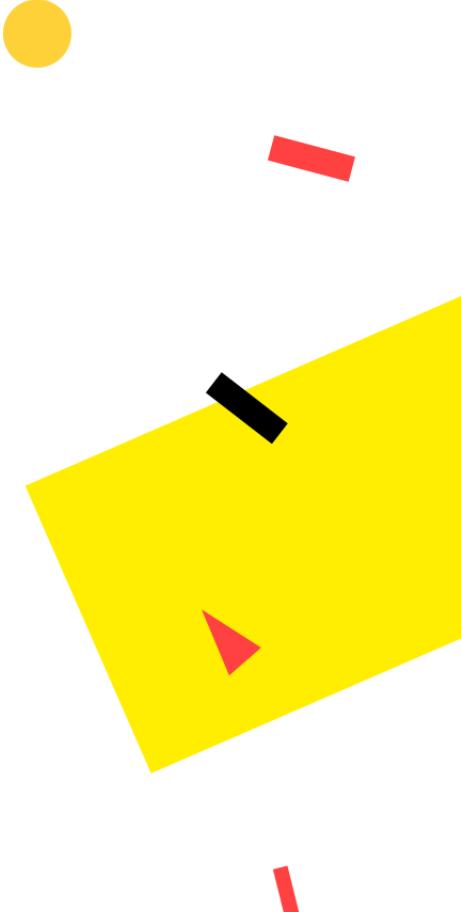


Используем USB-токены для аутентификации в браузере

Алексей Авдеев, Mish.Design





0 себе

1. 🧑 Алексей Авдеев (https://twitter.com/avdeev_alexey)
2. 💼 СТО, руковожу разработкой
3. 🏙 Из Нижнего Новгорода, работаю в Москве
4. 🌐 [Mish.Design](#)
5. 🤖 Программирую с 2002 года

↑↓ Вы ретвитнули



sadcore bitch
@ohkatewow

...

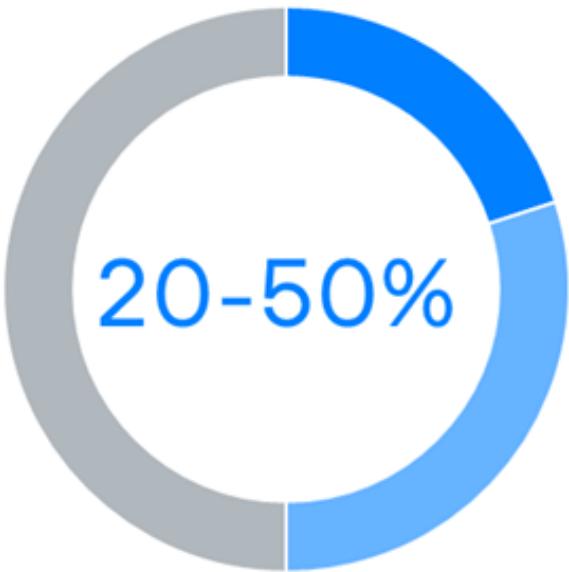
волки бэкендеров делают auth

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

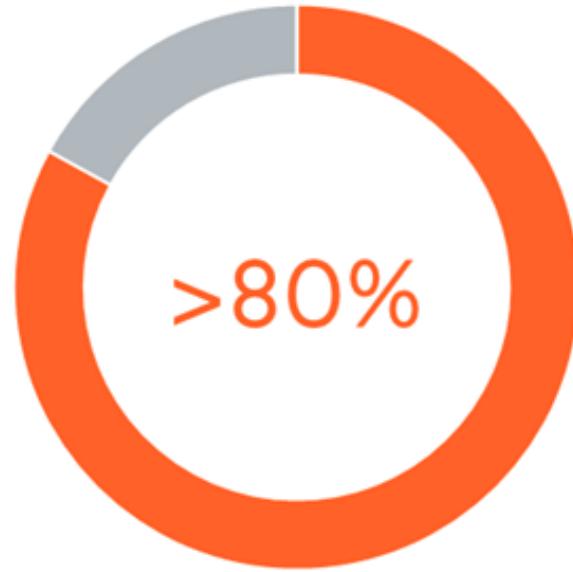
7

nomios / infradata



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

secure and connected

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 you've been pwned

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

12

FC Frontend Conf 2021



Сбер

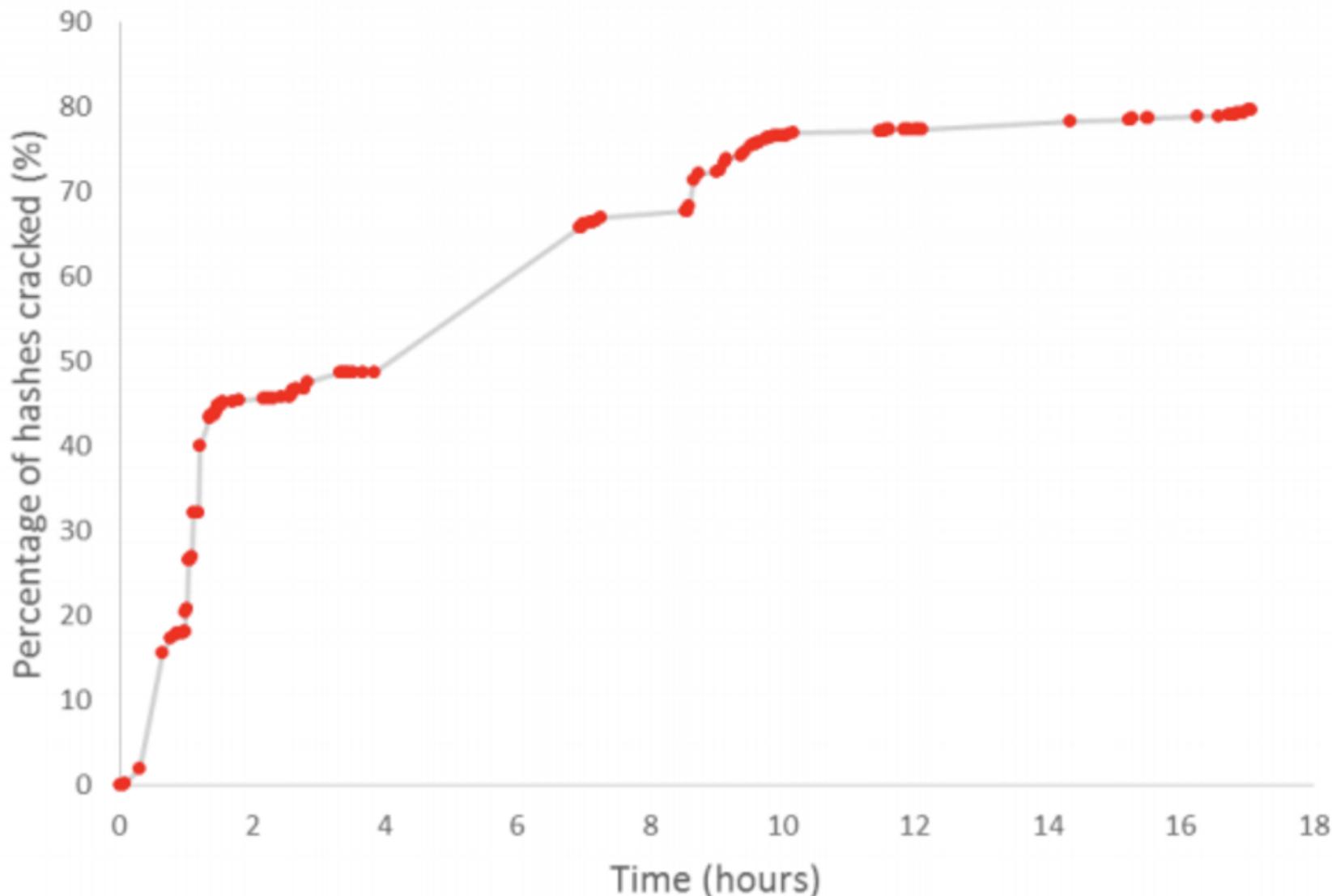
@sberbank

...

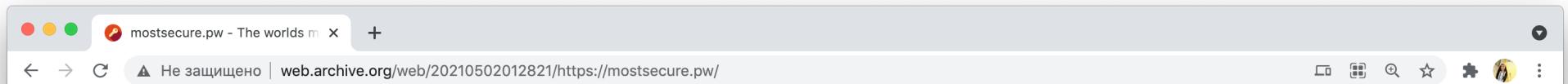
В ответ @a_okshus

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



Много паролей



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



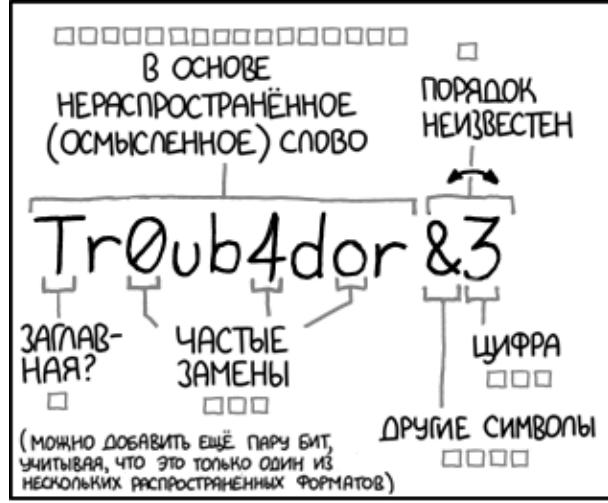
Features

- 🔒 Upper- and Lowercase Characters
 - 🔒 Numbers
 - 🔒 Ambiguous Characters

ISO 27001 compliant

Our research- as well as our support center is ISO/IEC 27001 certified to ensure 100% information security.

Парольные фразы



~28 БИТ ЭНТРОПИИ

$2^{28} = 3$ ДНЯ ПРИ 1000 ПОПЫТОК/СЕК

(ПРАВДОПОДОБНАЯ АТАКА НА СЛЯВЫЙ ЧДАЛЕННЫЙ 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 КУЛЁМ?

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 ЧУЖЕ 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

(c) Билл Гейтс, 2004

Многофакторная автентификация (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):saramorrison...

575 362

Google (home)

915 708

Add token

Do you want to add the token named
"iamsaramorrison"?

No

Yes

Discord (s)

094 664

Robinhood

689 030

Chorus (sara.morrison)

Google Authenticator

Instagram (iamsaramorrison)

032 511

Slack (Suburbia Roller Derby):saramorrison...

115 639

Google (home)

712 988

Facebook

158 185

Amazon (home)

540 809

Discord (s)

796 919

Robinhood

Confirmation Code

Enter Code

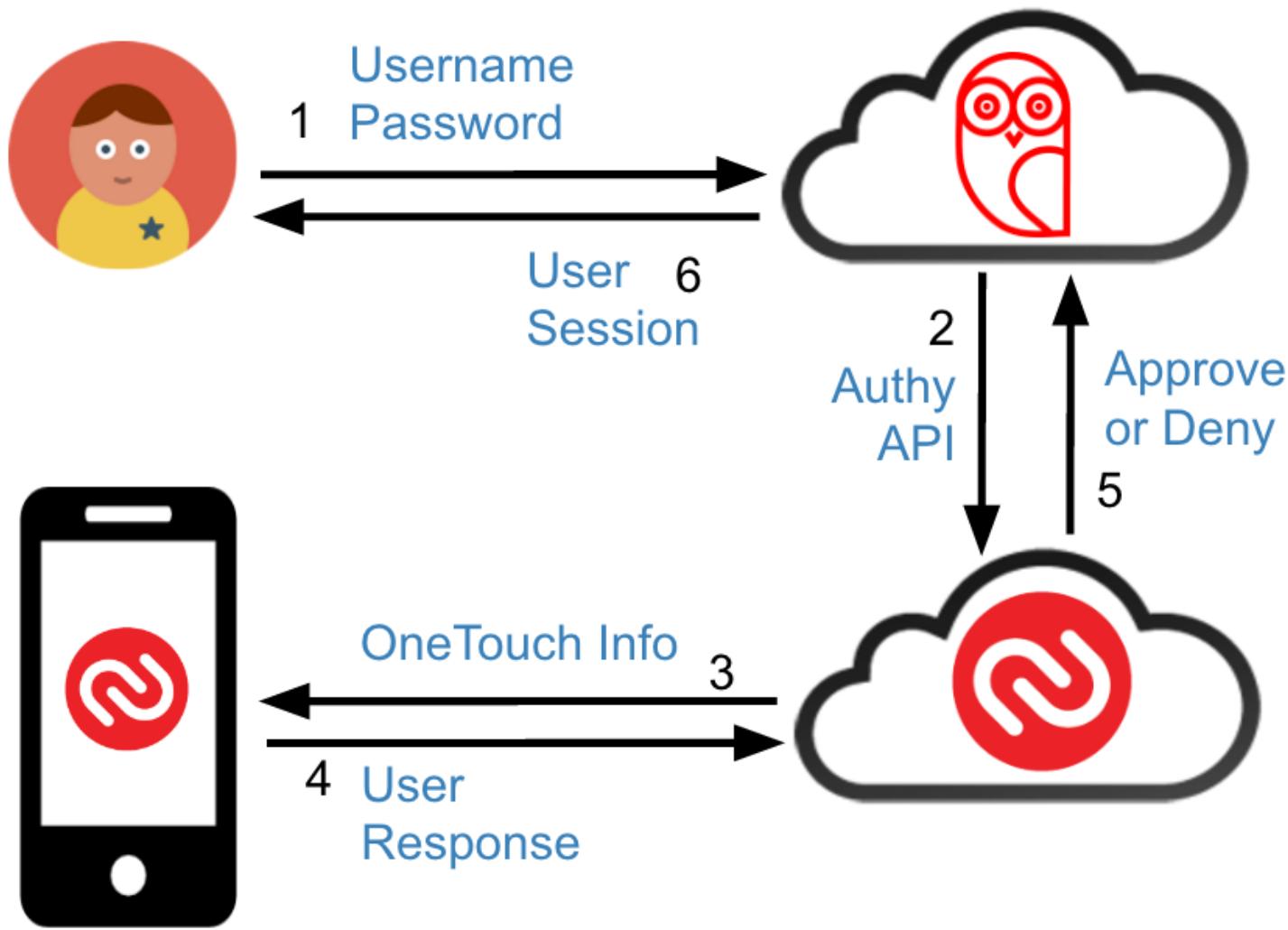
Enter the 6-digit code generated by Google
Authenticator.

0 3 2 5 1 1

Next

1	2	3
A B C	D E F	G H I
4	5	6
G H I	J K L	M N O
7	8	9
P Q R S	T U V	W X Y Z
0		X

extend
F 2021



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

www.ac-mail.ru/gmailblock/index.php?email=

[Ticket#5-400000000118] Прекращение предоставления услуг

Администрация Gmail support.service@gmail.ru via unde
to me Nov 17 (3 days ago)

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.

Оспорить заявление Вы можете пройдя по ссылке и авторизовавшись на сервере:

[Оспорить 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
3fail=1&id=1522F%263316%112222&126%F256%86&session=56F56%52D%3125

Токен



Стандарты и сертификаты

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

Токены без подключения





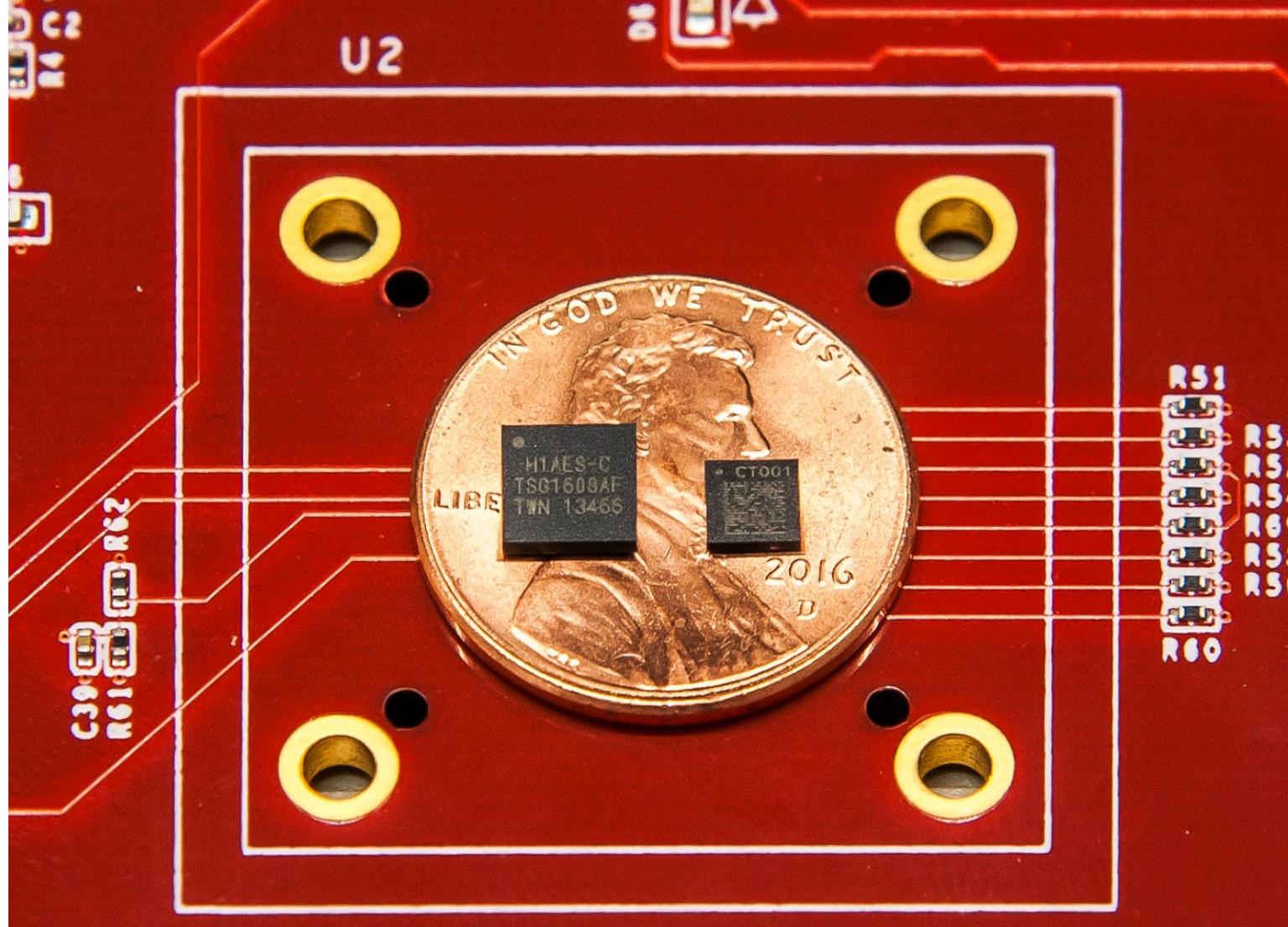
Беспроводные токены

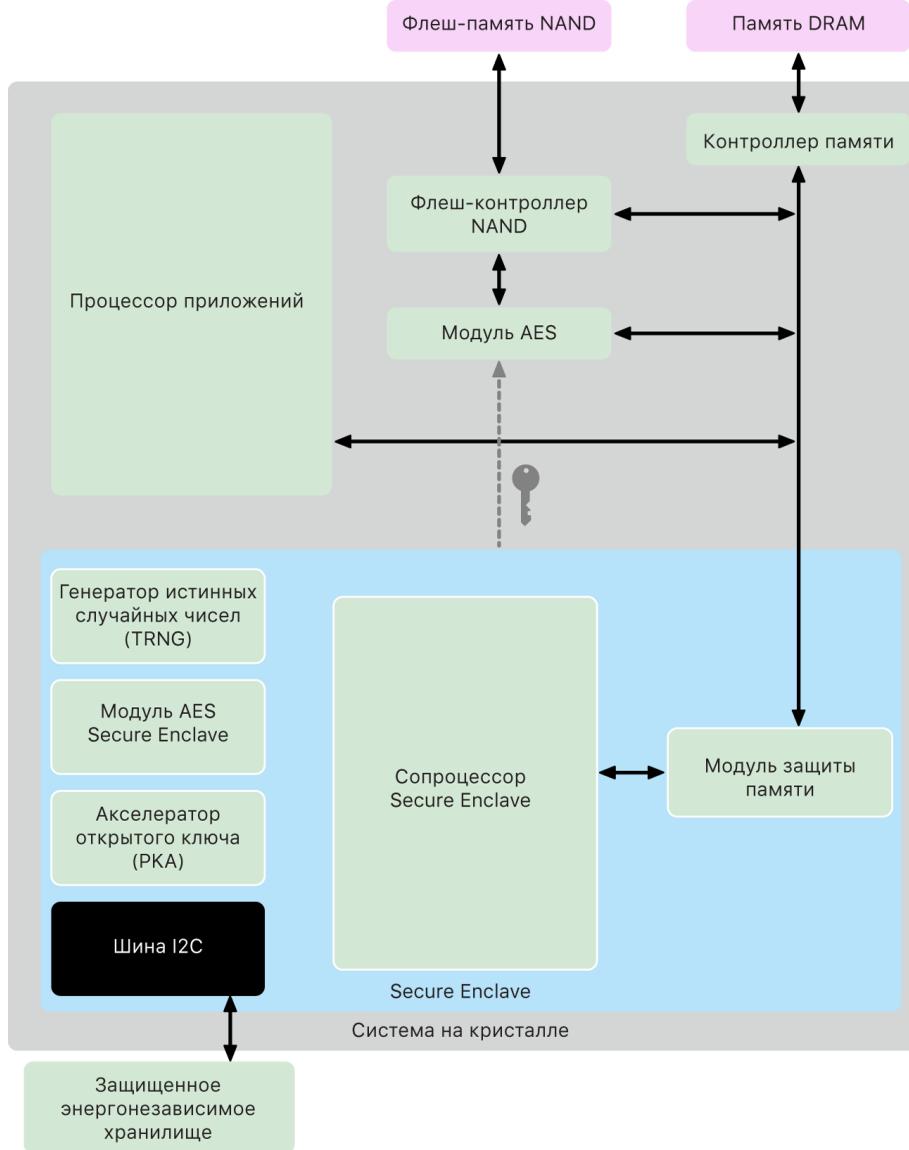


Токены с подключением



Встроенная криптография





Модель зрелости надежности автентификации

THE CONSUMER AUTHENTICATION STRENGTH MATURITY MODEL (CASMM) v5



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:

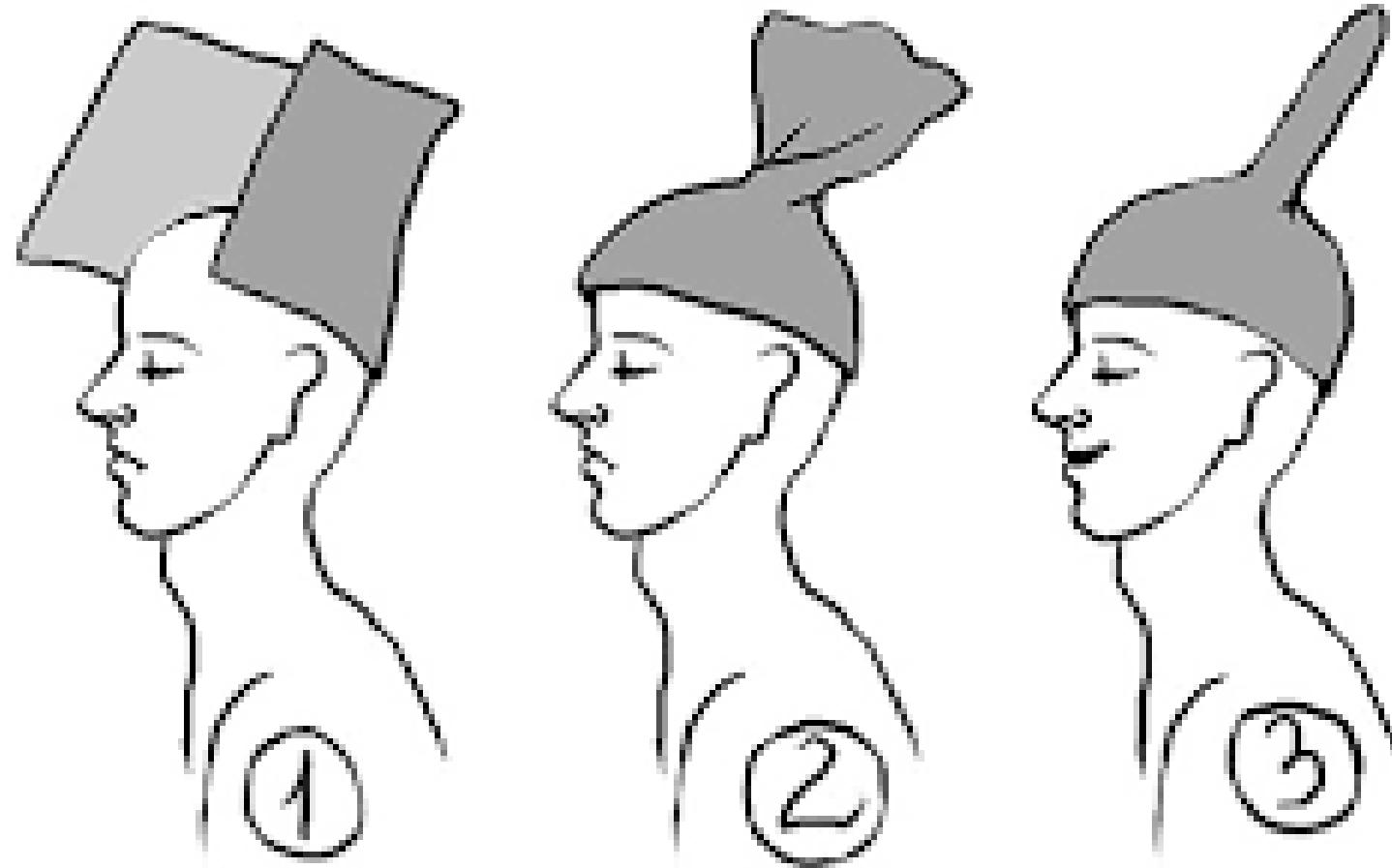
НА ЕГО НОУТЕ ВСЁ ЗАШИФРОВАНО.
ДАЙ ЕМУ НАРКОТЫ И ДУБАСЬ
ЭТИМ ГАЕЧНЫМ КЛЮЧОМ
ЗА 5 БАКСОВ, ПОКА ОН
НЕ СКАЖЕТ ПАРОЛЬ.

ПОНЯЛ.



Правила компьютерной безопасности

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



Fast IDentity Online (FIDO)



simpler
stronger
authentication



QUALCOMM



Lenovo



Synaptics



aetna



Bank of America



Microsoft

dedicated to changing the way online authentication is done.

docomo



RAON
SECURE

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

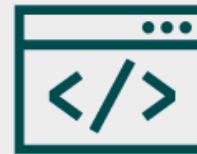
L1



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



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

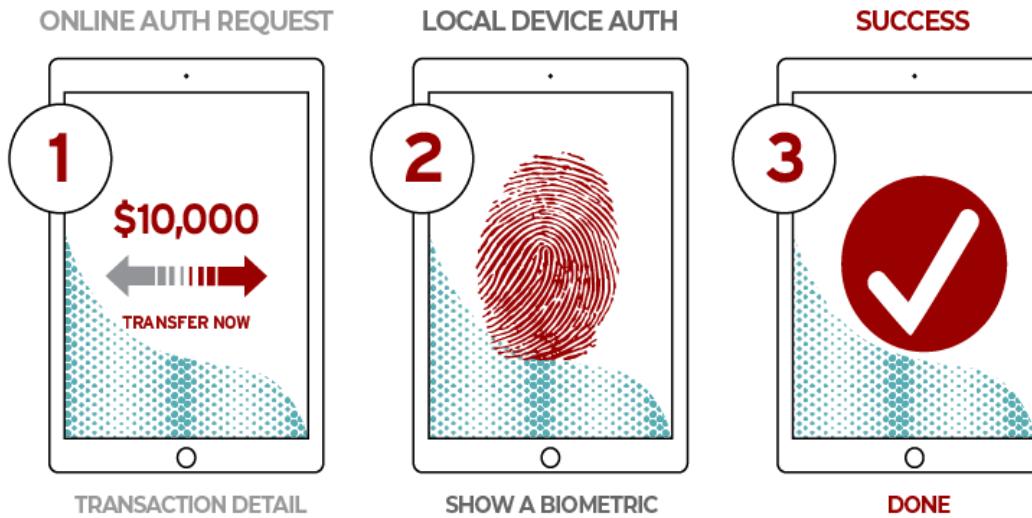


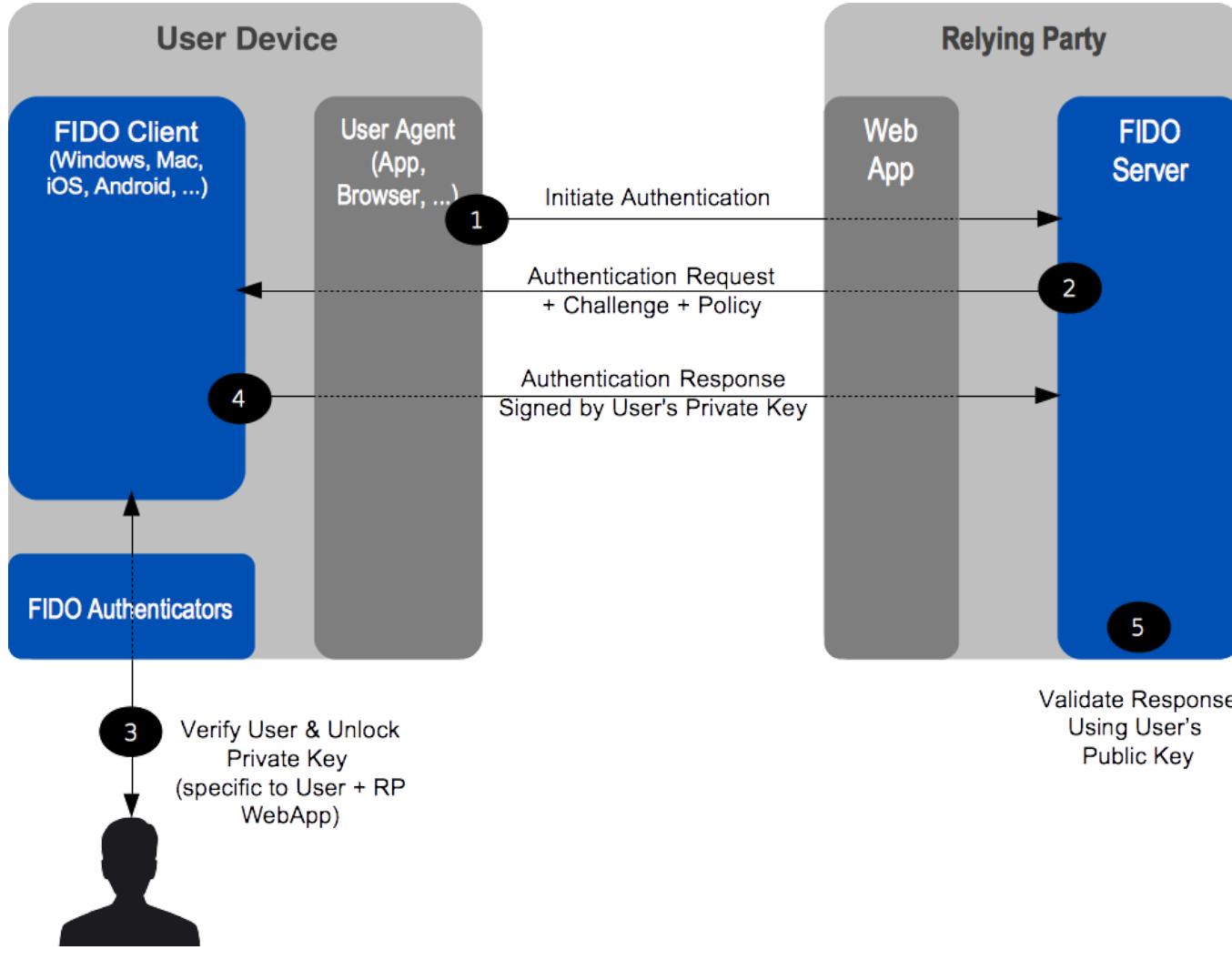
FIDO2 built into a downloadable web browser app
Certification: L1

Universal Authentication

**Framework
(UAF, 2014)**

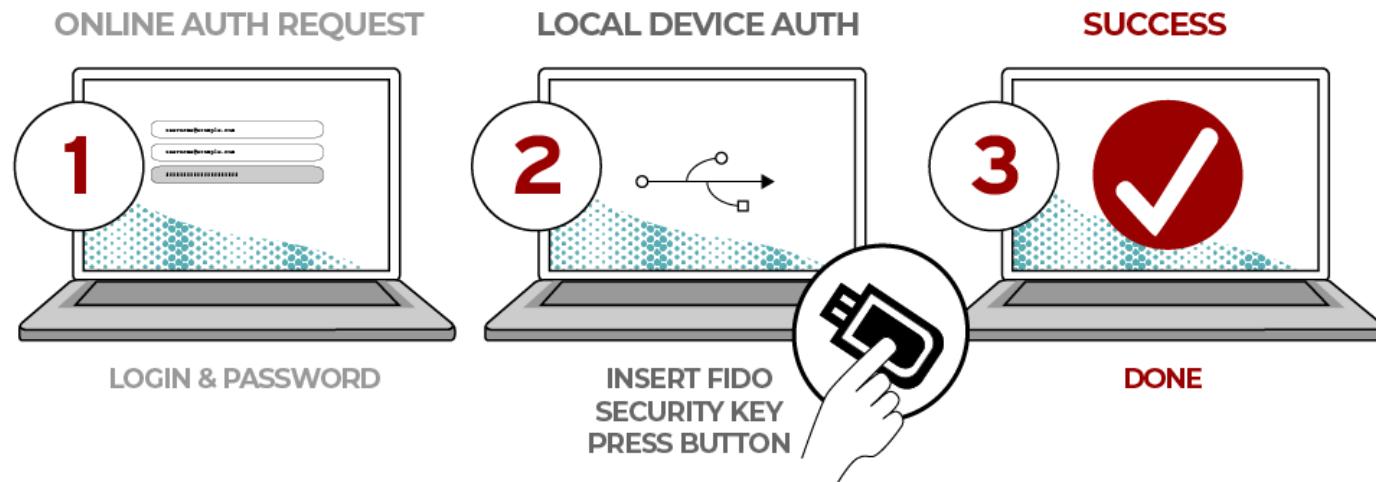
PASSWORDLESS EXPERIENCE (UAF standards)



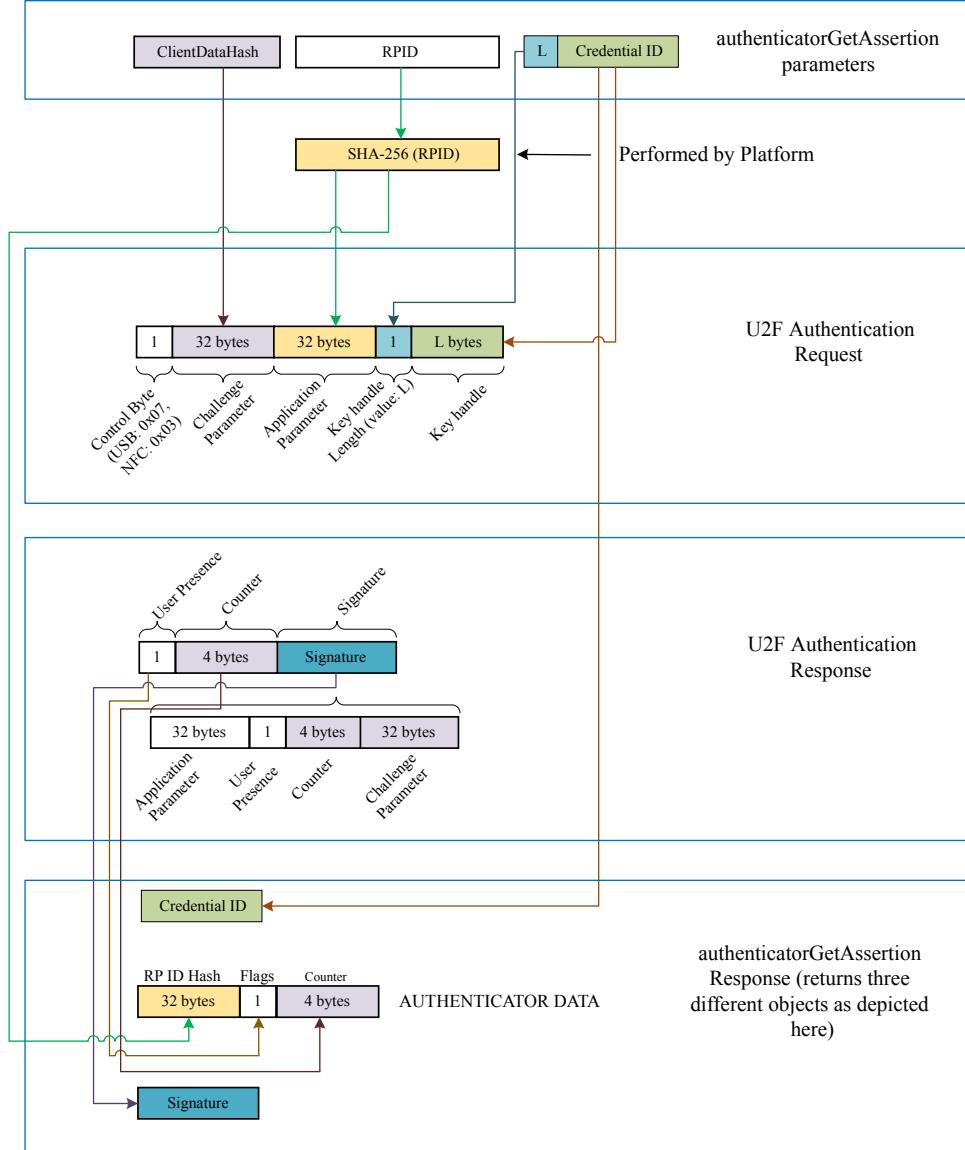


Universal 2nd Factor (U2F)

SECOND FACTOR EXPERIENCE (U2F standards)



Client to Authenticator Protocol (CTAP)



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

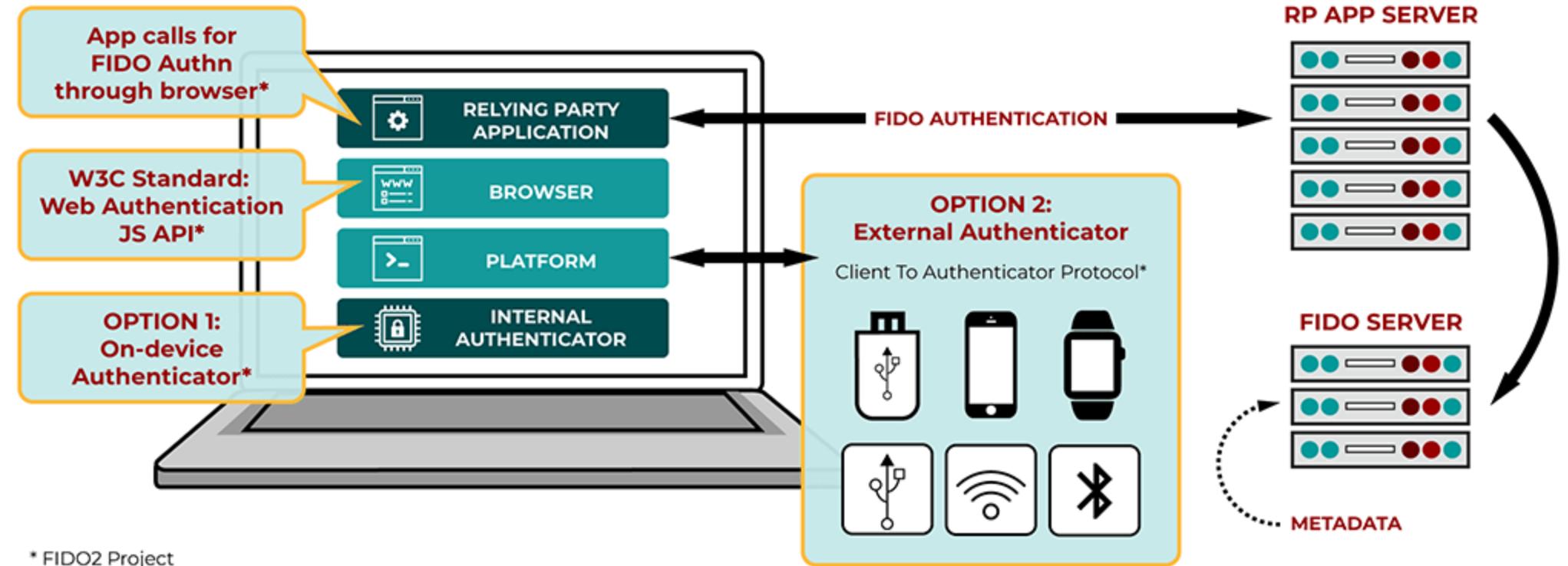
Browser

backwards
compatibility

CTAP2
(CBOR)

U2F = CTAP1
(RawMessage)

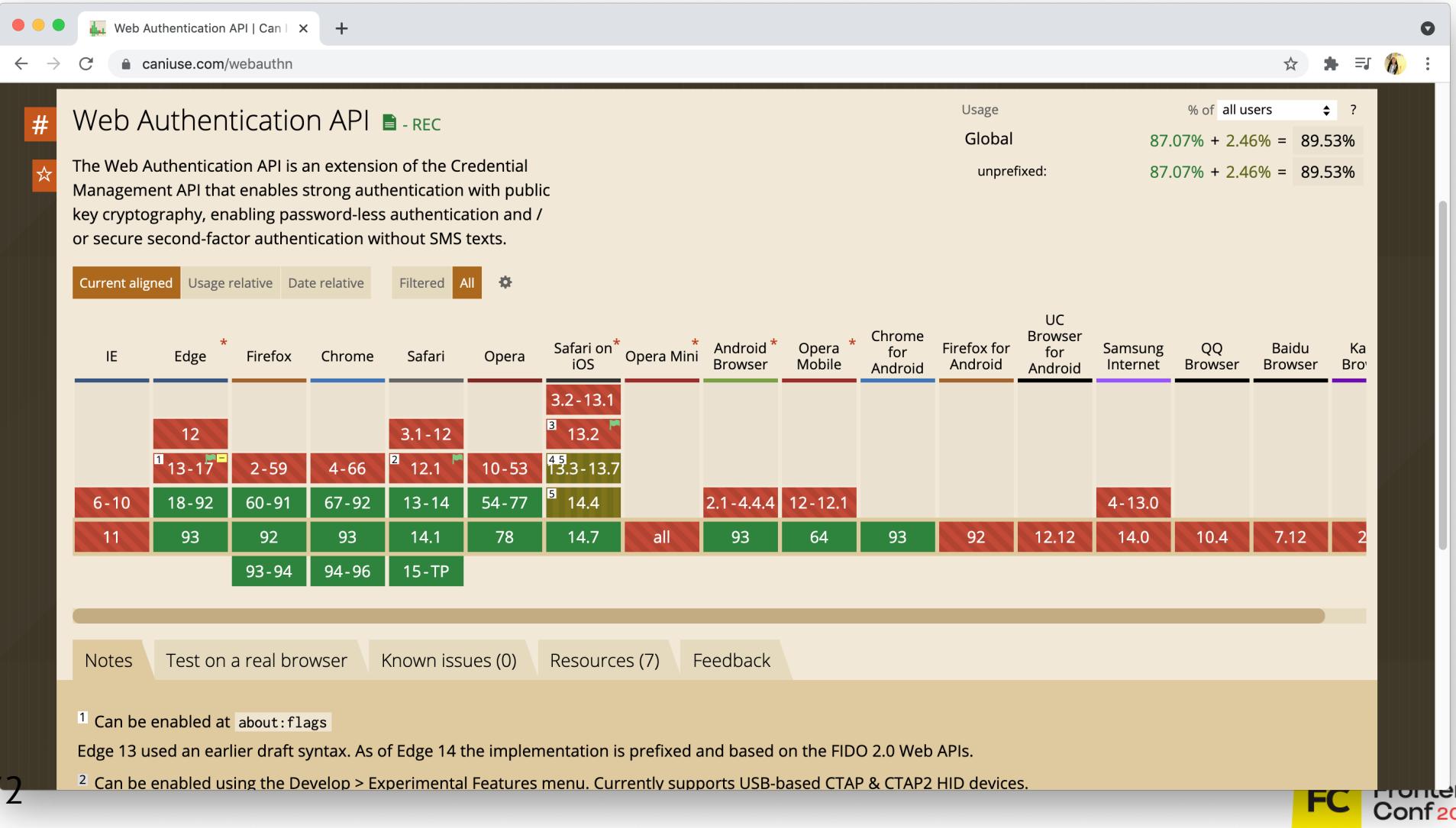
Client to authenticator
protocol
(CTAP) layer
NFC/USB/HID

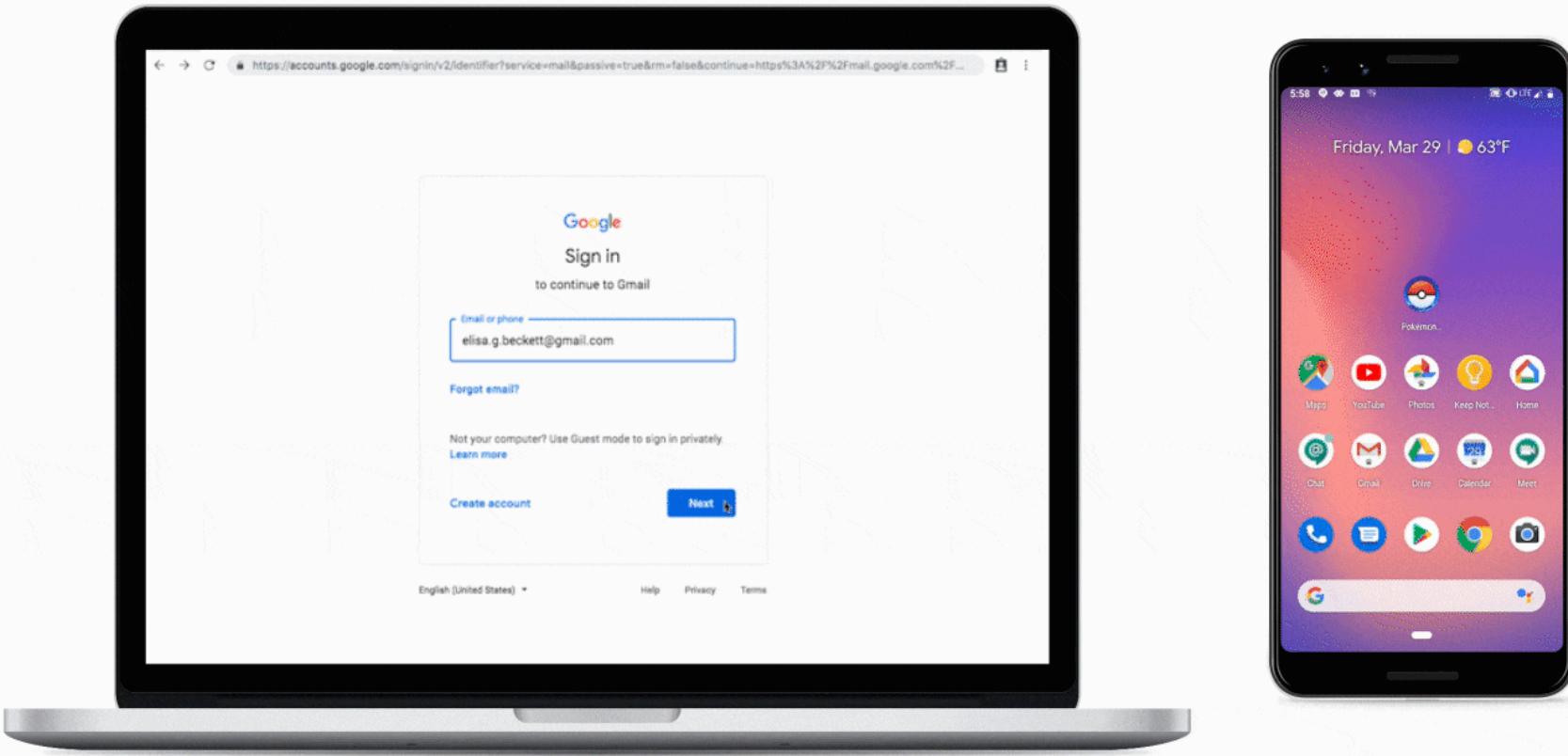


* FIDO2 Project

Passwordless = CTAP2 & WebAuthn







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

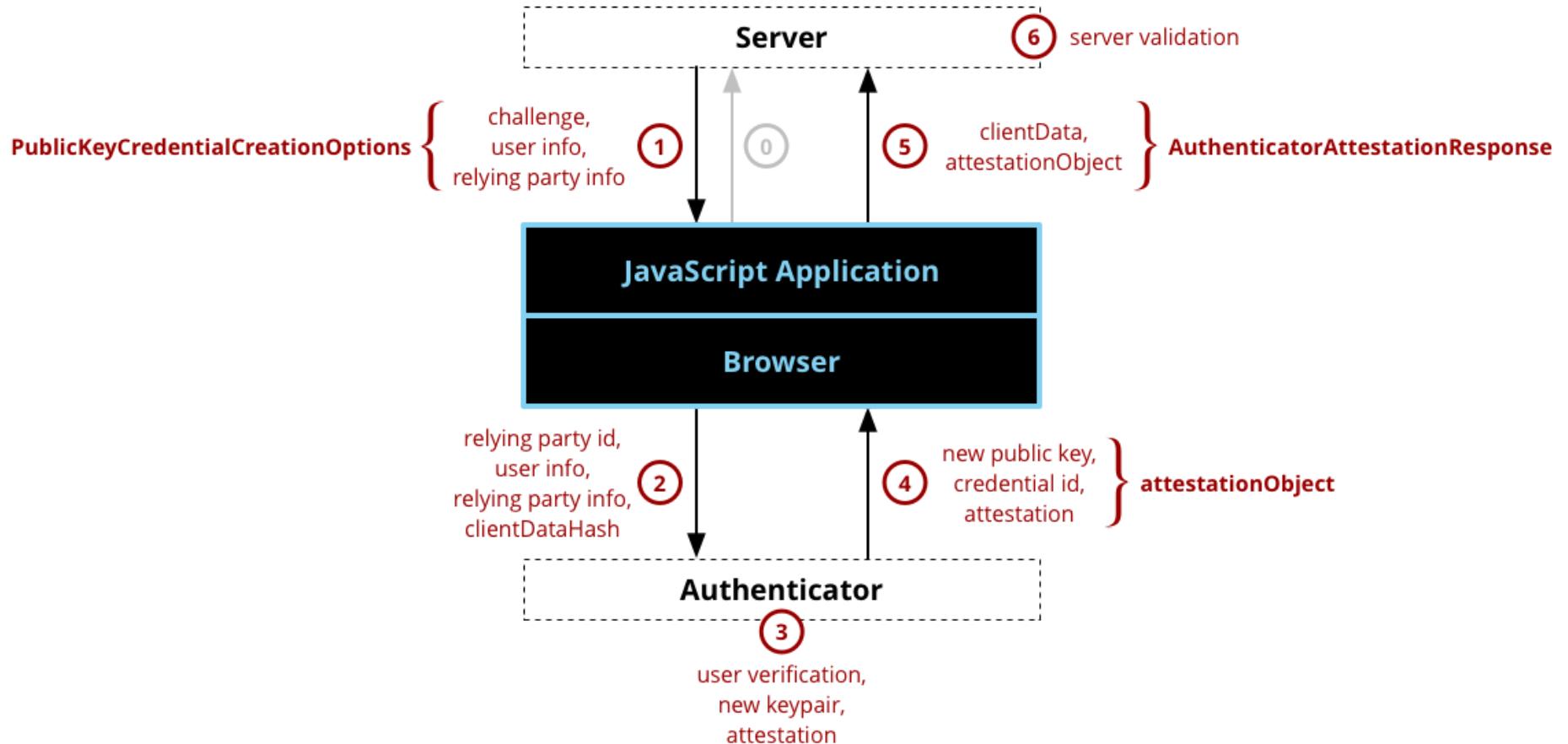
OFF

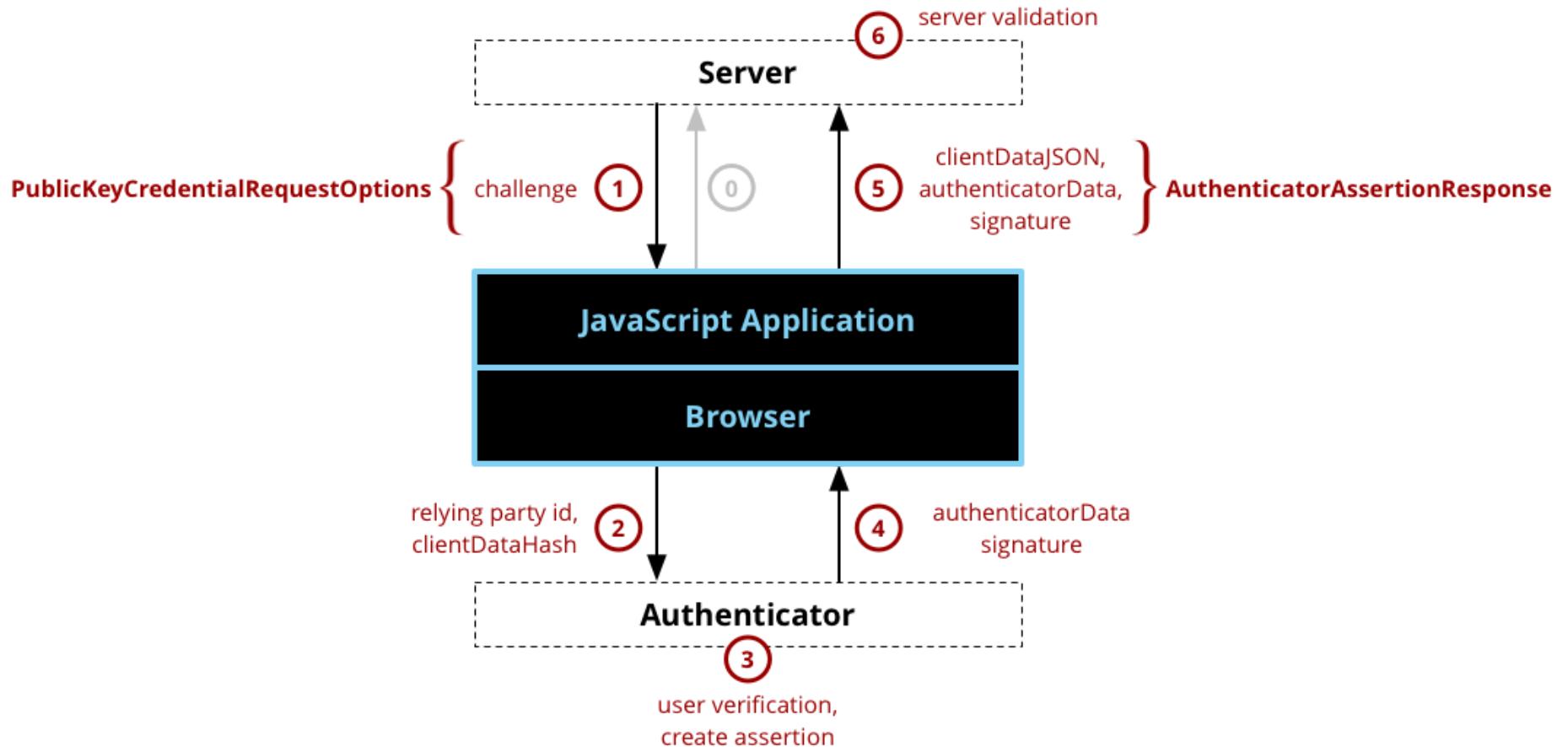
[Turn on](#)

Доступные методы

01. navigator.credentials.create()

02. navigator.credentials.get()





демо

The screenshot shows a web browser window with the URL `webauthn.io`. The page title is "Using WebAuthn". Below the title, a sub-header says "Get started using WebAuthn with one of these libraries:". The page displays nine cards arranged in a 3x3 grid, each representing a different library:

- 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 webauthn

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
- 🌐 github.com/avdeev
- 🌐 twitter.com/avdeev_alexey
- 🌐 alexey-avdeev.com/usb-tokens
- 🌐 Mish.Design

