



DATAWAY
SECURITY

Аппаратный ключ аутентификации в облачных средах

Как получить пароль пользователя?

Фишинг - наиболее популярная атака на получения персональных данных пользователей

Фишинговые атаки выросли по сравнению 2018 годом на 40,9%

84% атак было направленно на получения учетных данных пользователей для финансовых, почтовых, облачных, платежных и SaaS-сервисов

98% атак прошли безопасность электронной почты организации и попали во входящие сообщения пользователя, не содержали вредоносного ПО

В основном атаки были направлены на финансы, отделы HR и электронную коммерцию

Отчет PhishLabs 2019 г.



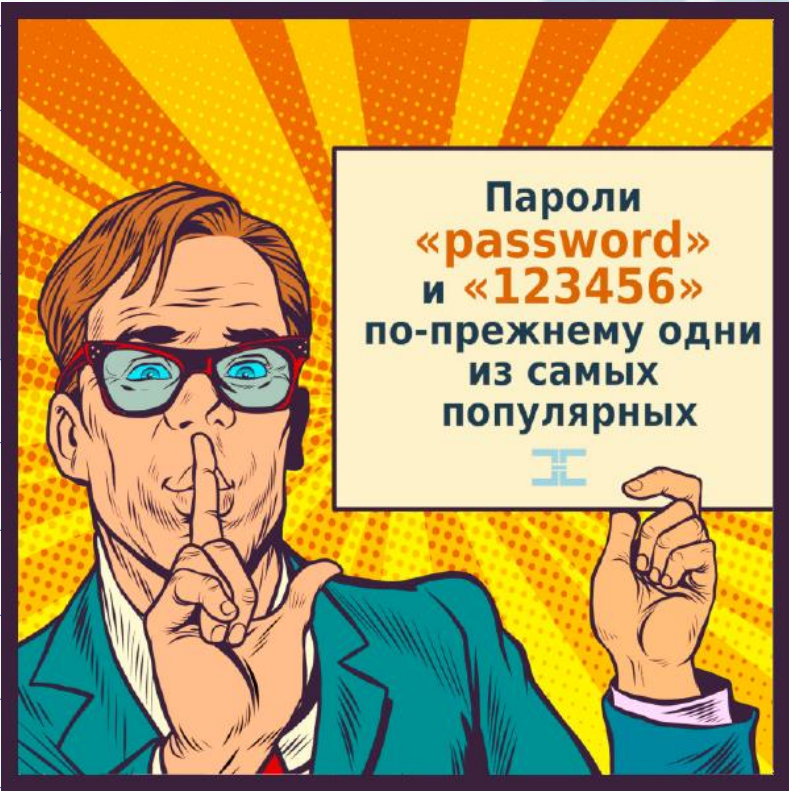
Специалисты Google – назвали фишинг самым опасным видом атак

Как получить пароль пользователя?

Brute Force паролей и взлом сайтов с пользовательскими паролями, шпионские программы

ТОП-10 Худших паролей 2019 г.

Пароль	Частота использования
12345	2 812 220
123456	2 485 216
1234567898	1 052 268
test1	993 756
password	830 846
12345678	512 560
zinch	483 443
g_czechout	372 278
asdf	359 920
qwerty	348 762



Пароль	password
Хэш пароля, вычисленный по различным алгоритмам	
Adler32	0f910374
CRC32	35c246d5
Haval	2221b19499669a2da53c49caf3c5e5be
MD2	f03881a88c6e39135f0ecc60efd609b9
MD4	8a9d093f14f8701df17732b2bb182c74
MD5	5f4dcc3b5aa765d61d8327deb882cf99
RipeMD128	c9c6d316d6dc4d952a789fd4b8858ed7
RipeMD160	2c08e8f5884750a7b99f6f2f342fc638db25ff31
SHA-1	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
SHA-256	5e884898da28047151d0e56f8dc6292773603d0d6aabbdd6
SHA-384	a8b64babd0aca91a59bdbb7761b421d4f2bb38280d3a75ba
SHA-512	b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b3
Tiger	d476a6b8b5c35ce912781497d02d09faeb8aa05a489223f5
Whirlpool	5b59c49b6dc8bcb2a554a64c42e859c6d43c5fbfe9adc41d6f

Знакомые методы 2FA

1. OATH аутентификация



- Подвержена фишинг атакам
- Чувствительны в времени синхронизации TOTP
- Токены имеют ограниченный жизненный цикл
- **Поддержка ограниченного кол-ва web-приложений**

2. SMS аутентификация



- Подвержены атакам подмены SIM карты
- **Серьёзная уязвимость протокола SS7, ОКС-7!!**

3. PKI аутентификация



- Проблемная интеграция
- Зависимость от центра сертификаций и центра регистраций
- Ограниченный жизненный цикл сертификата
- **Установка дополнительного ПО и драйверов**

FIDO – Протоколы и стандарты

FIDO – Fast iDentity Online (на основе открытого исходного кода)

FIDO Alliance – разработка и стандартизация открытых стандартов для аутентификации

UAF – Universal Authentication Framework. Стандарт FIDO для беспарольной аутентификации

U2F – Universal 2-Factor Authentication. Стандарт FIDO для двухфакторной аутентификации (CTAP1)

FIDO2 – Новый стандарт FIDO для WEB аутентификации:

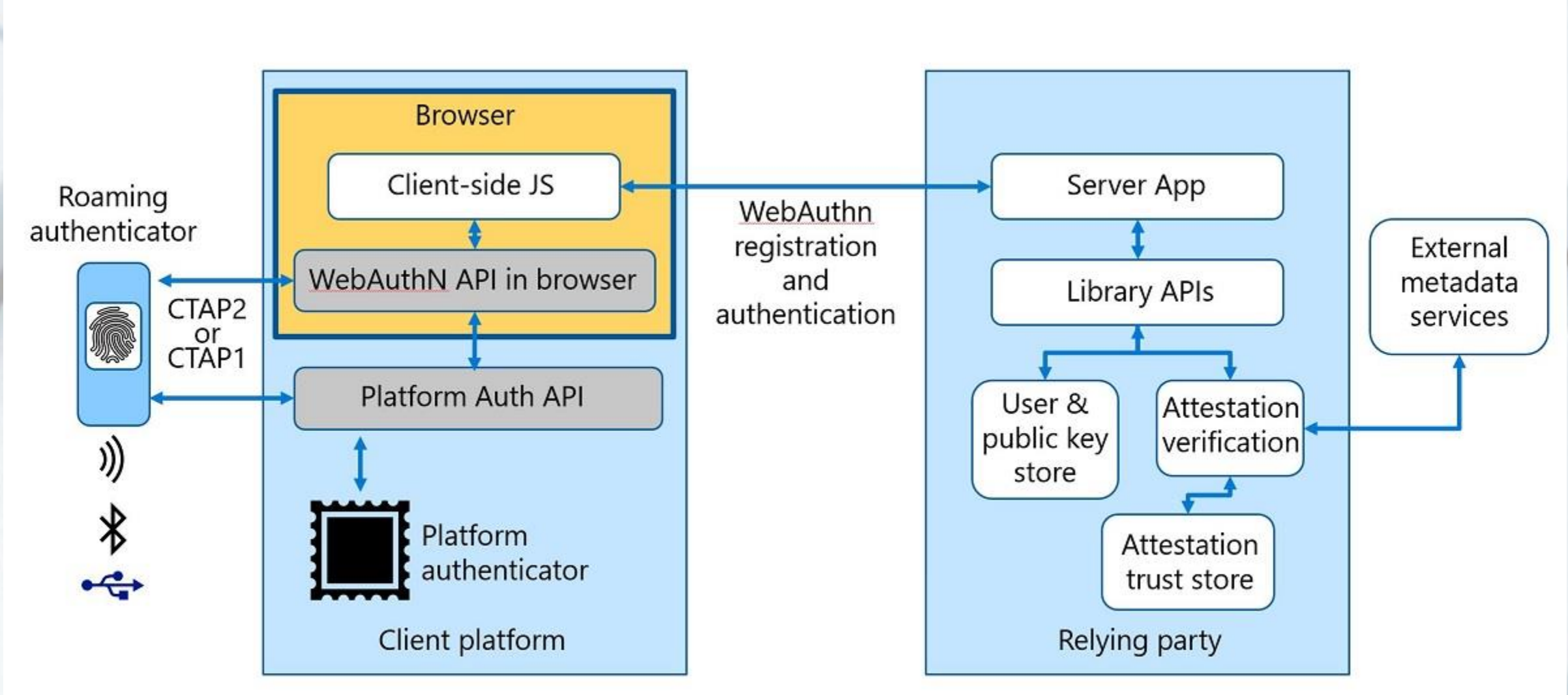
CTAP1 – FIDO Client-to-Authentication protocol v.1*

CTAP2 – FIDO Client-to-Authentication protocol v.2*

WebAuthn – JS API браузера, который описывает интерфейс для создания и управления учетными данными открытого ключа.

*CTAP – Набор протоколов низкого уровня для связи с аутентификаторами через BLE / NFC / USB

Как работает FIDO2



Браузеры и компании поддерживающий FIDO



Как выглядят ключи безопасности



Применение ключа безопасности в Google аккаунте

Google Аккаунт

Второй этап аутентификации позволяет подтвердить, что пароль ввели именно вы. Подробнее...

?

⋮

A



← Двухэтапная аутентификация

НОВИНКА! Добавьте встроенный электронный ключ



Добавить

Его можно использовать так же, как электронные ключи с технологией Bluetooth или USB.

Электронный ключ (по умолчанию) ?

 MYDIDOKEY102001597 (время добавления: 4 января, 14:43) 

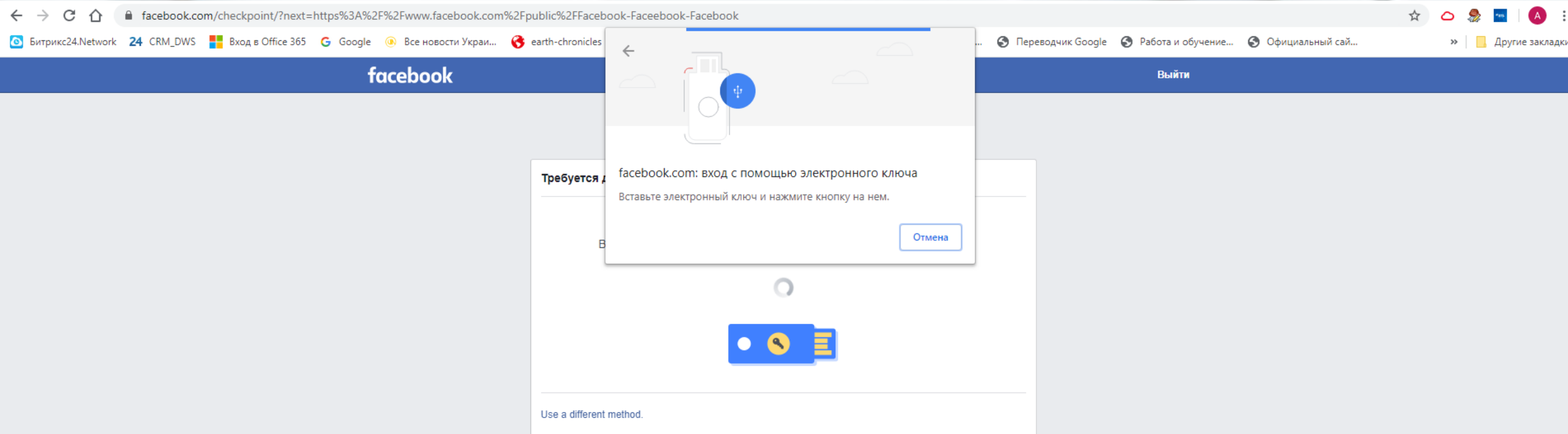
Дата последнего использования: 24 января, 20:18
Chrome для Windows

 FIDO_NFC (время добавления: 17 июня 2019 г.) 

Дата последнего использования: 2 декабря 2019 г.
SM-M307FN

ДОБАВИТЬ ЭЛЕКТРОННЫЙ КЛЮЧ

Применение ключа безопасности в Facebook



Применение ключа безопасности в Microsoft AZURE AD

The screenshot displays the Microsoft Azure portal interface for configuring an authentication method policy. The browser address bar shows the URL: `portal.azure.com/?l=en-us#blade/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/AdminAuthMethods`. The page title is "Authentication methods - Authentication method policy (Preview)".

On the left sidebar, under "Manage", the "Authentication method policy (...)" is selected, with "Password protection" as a sub-option.

The main content area shows a configuration page for FIDO2 Security Key. It includes a "Reset" button and a link to "Click here to enable users for the enhanced registration preview." Below this, a table lists the configured methods:

Method	Target	Enabled
FIDO2 Security Key	1 user	Yes
Microsoft Authenticator passwordless sign-in		No

Below the table, the "FIDO2 Security Key settings" section is expanded, showing three tabs: "ENABLE", "TARGET", and "GENERAL".

- ENABLE:** A toggle switch is set to "Yes". Under "USE FOR:", "Sign in" and "Strong authentication" are selected.
- TARGET:** A dropdown menu is set to "All users". Below it, a table lists the selected users:

Name	Type	Registration
Alexander Khomutov	User	Optional
Denis-Admin	User	Optional

- GENERAL:** Contains several settings:
 - "Allow self-service set up": Toggle set to "Yes".
 - "Enforce attestation": Toggle set to "Yes".
 - "KEY RESTRICTION POLICY": "Enforce key restrictions" toggle set to "No".
 - "Restrict specific keys": Toggle set to "Allow".
 - "Add AAGUID": A text input field.

Добавить ключ безопасности в личном аккаунте

Add a method

Which method would you like to add?

Security key

Cancel

Add

Security key

Choose the type of security key that you have.

USB device

NFC device

Cancel

Identity IT Pro

My Profile

?

Overview

Security info

Organizations

Devices

Privacy

Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification

Change

+ Add method

Phone

+1 1234567890

Change

Delete

Microsoft Authenticator


XX-XXXXX

Delete

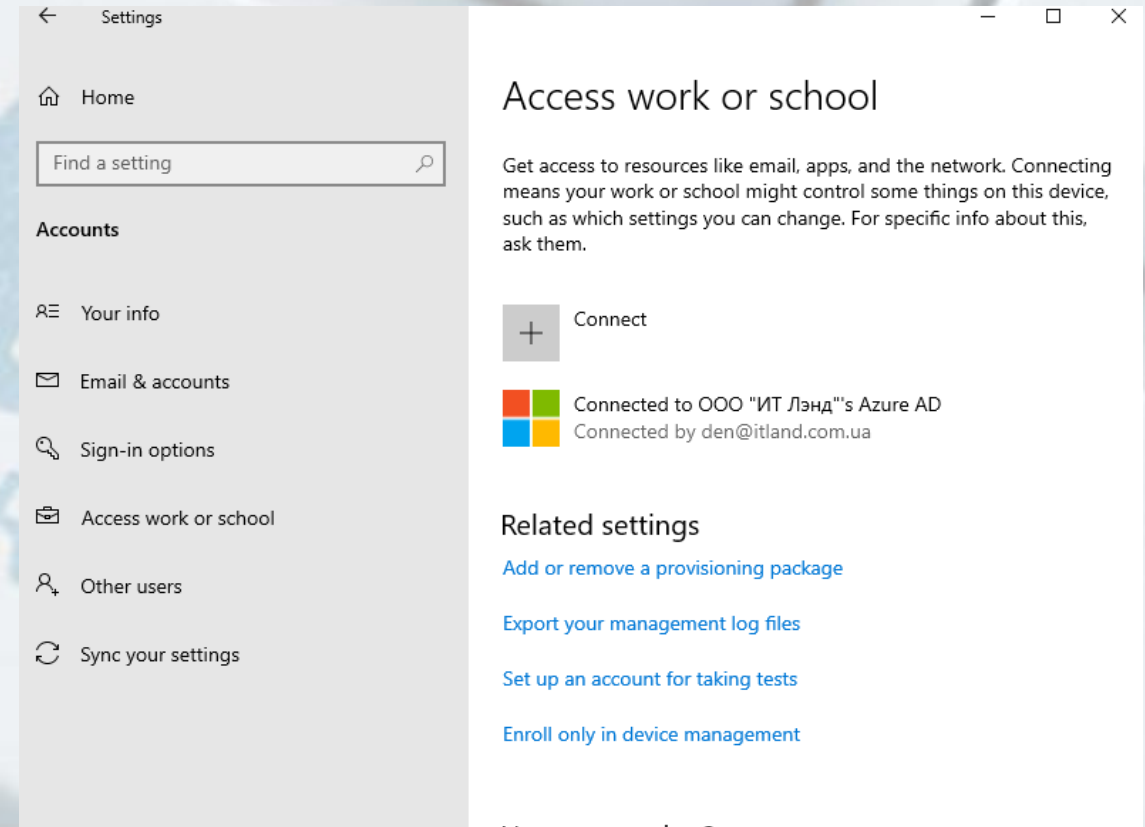
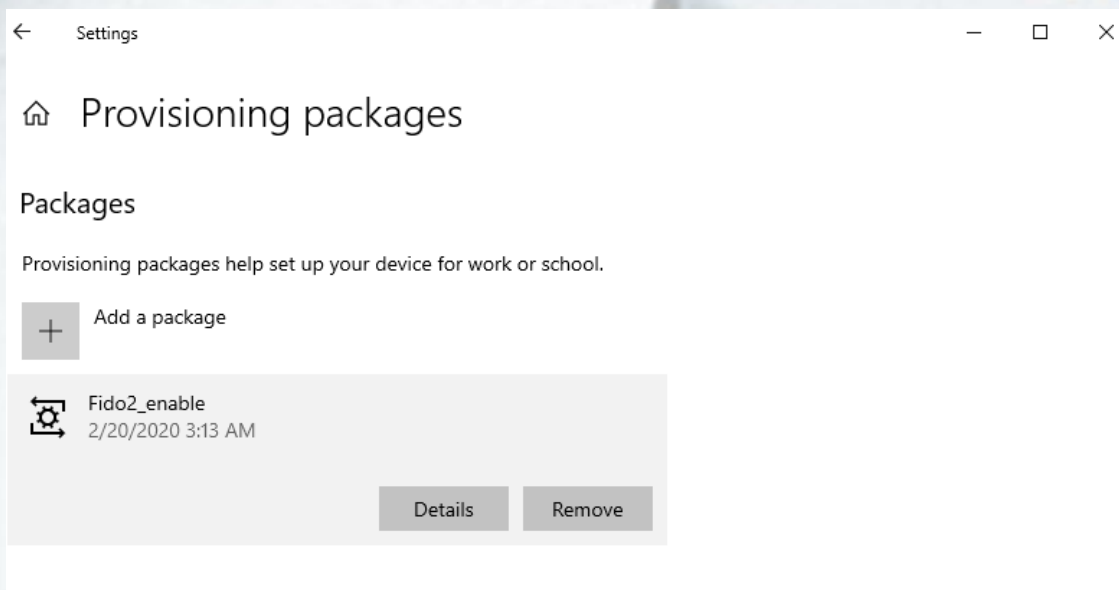
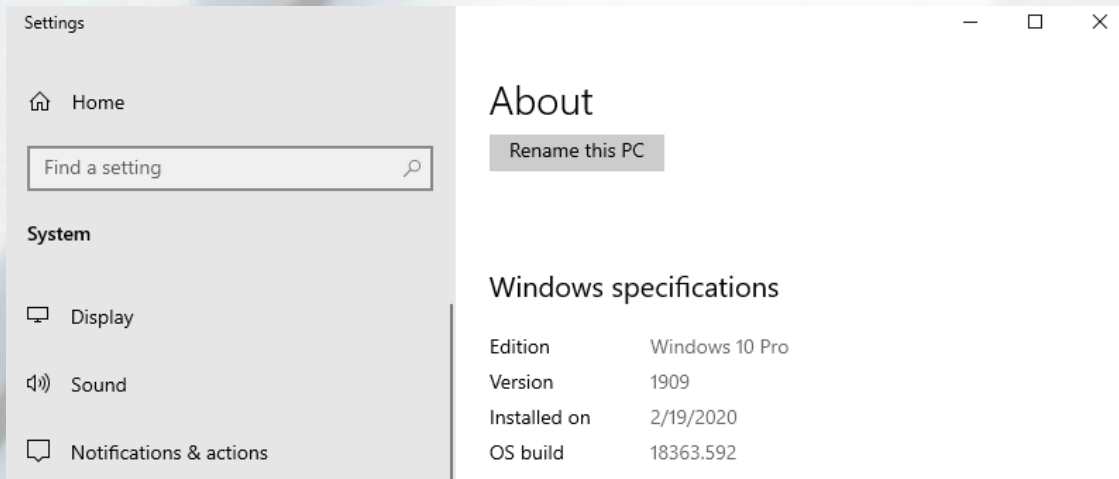
Security key

Security Key1

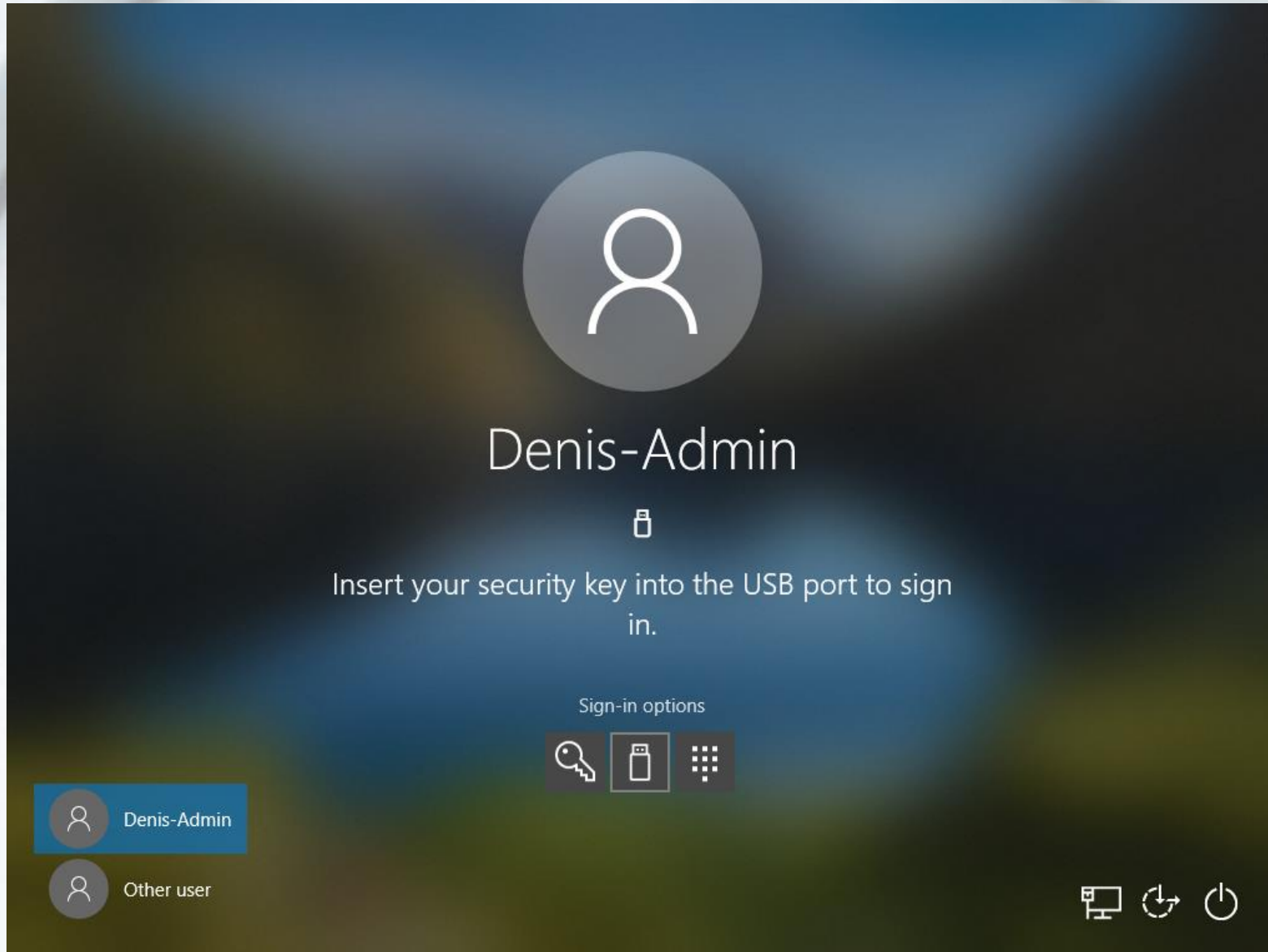
Delete

 **DATAWAY**
SECURITY

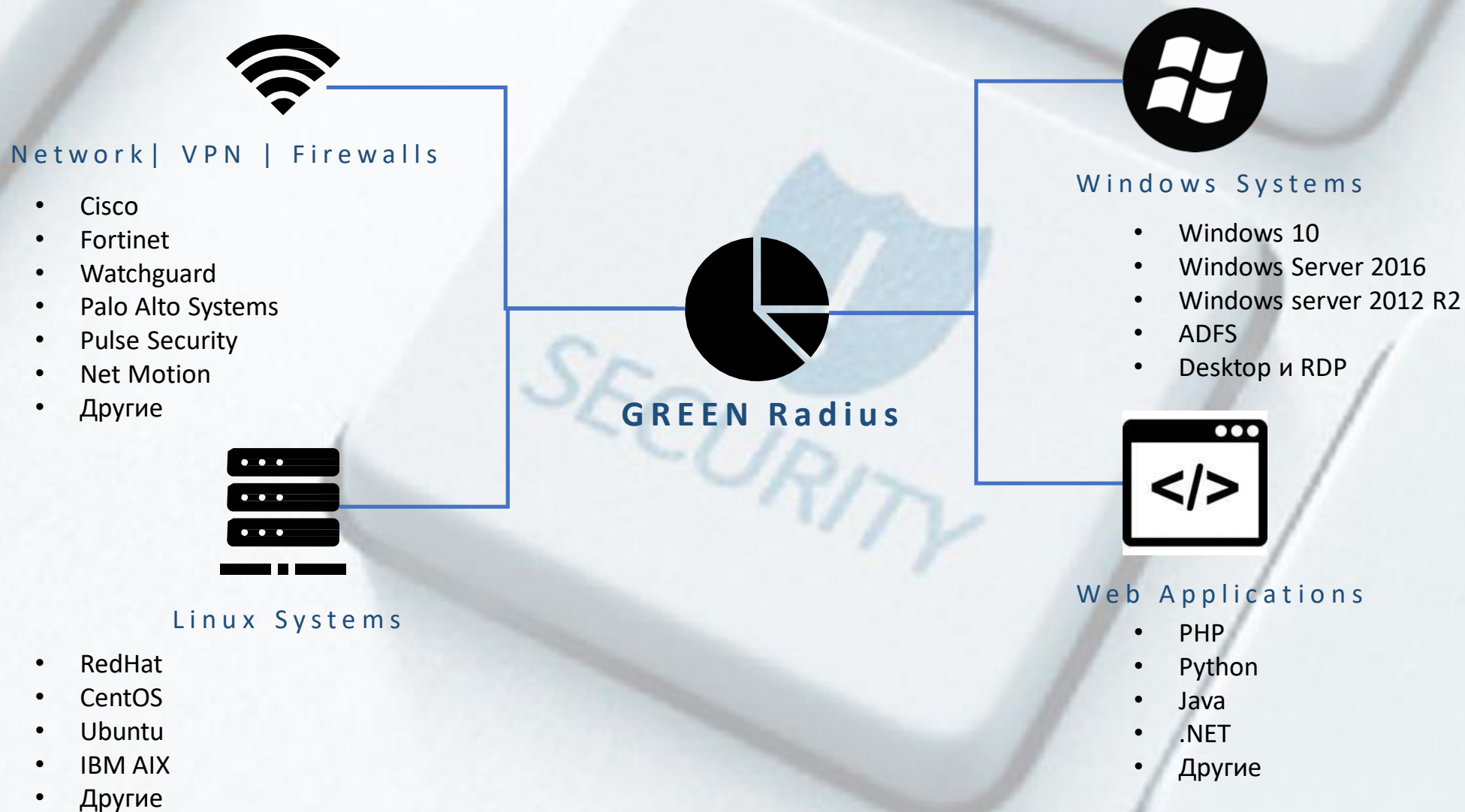
Произвести настройки на вашем ПК



Результат. Беспарольная аутентификации пользователя



Ключ безопасности в корпоративных средах





DATAWAY
SECURITY

СПАСИБО!

Приглашаем вас посетить на наш стенд

[www. datawaysecuriy.com.ua](http://www.datawaysecuriy.com.ua)
info@datawaysecurity.com.ua
Тел.: 044 501-1151