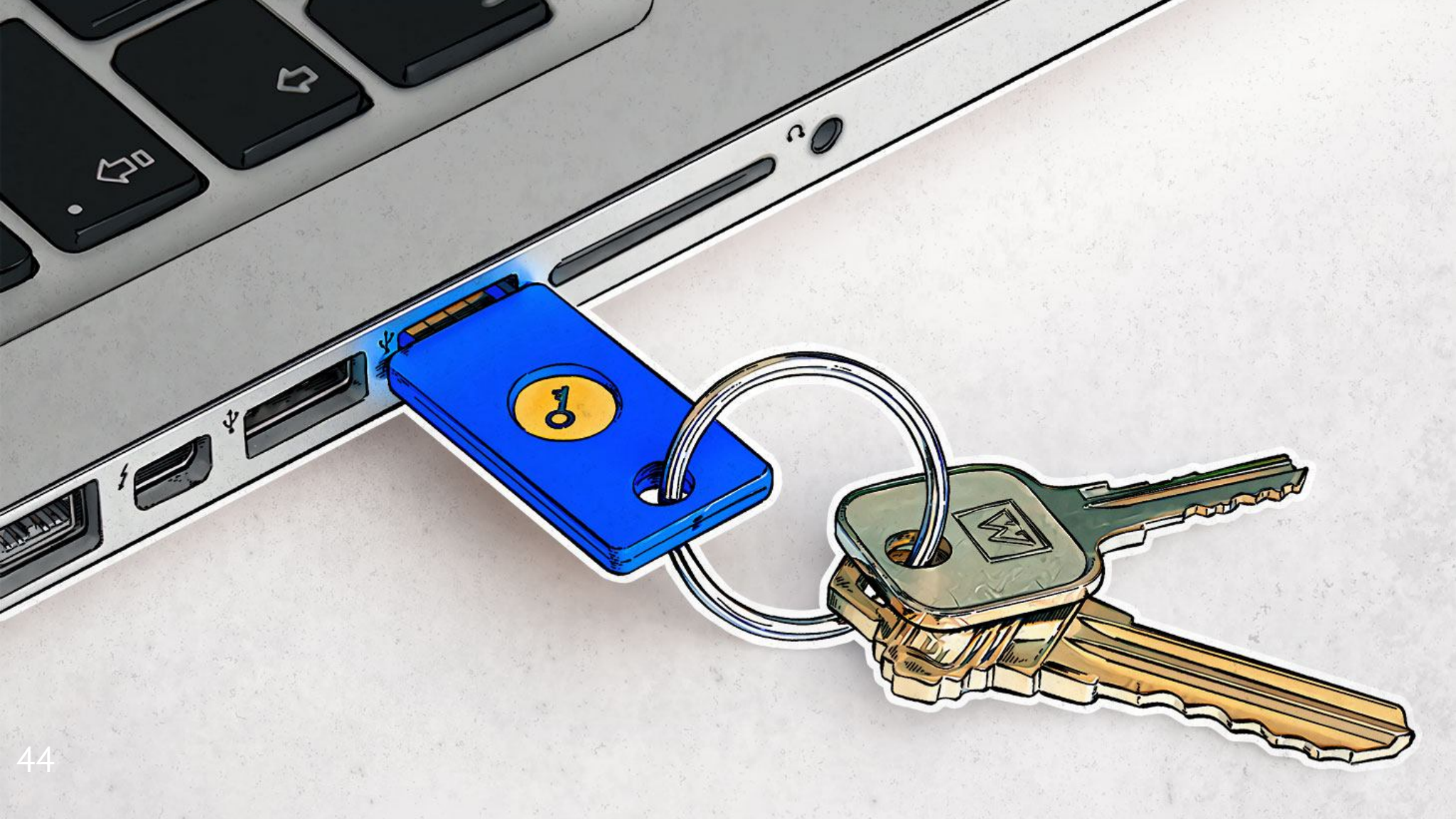
Токены без подключения


Password:
PASSCODE:
Log On
54392971
CRYPTOCard

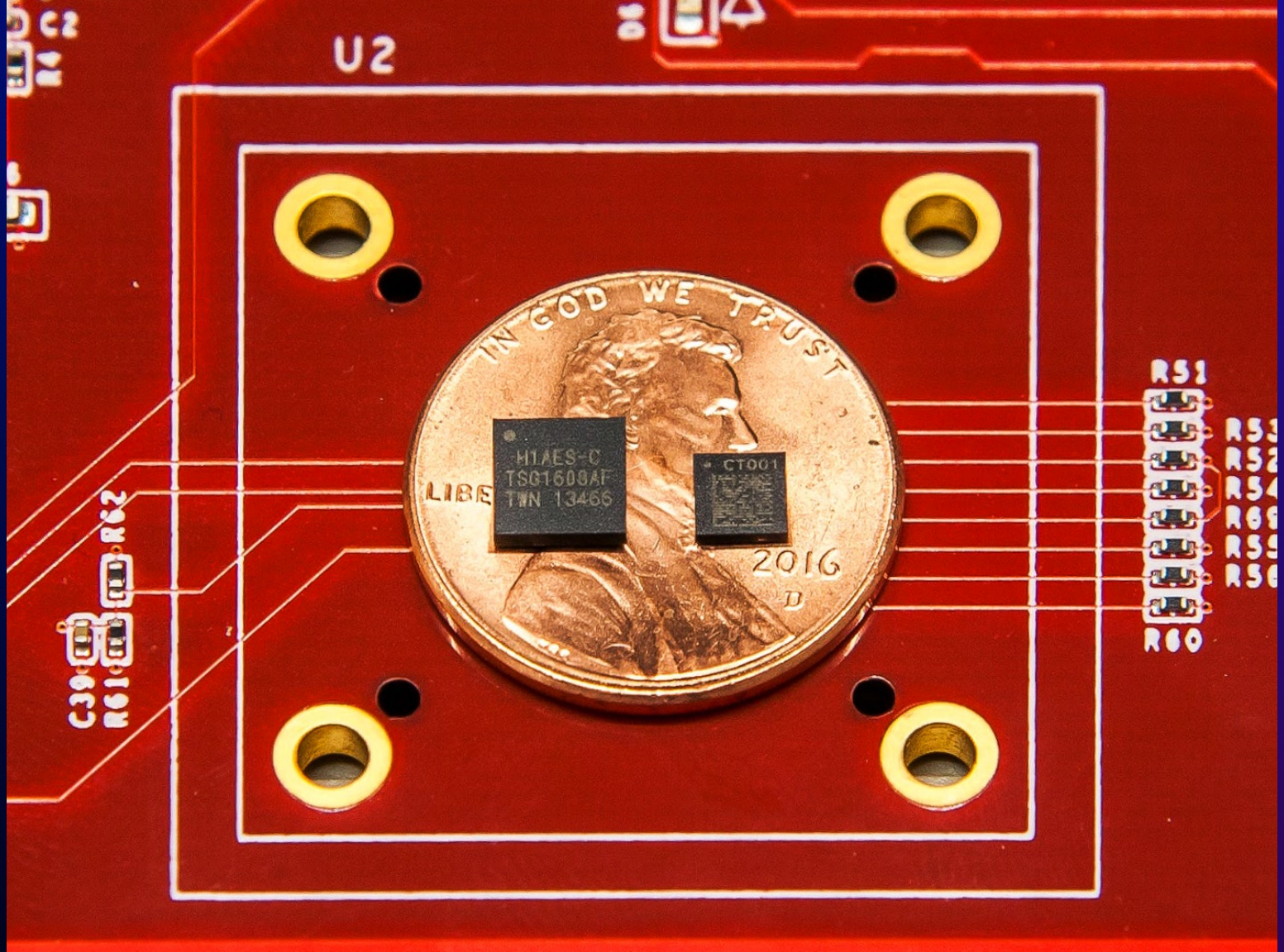

ENTER PIN
HID
1 2 3
4 5 6
7 8 9
MENU
0
OK
ENTER PIN
HID

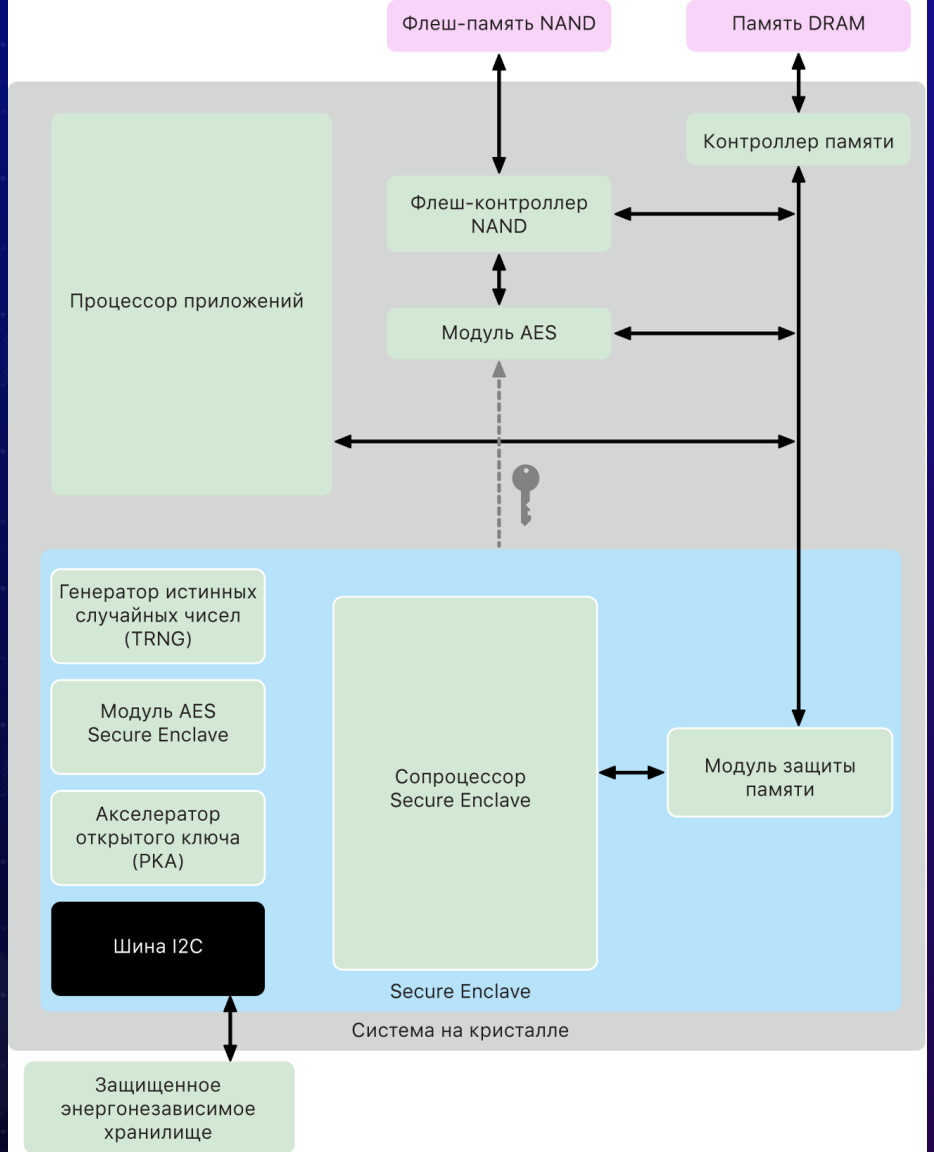
Беспроводные токены

Токены с подключением



Встроенная криптография


U2
IN GOD WE TRUST
LIBE
2016
D
H1AES-C
TSG1608AF
TWN 13466
CT001
R51
R60
C39
R61
R62


Флеш-память NAND
Память DRAM
Контроллер памяти
Флеш-контроллер NAND
Процессор приложений
Модуль AES
Генератор истинных случайных чисел (TRNG)
Модуль AES Secure Enclave
Акселератор открытого ключа (PKA)
Шина I2C
Сопроцессор Secure Enclave
Модуль защиты памяти
Secure Enclave
Система на кристалле
Защищенное энергонезависимое хранилище

The Consumer Authentication Strength Maturity Model (CASMM) v5

8 PASSLESS

Passwordless *Examples*: WebAuthN, FIDO2

Rather than authenticating with passwords, you authenticate using OS-integrated biometrics.

VULNERABLE TO: SOCIAL ENG / EXTORTION

7 TOKEN2FA

Token-based 2FA *Examples*: OTP Token

In addition to quality passwords in a manager, you authenticate using a physical token that only you have.

VULNERABLE TO: PHISHING

6 APP2FA

App-based 2FA *Examples*: Google Authenticator, Authy

In addition to quality passwords in a manager, you authenticate using an application that only you can access.

VULNERABLE TO: DEVICE COMPROMISE

5 SMS2FA

SMS-based 2FA *Examples*: Any SMS-based auth

In addition to quality passwords in a manager, you authenticate using a text sent to your mobile device.

VULNERABLE TO: SIM-SWAPPING / SMS-HIJACKING

4 PASSMAN

Password Manager *Examples*: 1Password, LastPass

In addition to having unique passwords, you also store them securely in an encrypted archive.

VULNERABLE TO: ACCOUNT RESET / TAKEOVER

3 QUALPASS

Quality Passwords *Examples*: A012-2vOs-11xM

Your passwords are not just unique, but they're long, random, and they include special characters.

VULNERABLE TO: PASSWORD DUMPS / CRACKING

2 UNIQPASS

Unique Passwords *Examples*: DOBs, Teams, Schools

Your passwords are unique, but they're too short, simple, or contain personal information.

VULNERABLE TO: LIVE PASSWORD GUESSING

1 SHARPASS

Shared Passwords *Examples*: Gmail, Wells Fargo, Netflix

You use the same password in multiple places across the internet.

VULNERABLE TO: CREDENTIAL STUFFING

DANIEL MIESSLER 2021


ВООБРАЖЕНИЕ КРИПТОМАНЬЯКА:
НА ЕГО НОУТЕ ВСЁ ЗАШИФРОВАНО! ДАВАЙ ПОСТРОИМ КЛАСТЕР ЗА МИЛЛИОН ДОЛЛАРОВ И ВСЁ ВЗЛОМАЕМ.
НЕ ВЫЙДЕТ – ТАМ 4096-БИТНЫЙ RSA!
ЧЁРТ! НАШ КОВАРНЫЙ ПЛАН СОРВАН!
ЧТО ПРОИЗОШЛО БЫ В РЕАЛЬНОСТИ:
НА ЕГО НОУТЕ ВСЁ ЗАШИФРОВАНО. ДАЙ ЕМУ НАРКОТЫ И ДУБАСЬ ЭТИМ ГАЕЧНЫМ КЛЮЧОМ ЗА 5 БАКСОВ, ПОКА ОН НЕ СКАЖЕТ ПАРОЛЬ.
ПОНЯЛ.

Правила компьютерной безопасности

- не используйте компьютер
- не включайте компьютер
- не владейте компьютером

Fast IDentity Online (FIDO)


fido™
ALLIANCE
simpler
stronger
authentication


Google
NXP
PayPal
gemalto
security to be free
Daon
QUALCOMM
SAMSUNG
Alibaba Group
amazon
Lenovo
BCcard
Infineon
RSA
yubico
Trust the Net.
fido
ALLIANCE
egis
AMERICAN EXPRESS
intel
nok nok
ING
Synaptics
IDEMIA
FEITIAN
WE BUILD SECURITY
ARM
aetna
Bank of America
Microsoft
docomo
RAON
SECURE
dedicated to changing the way online authentication is done.

FIDO Authenticator Certification Examples

L3+  USB U2F Token built on a CC-certified Secure Element **Certification: L3+**

L3  USB U2F Token built on a basic simple CPU, OS, is certified. Good physical anti-tampering enclosure

UAF implemented is a TA running on a certified TEE with POP memory

L2 

UAF implemented as a TA in an uncertified TEE

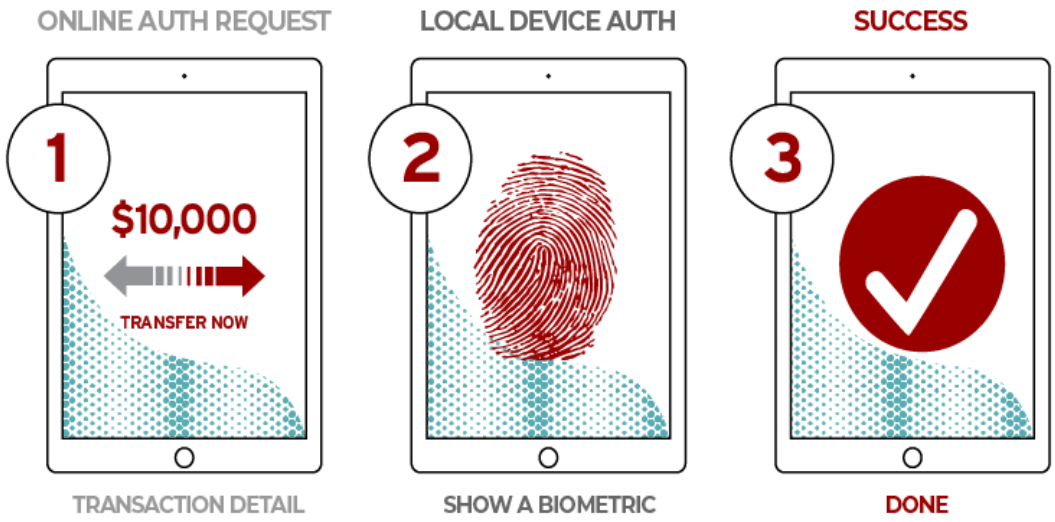
L1  Downloaded app making use of Touch ID on iOS **Certification: L1**

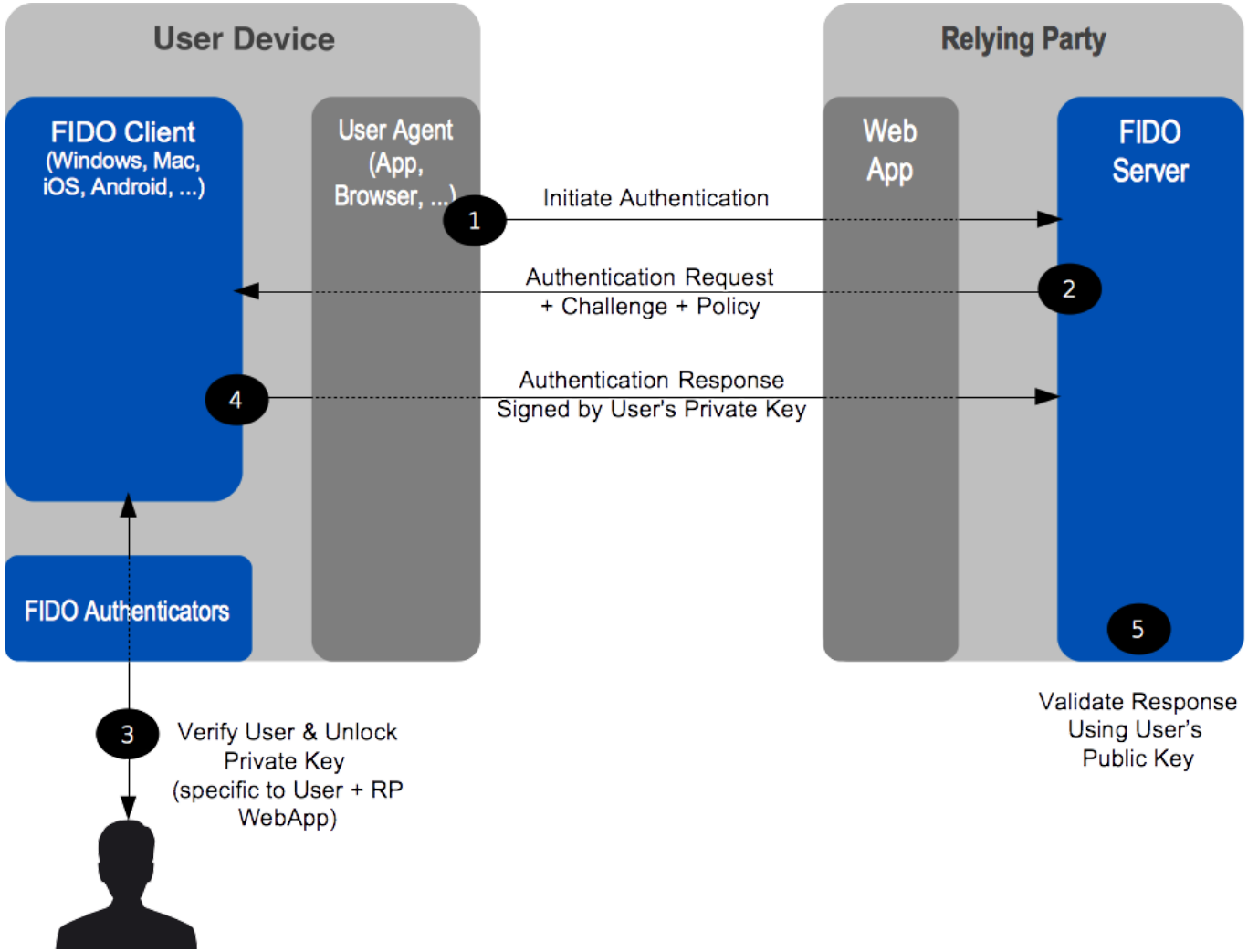
 FIDO2 making use of the Android keystore. Keystore is not certified **Certification: L1**

 FIDO2 built into a downloadable web browser app **Certification: L1**

Universal Authentication Framework (UAF, 2014)

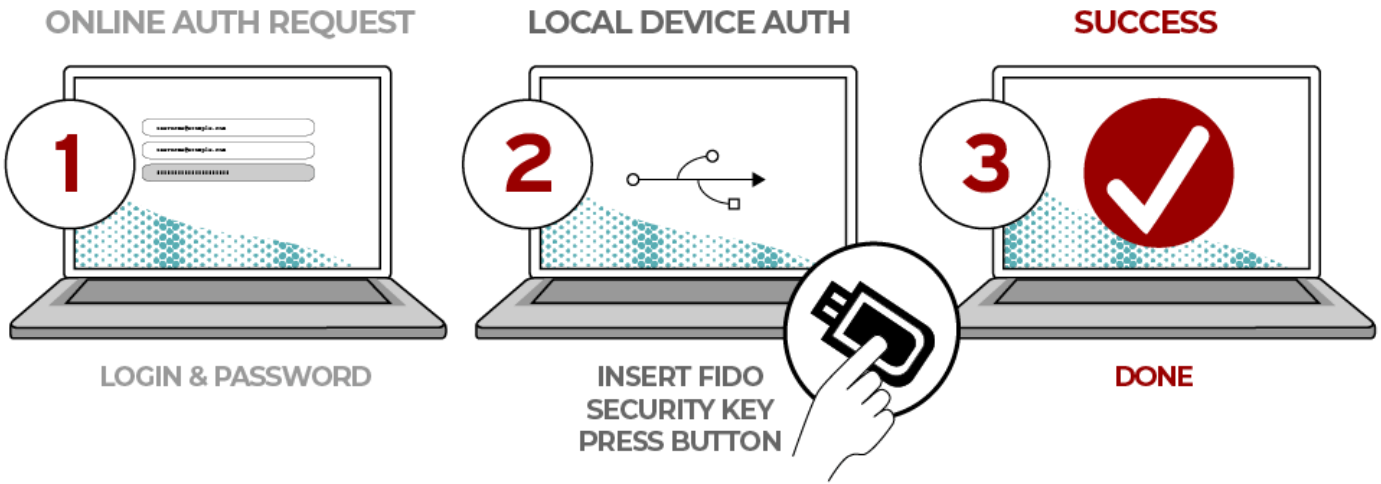
PASSWORDLESS EXPERIENCE (UAF standards)



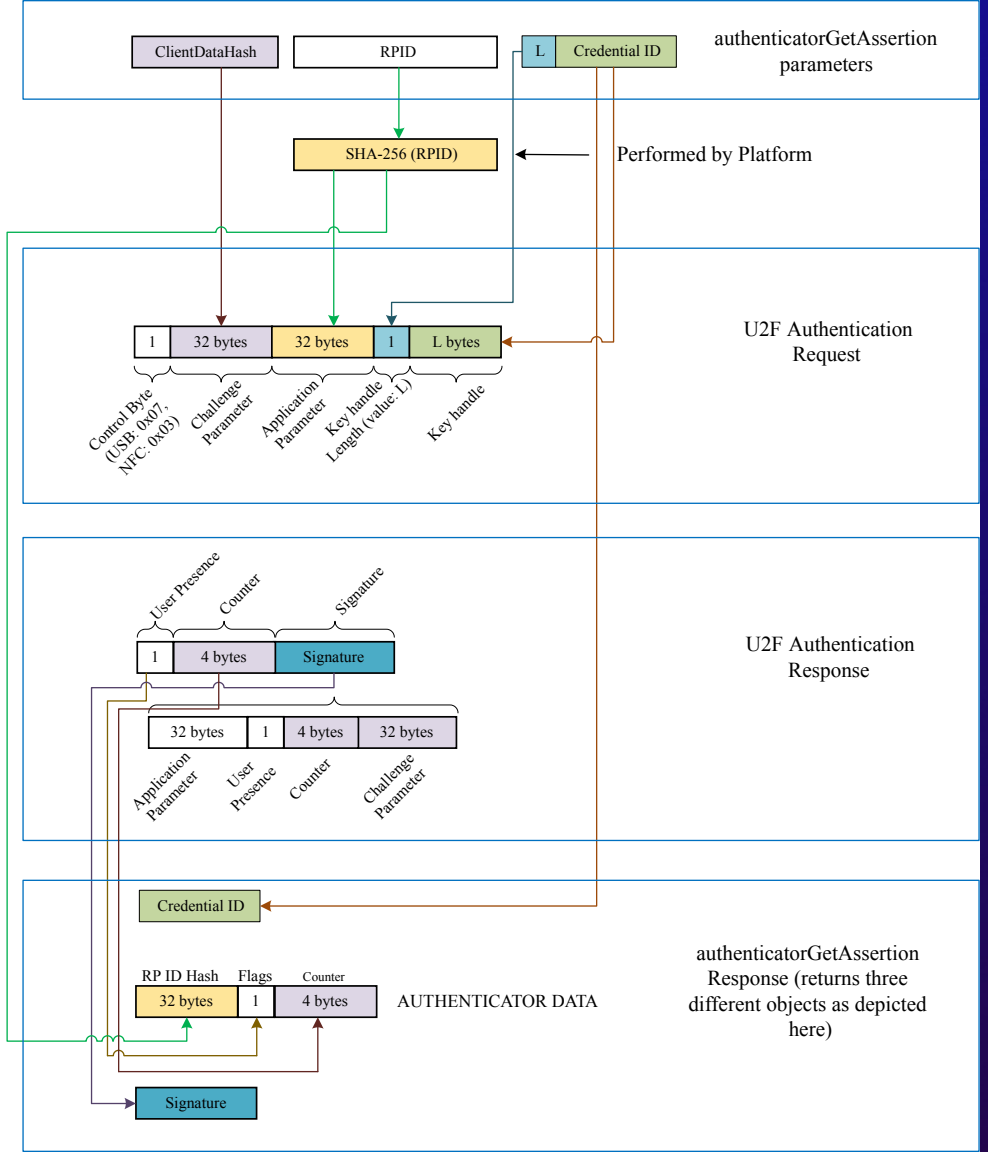

User Device
Relying Party
FIDO Client
(Windows, Mac,
iOS, Android, ...)
User Agent
(App,
Browser, ...)
Web
App
FIDO
Server
1
Initiate Authentication
Authentication Request
+ Challenge + Policy
2
4
Authentication Response
Signed by User's Private Key
FIDO Authenticators
5
3
Verify User & Unlock
Private Key
(specific to User + RP
WebApp)
Validate Response
Using User's
Public Key

Universal 2nd Factor (U2F)

SECOND FACTOR EXPERIENCE (U2F standards)



Client to Authenticator Protocol (CTAP)


ClientDataHash
RPID
L
Credential ID
authenticatorGetAssertion parameters
SHA-256 (RPID)
Performed by Platform
1
32 bytes
32 bytes
1
L bytes
Control Byte (USB: 0x07, NFC: 0x03)
Challenge Parameter
Application Parameter
Key handle Length (value: L)
Key handle
U2F Authentication Request
User Presence
Counter
Signature
1
4 bytes
Signature
32 bytes
1
4 bytes
32 bytes
Application Parameter
User Presence
Counter
Challenge Parameter
U2F Authentication Response
Credential ID
RP ID Hash
Flags
Counter
32 bytes
1
4 bytes
AUTHENTICATOR DATA
Signature
authenticatorGetAssertion Response (returns three different objects as depicted here)

FIDO 1.0 (2015)

FIDO 2.0 (2017)

Web Authentication API (WebAuthn)

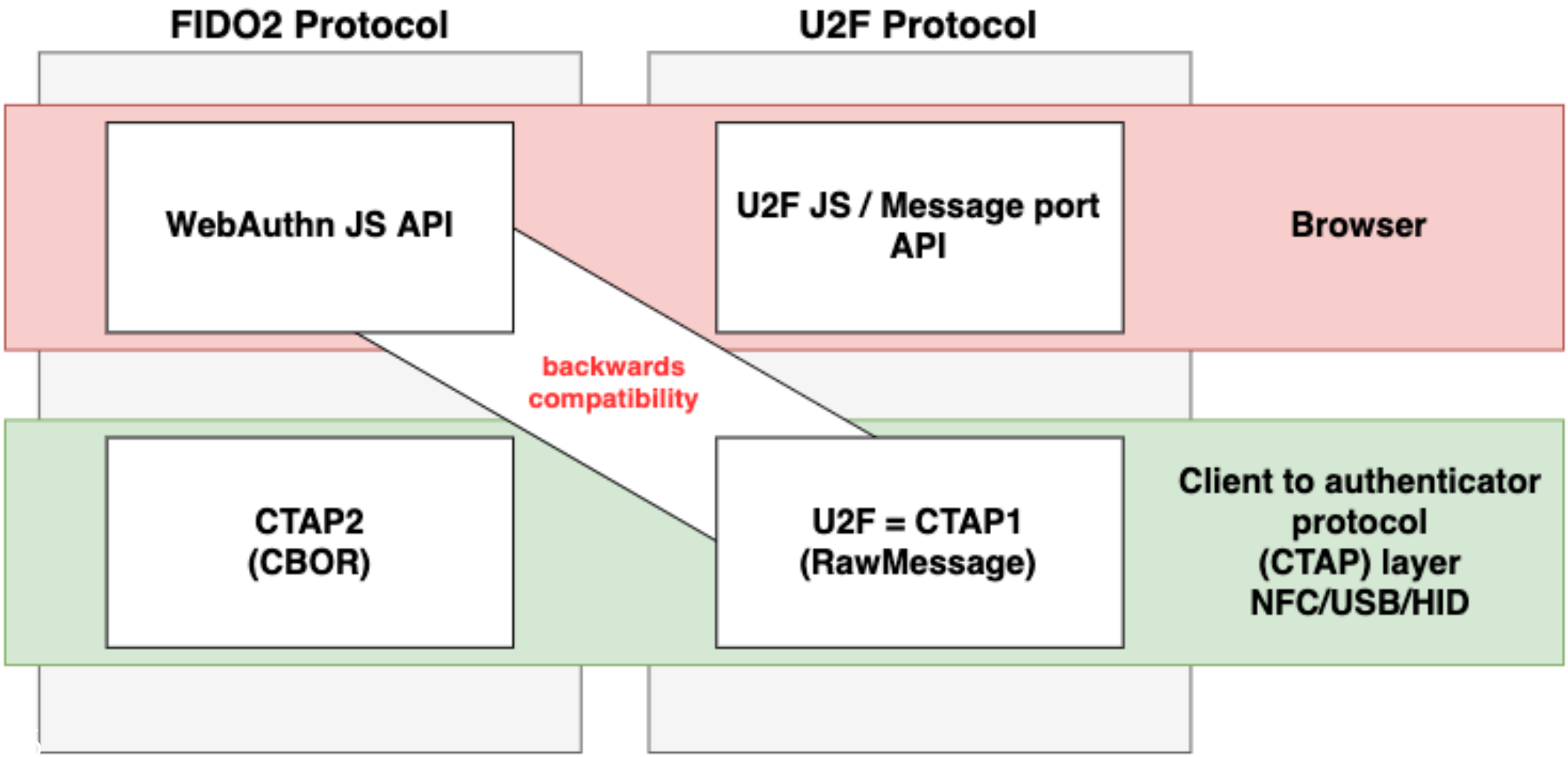
Закрепленный твит

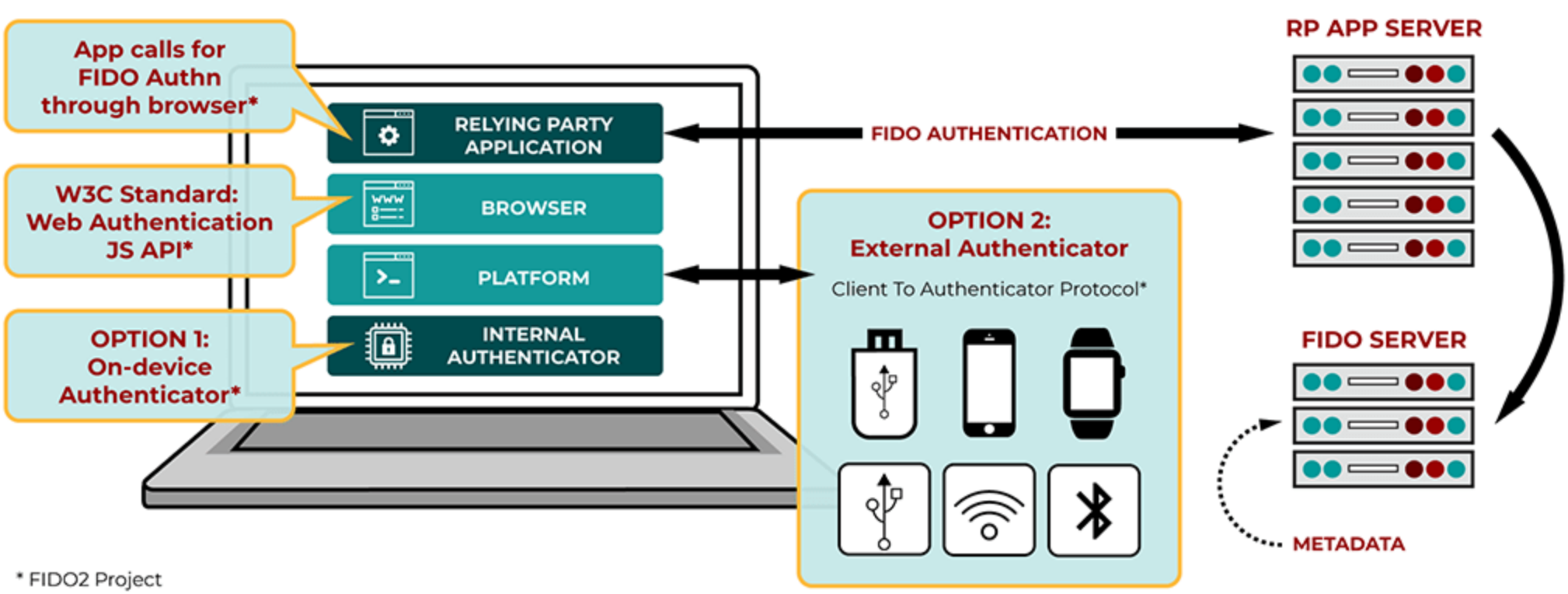
The FIDO Alliance
@FIDOAlliance

Wondering about the relationship between #FIDO and WebAuthn? A good rule of thumb to remember is FIDO2 = the #WebAuthn + CTAP protocols. 1/4

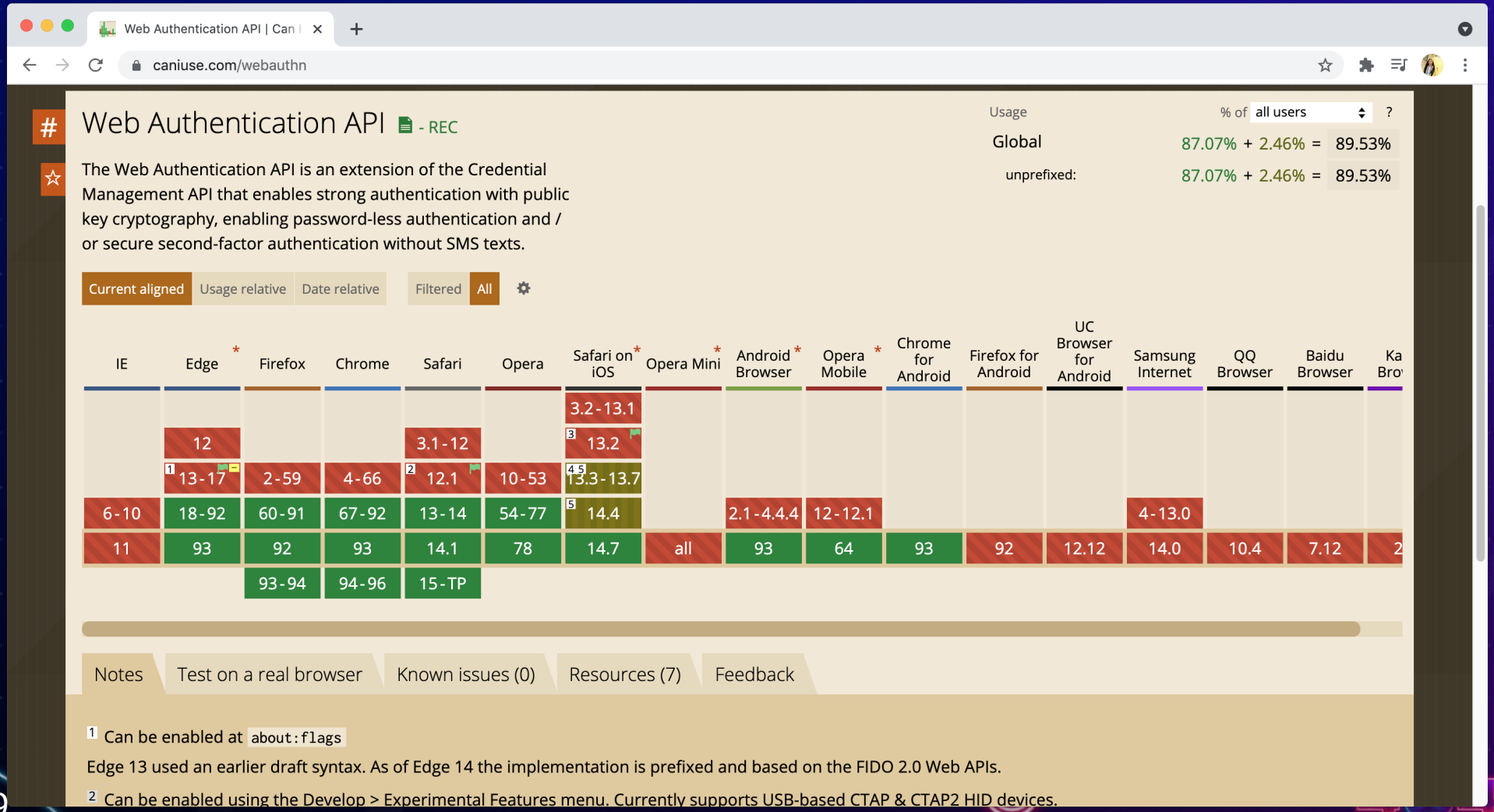
Перевести твит

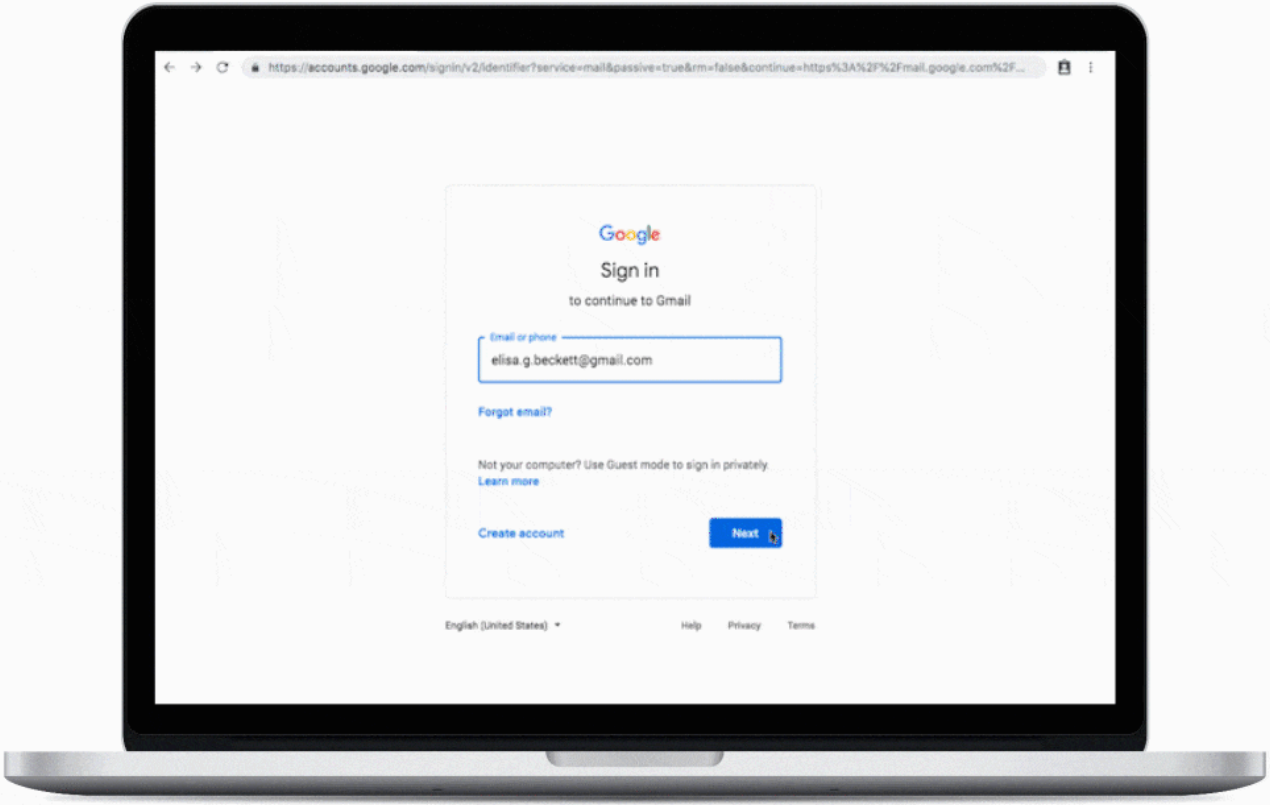
9:28 PM · 5 июн. 2020 г. · Twitter Web App


FIDO2 Protocol
U2F Protocol
WebAuthn JS API
U2F JS / Message port API
Browser
backwards compatibility
CTAP2 (CBOR)
U2F = CTAP1 (RawMessage)
Client to authenticator protocol (CTAP) layer NFC/USB/HID


App calls for FIDO Authn through browser*
W3C Standard: Web Authentication JS API*
OPTION 1: On-device Authenticator*
RELYING PARTY APPLICATION
BROWSER
PLATFORM
INTERNAL AUTHENTICATOR
FIDO AUTHENTICATION
RP APP SERVER
OPTION 2: External Authenticator
Client To Authenticator Protocol*
FIDO SERVER
METADATA
* FIDO2 Project

Passwordless = CTAP2 & WebAuthn


Web Authentication API | Can
caniuse.com/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
87.07% + 2.46% = 89.53%
unprefixed:
87.07% + 2.46% = 89.53%
Current aligned
Usage relative
Date relative
Filtered
All
IE
Edge
Firefox
Chrome
Safari
Opera
Safari on iOS
Opera Mini
Android Browser
Opera Mobile
Chrome for Android
Firefox for Android
UC Browser for Android
Samsung Internet
QQ Browser
Baidu Browser
3.2-13.1
12
3.1-12
13.2
13-17
2-59
4-66
12.1
10-53
13.3-13.7
6-10
18-92
60-91
67-92
13-14
54-77
14.4
2.1-4.4.4
12-12.1
4-13.0
11
93
92
93
14.1
78
14.7
all
93
64
93
92
12.12
14.0
10.4
7.12
93-94
94-96
15-TP
Notes
Test on a real browser
Known issues (0)
Resources (7)
Feedback
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.


https://accounts.google.com/signin/v2/identifier?service=mail&passive=true&rm=false&continue=https%3A%2F%2Fmail.google.com%2F...
Google
Sign in
to continue to Gmail
Email or phone
elisa.g.beckett@gmail.com
Forgot email?
Not your computer? Use Guest mode to sign in privately.
Learn more
Create account
Next
English (United States)
Help
Privacy
Terms


5:58
Friday, Mar 29 | 63°F
Pokémon...
Maps
YouTube
Photos
Keep Not...
Home
Chat
Gmail
Drive
Calendar
Meet

Additional security

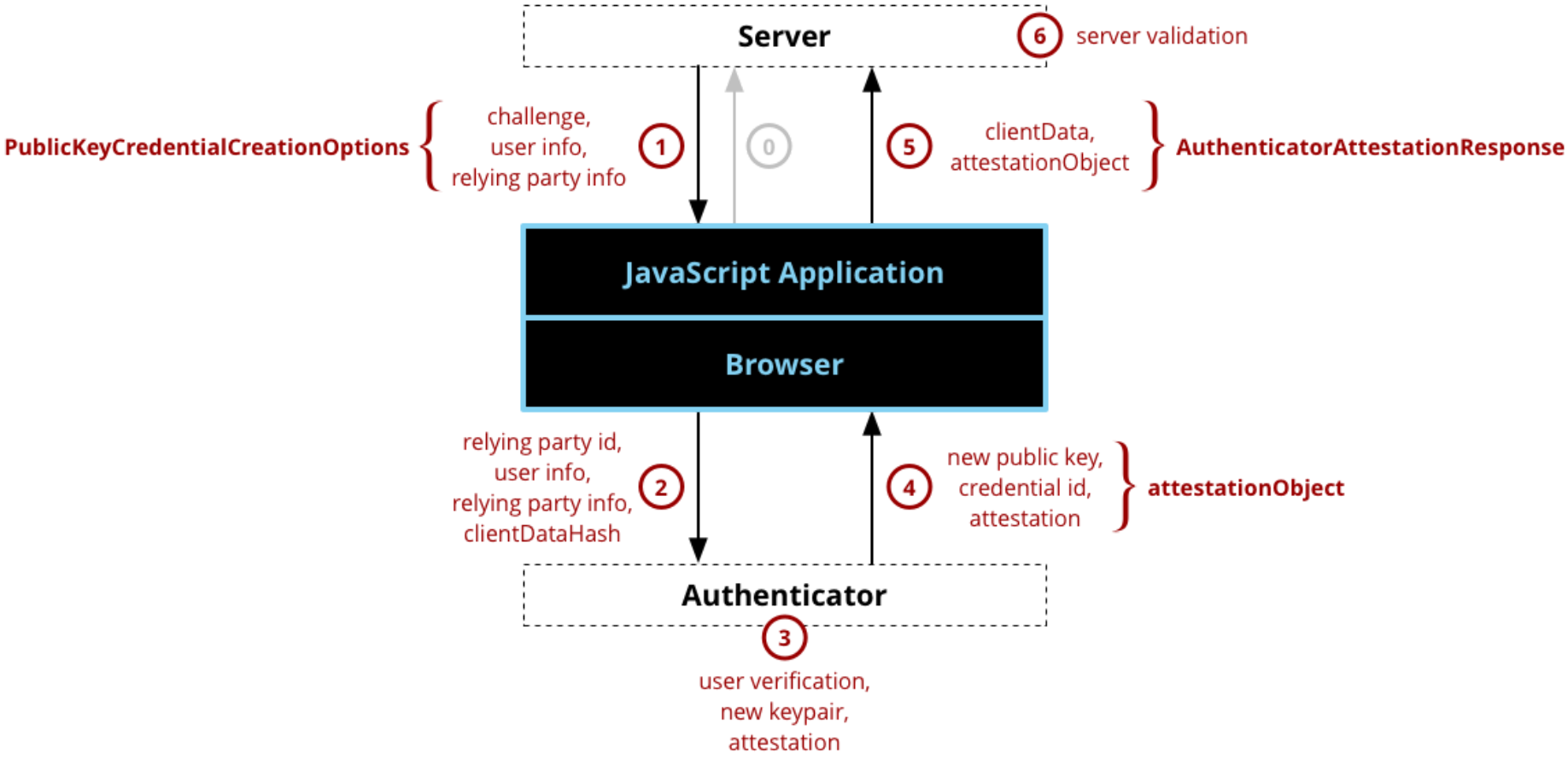
Increase your security by removing your password or by requiring two steps to verify your account when you sign in. Learn more if it is right for you.

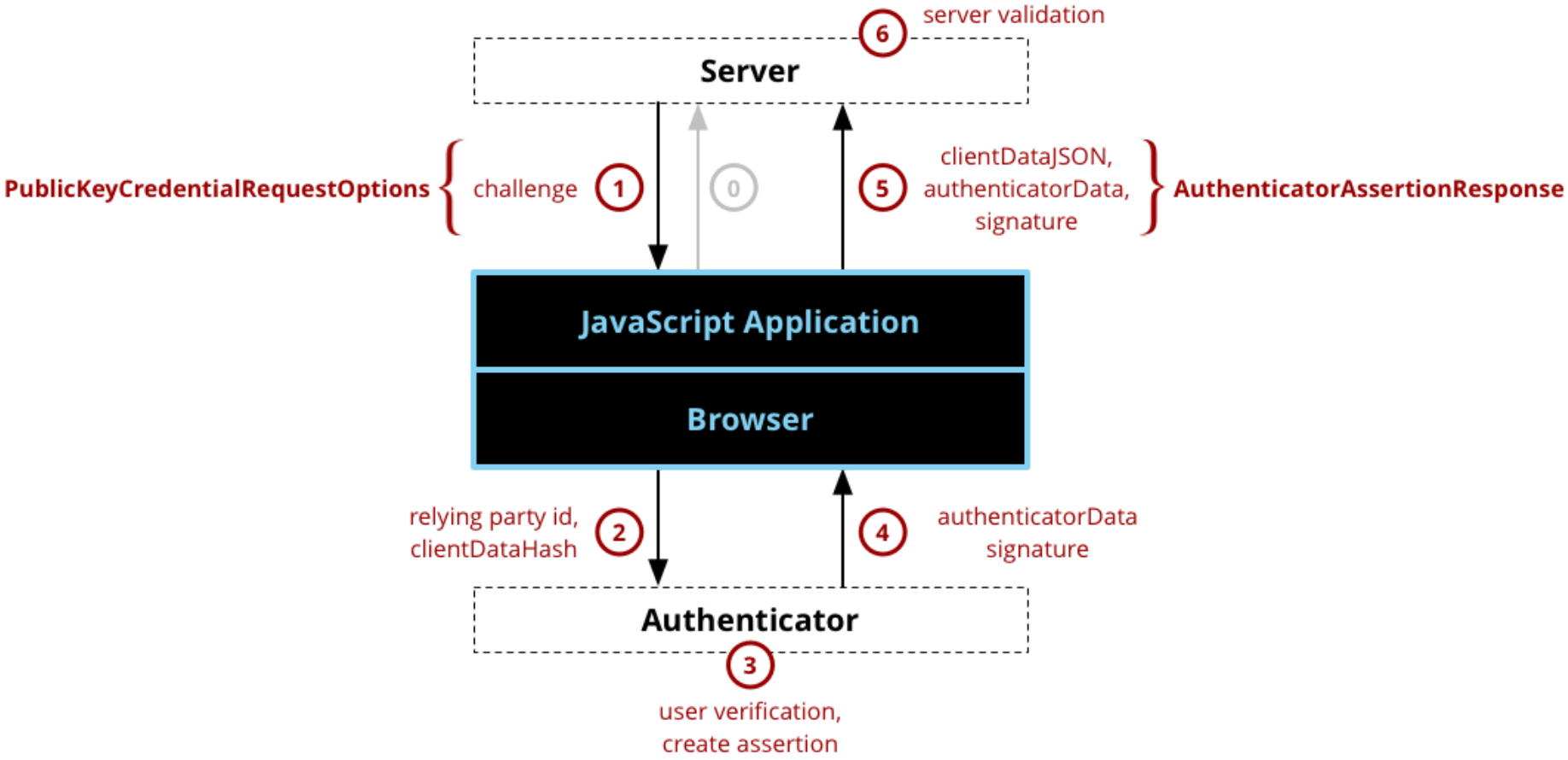
Two-step verification
OFF
Turn on

Passwordless account
OFF
Turn on

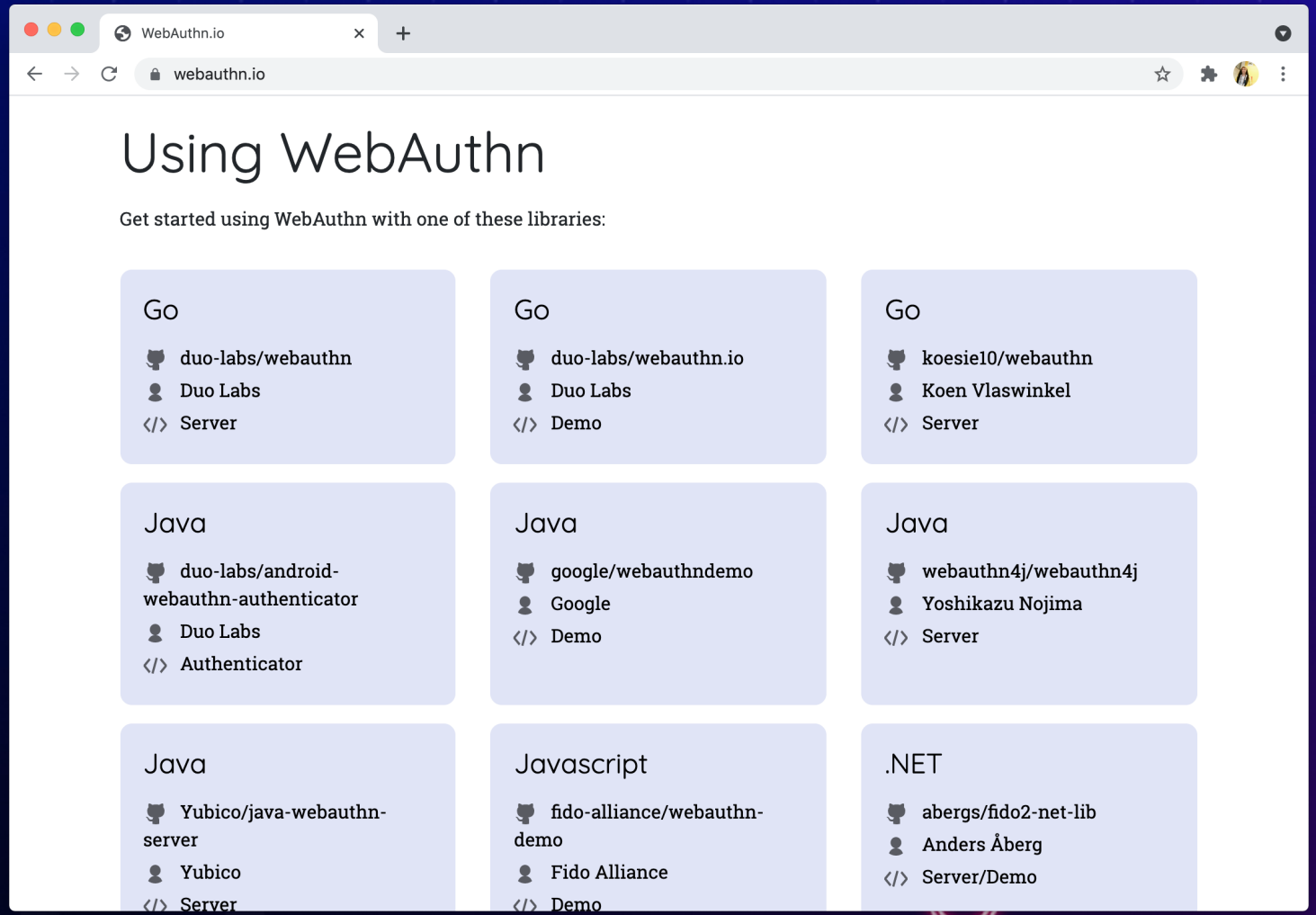
Доступные методы

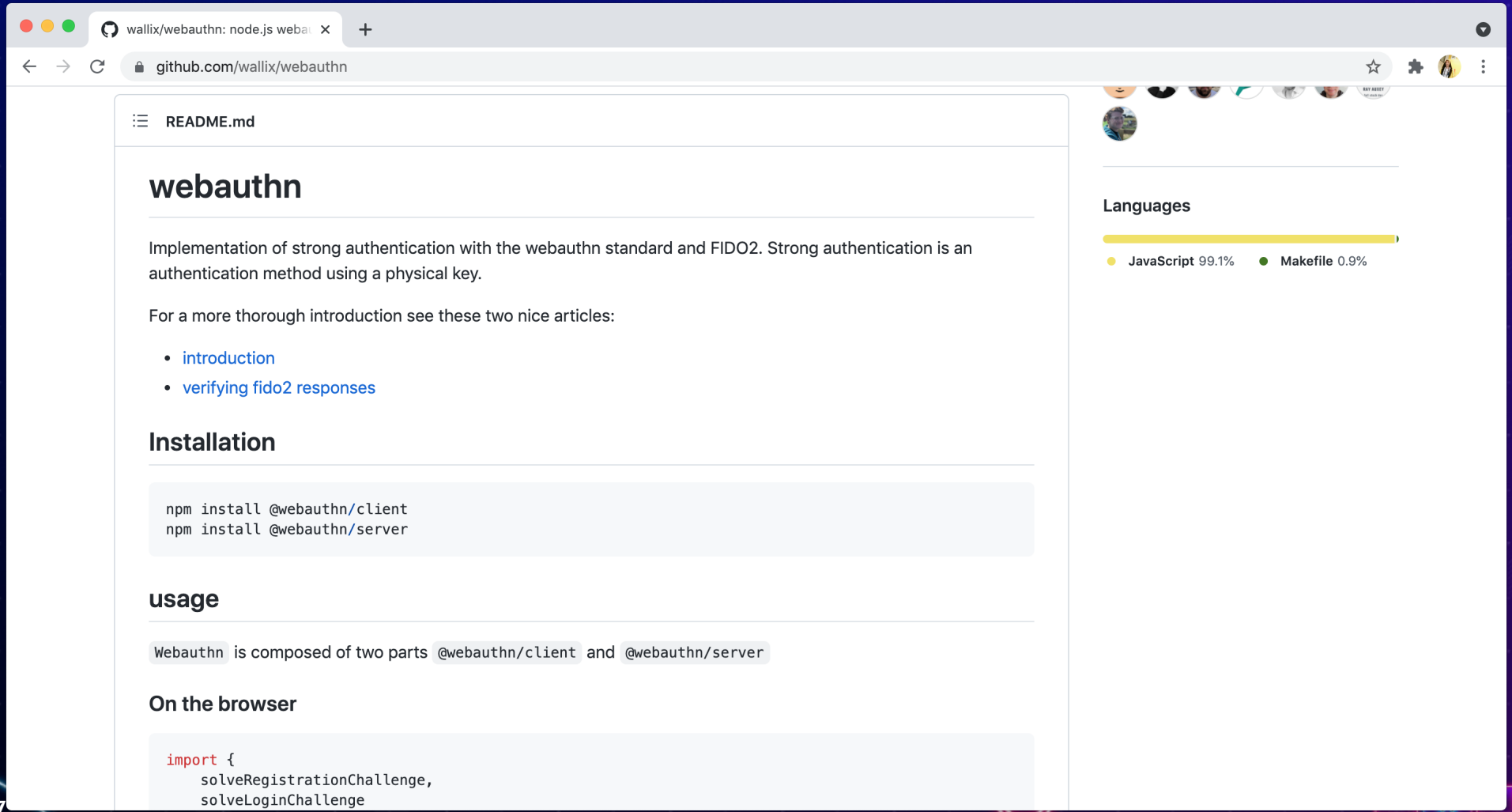
```
01. navigator.credentials.create()
02. navigator.credentials.get()
```


Server
6
server validation
PublicKeyCredentialCreationOptions
challenge,
user info,
relying party info
1
0
5
clientData,
attestationObject
AuthenticatorAttestationResponse
JavaScript Application
Browser
relying party id,
user info,
relying party info,
clientDataHash
2
4
new public key,
credential id,
attestation
attestationObject
Authenticator
3
user verification,
new keypair,
attestation


6
server validation
Server
PublicKeyCredentialRequestOptions
challenge
1
0
5
clientDataJSON,
authenticatorData,
signature
AuthenticatorAssertionResponse
JavaScript Application
Browser
relying party id,
clientDataHash
2
4
authenticatorData
signature
Authenticator
3
user verification,
create assertion

Демо


WebAuthn.io
webauthn.io
Using WebAuthn
Get started using WebAuthn with one of these libraries:
Go
duo-labs/webauthn
Duo Labs
Server
Go
duo-labs/webauthn.io
Duo Labs
Demo
Go
koesie10/webauthn
Koen Vlaswinkel
Server
Java
duo-labs/android-webauthn-authenticator
Duo Labs
Authenticator
Java
google/webauthndemo
Google
Demo
Java
webauthn4j/webauthn4j
Yoshikazu Nojima
Server
Java
Yubico/java-webauthn-server
Yubico
Server
Javascript
fido-alliance/webauthn-demo
Fido Alliance
Demo
.NET
abergs/fido2-net-lib
Anders Åberg
Server/Demo


wallix/webauthn: node.js weba
github.com/wallix/webauthn
README.md
webauthn
Implementation of strong authentication with the webauthn standard and FIDO2. Strong authentication is an authentication method using a physical key.
For a more thorough introduction see these two nice articles:
introduction
verifying fido2 responses
Installation
npm install @webauthn/client
npm install @webauthn/server
usage
Webauthn is composed of two parts @webauthn/client and @webauthn/server
On the browser
import {
solveRegistrationChallenge,
solveLoginChallenge
Languages
JavaScript 99.1%
Makefile 0.9%

Что дальше

Заботьтесь о пользователях

👏 Спасибо!

- 👨 Алексей Авдеев
- 🌐 https://github.com/avdeev
- 🌐 https://twitter.com/avdeev_alexey
- 🌐 Mish.Design