# Развитие и текущее применение систем многофакторной аутентификации пользователей СЭДО

# Утечки данных пользователей в 2014-2016 годах

## 2014

Google

Яндекс @mail.ru

Dropbox

iCloud

**>18 млн.**

## 2015

ASHLEY MADISON.COM

**>37 млн.**

## 2016

tumblr. myspace

LinkedIn

Рамблер/

YAHOO!

**>1,5 млрд.**

>4 млн/день

# Утечки и взломы. Причины и последствия

**17%** используют пароль **123456**

**47%** не меняют свои пароли более 5ти лет

**73%** используют одни и те же пароли на разных ресурсах

# Аутентификация в СЭДО сегодня

Login

*******

**Логин + пароль**

Простые пароли

**Токен**

Извлекаемый ключ

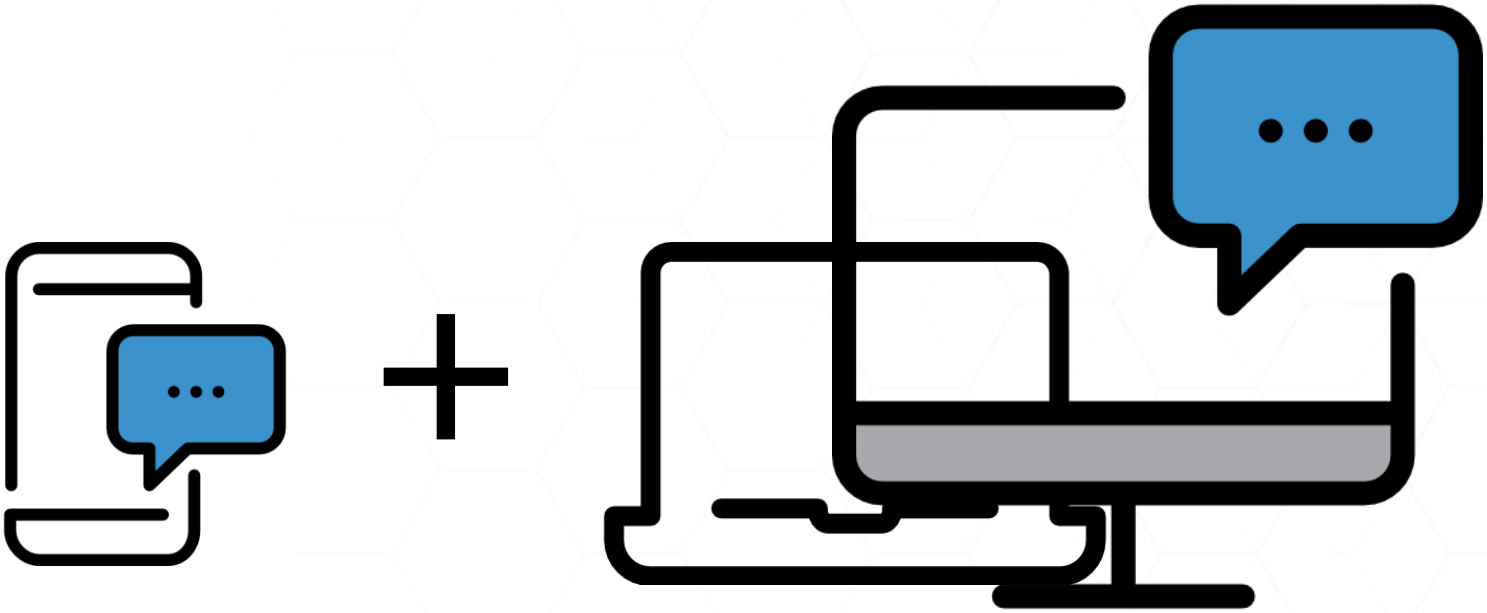
Пин-код «сохранен»

Не применим к облачной подписи

# Двухфакторная аутентификация

Метод идентификации пользователя при помощи запроса аутентификационных данных двух разных типов.

# Обязательный второй фактор



Телефон

Компьютер, ноутбук, планшет

# Краткий обзор второго фактора

**SMS**

\+

Работает не только на смартфонах

\-

Цена

?

Безопасность

**Messengers**

\+

Бесплатно (пока)

\-

Малое покрытие

?

Зависимость от чужого API

**TOTP**

\+

Малые изначальные вложения

\-

Отдельное приложение

?

Относительная безопасность

**Token**

\+

Безопасность

\-

Цена

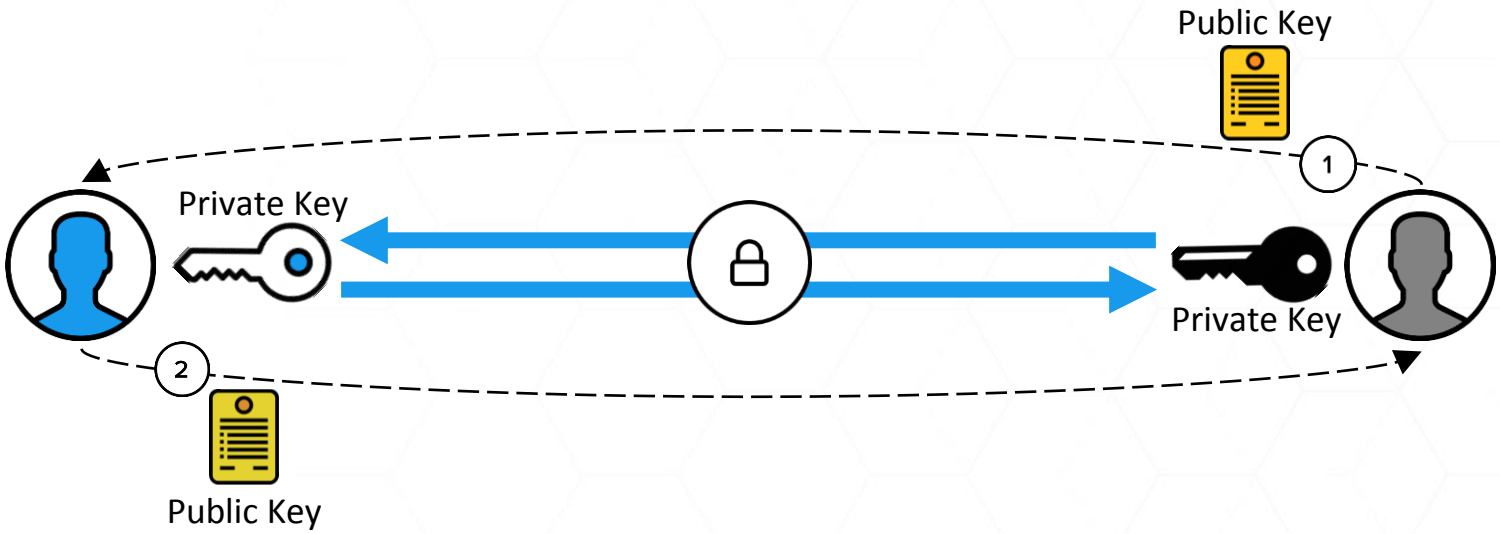
?

Удобство

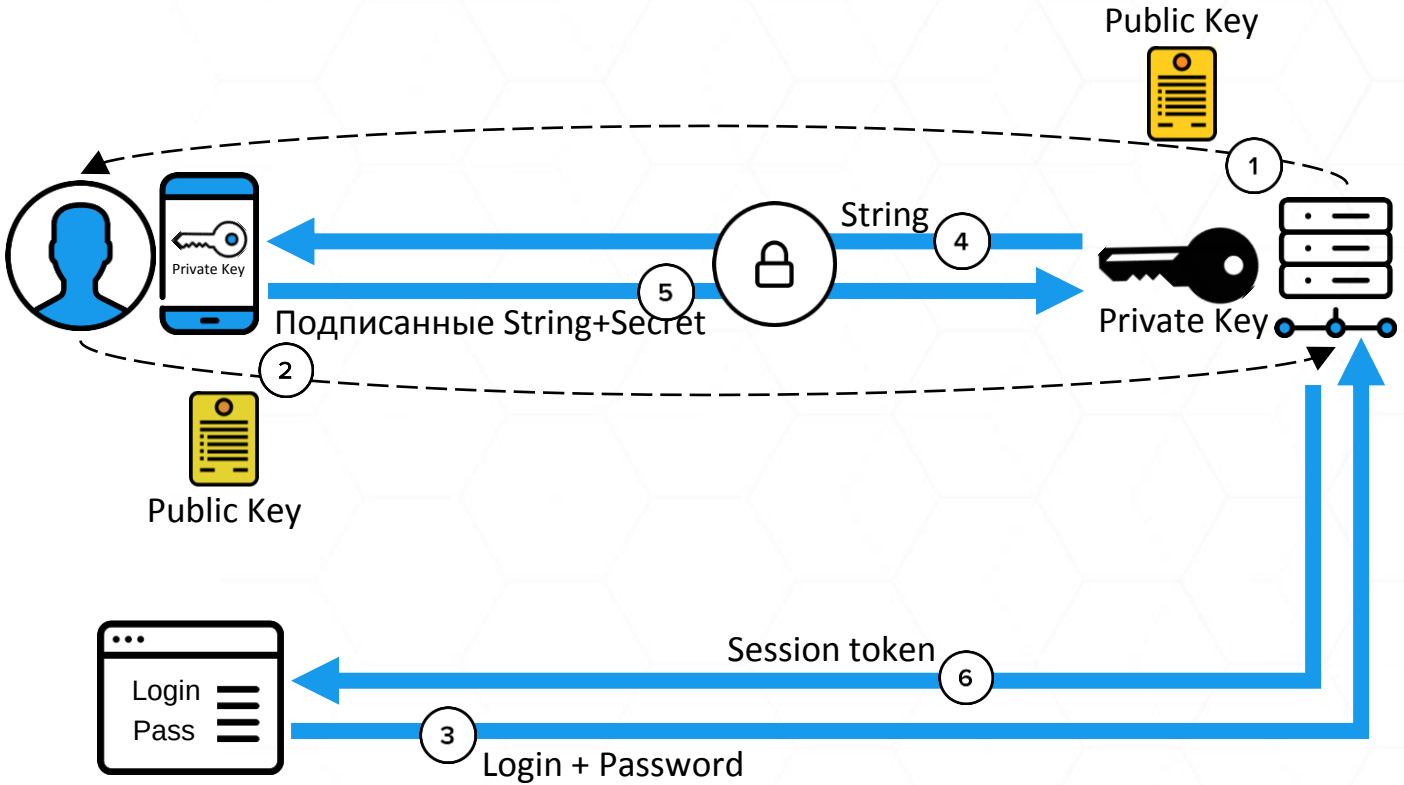
# End-to-end шифрование

Это способ обмена информацией, при котором только участники взаимодействия могут читать сообщения друг друга.

# End-to-end шифрование. Принцип работы

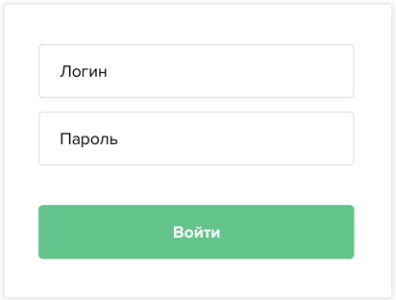


# End-to-end шифрование во втором факторе (Техническая схема)

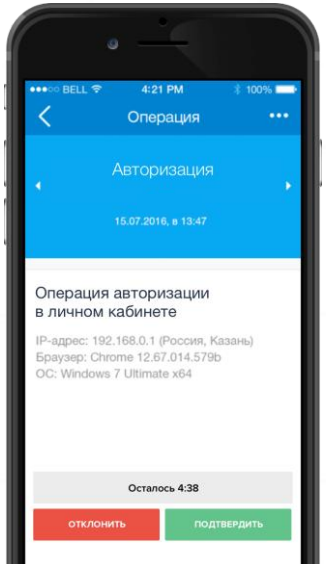


# End-to-end шифрование во втором факторе (Бизнес-процесс)

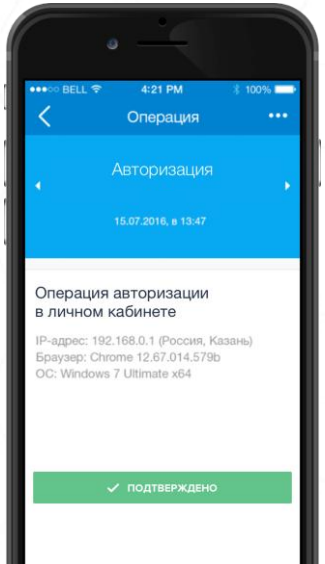

Клиент переходит на страницу личного кабинета. Вводит логин+пароль.




Cryptogramm ID запрашивает у пользователя подтверждение операции **push-уведомлением**




Пользователь подтверждает операцию через мобильное приложение.

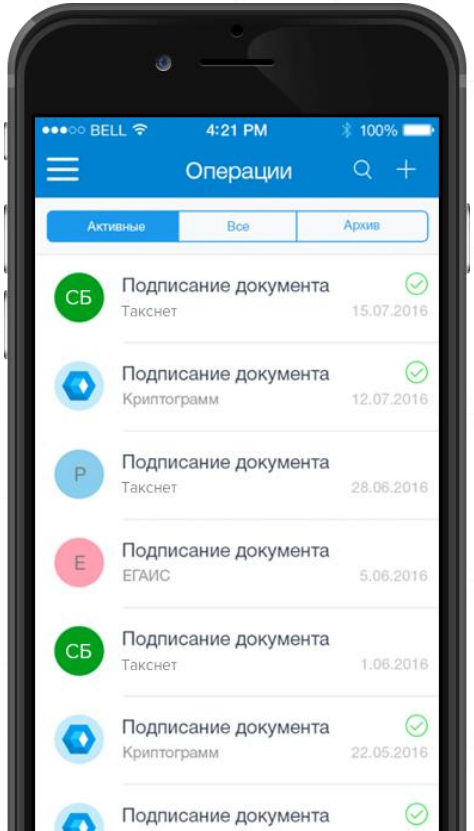



Происходит авторизация в личном кабинете пользователя.

**Авторизация выполнена успешно!**

# Cryptogramm ID

- Разграничение уровней логики приложения и безопасности
- Идентификация пользователя
- End-to-end защита данных
- Идентификация девайса
- Использование цифровых сертификатов



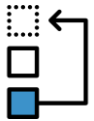
# Приучи к хорошему

## Популяризация идеи безопасности среди пользователей

- Публикации в блогах, соц. сетях, e-mail рассылках

## Стимулирование использования 2FA

- Геймификация в интерфейсе
- Система «вознаграждений» и «спец. предложений»



## Упрощение бизнес-процессов за счет 2FA

- Оптимизация существующих бизнес-процессов продукта

Артур Гайнуллин

artur@cryptogramm.ru

fb.com/gainullinme