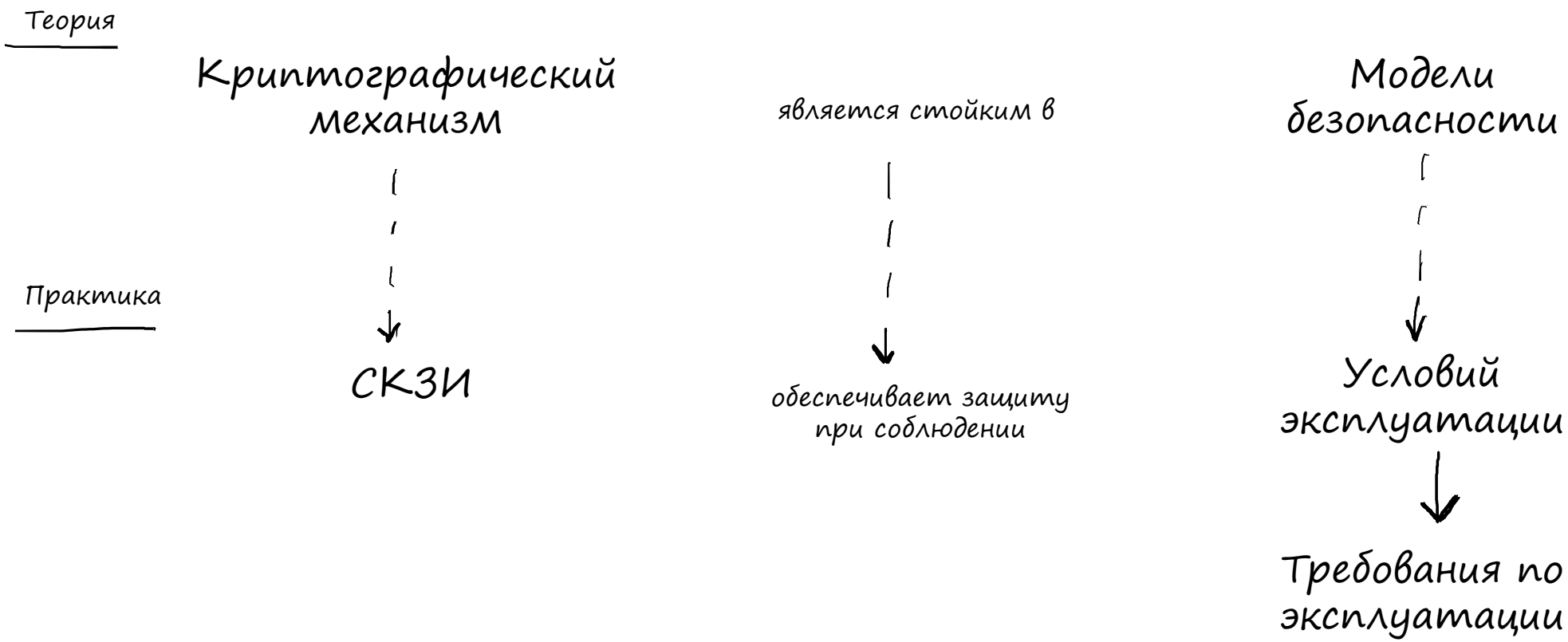
Электронная подпись в условиях массового применения

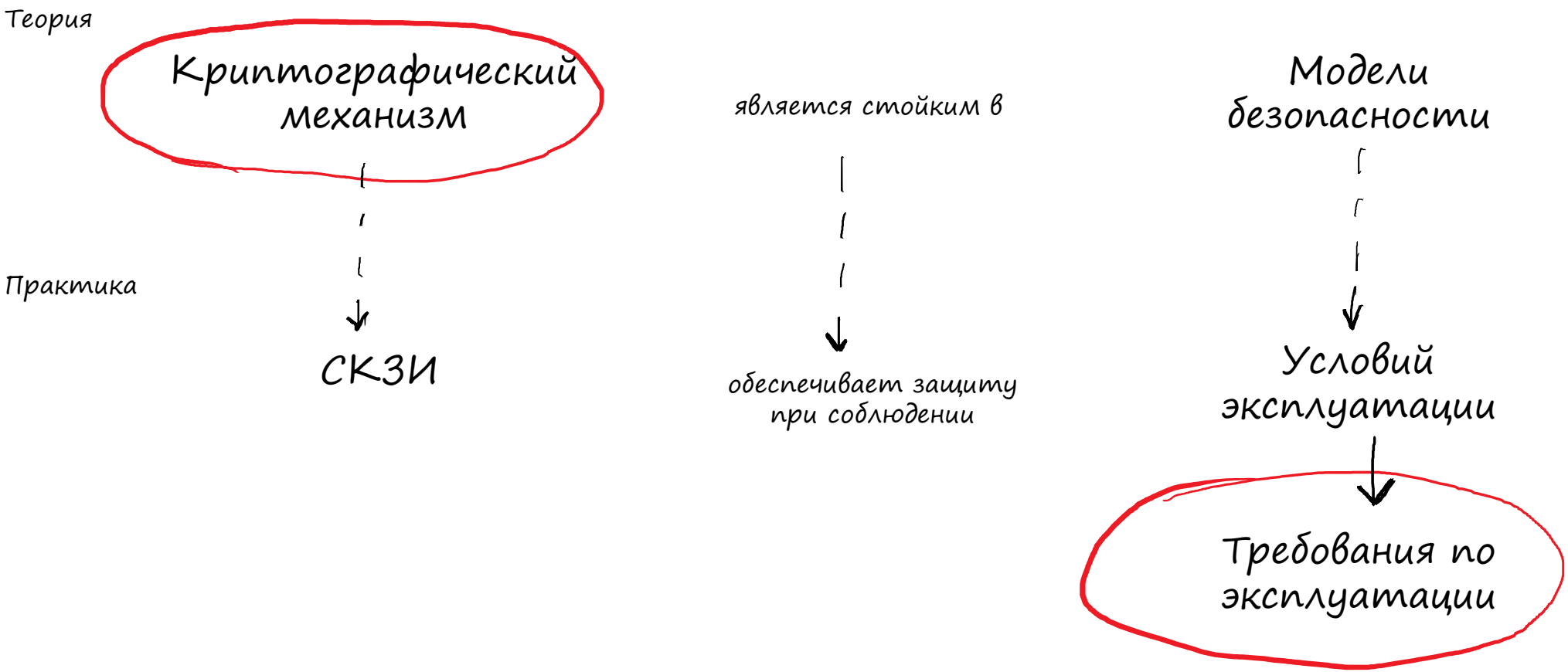
Алексеев Евгений Константинович, к.ф.-м.н., ООО «КРИПТО-ПРО»
Никифорова Лидия Олеговна, ООО «КРИПТО-ПРО»

КРИПТОПРО

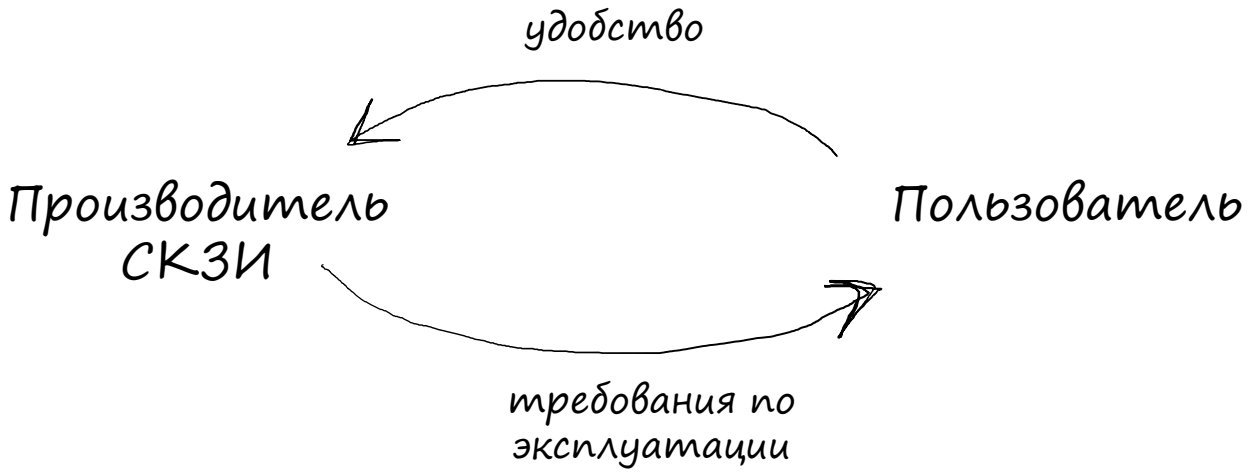
Криптография и практика



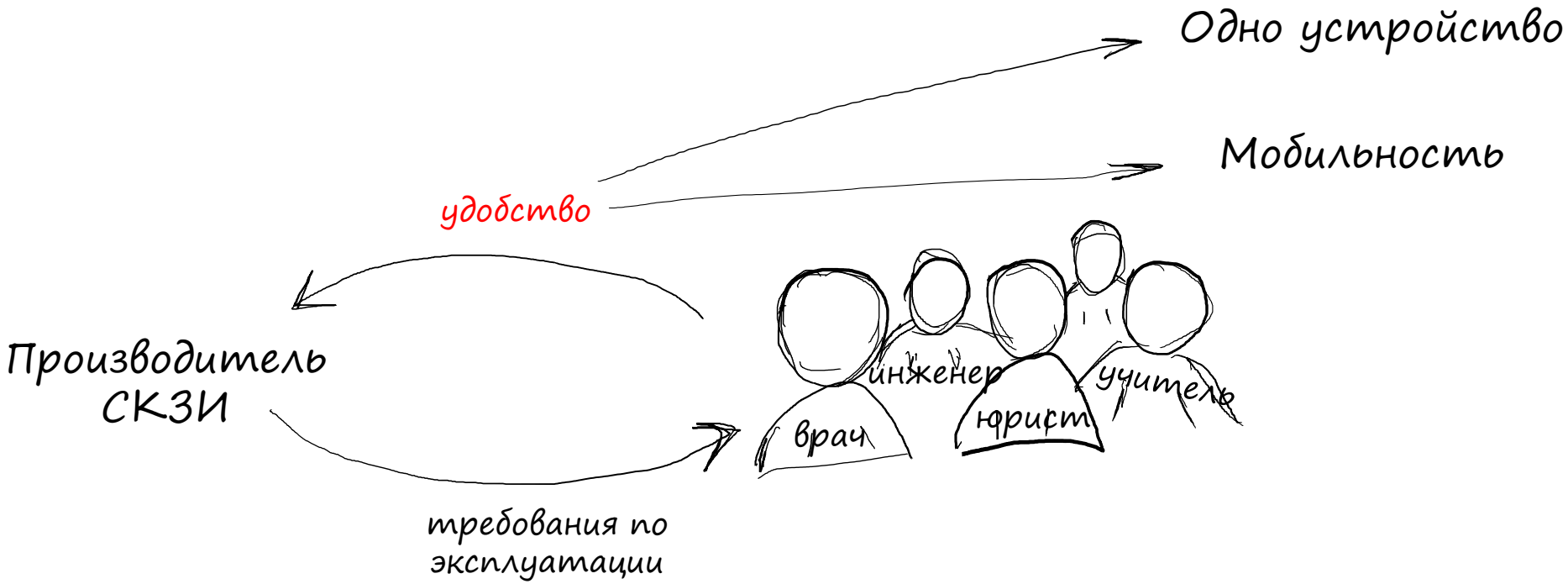
Криптография и практика



Массовая криптография



Массовая криптография



Массовая криптография

Одно устройство

Мобильность

удобство

Производитель СКЗИ

требования по эксплуатации

Максимальная защита в крайних случаях

Отсутствие необходимости доверия к третьим сторонам

Электронная подпись

Теория

Электронная подпись имеет юридическую силу (ФЗ 63)

Есть российский стандарт электронной цифровой подписи (ГОСТ Р 34.10-2012)

Практика

Требования по эксплуатации — направлены на — Обеспечение секретности ключа

Электронная подпись

Практика

Требования по эксплуатации — направлены на — Обеспечение секретности ключа

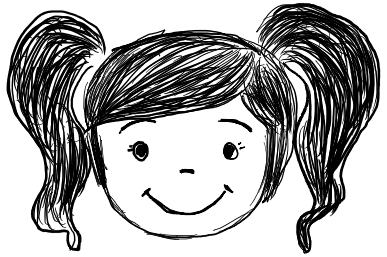
Рассмотрим различные подходы к обеспечению секретности ключа и оценим их с точки зрения массового применения

Ключ на токене + компьютер

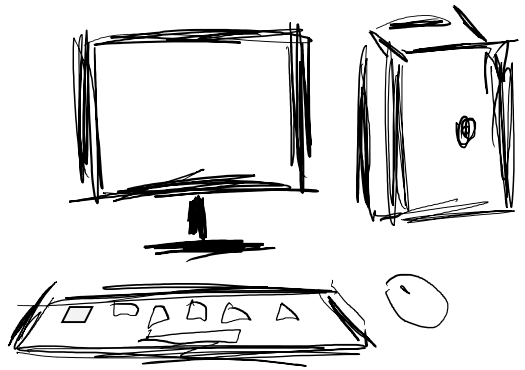
хранится ключ

производятся все операции с ключом

пароль



для доступа к ключу нужно ввести пароль

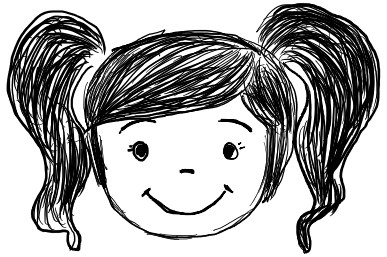


Требования по эксплуатации:

никому не давать токен, придумать хороший пароль, никому его не говорить

Ключ на токене + компьютер

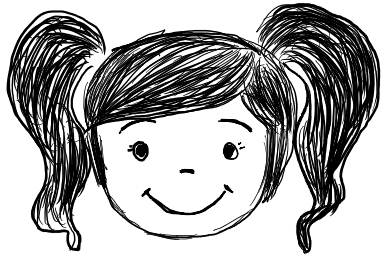
пароль

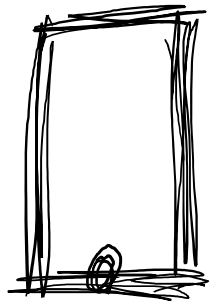


Одно устройство	Мобильность	Компрометация устройства	Компрометация устройства и пароля	Отсутствие необходимости доверия серверу

Ключ на токене + смартфон

пароль

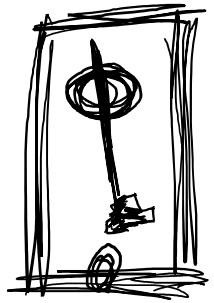




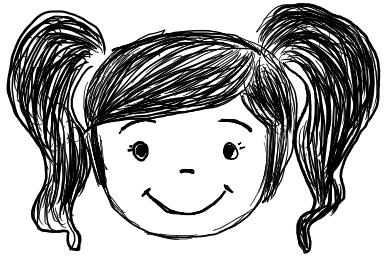
Тоже самое, но компьютер искать не нужно...

Одно устройство	Мобильность	Компрометация устройства	Компрометация устройства и пароля	Отсутствие необходимости доверия серверу

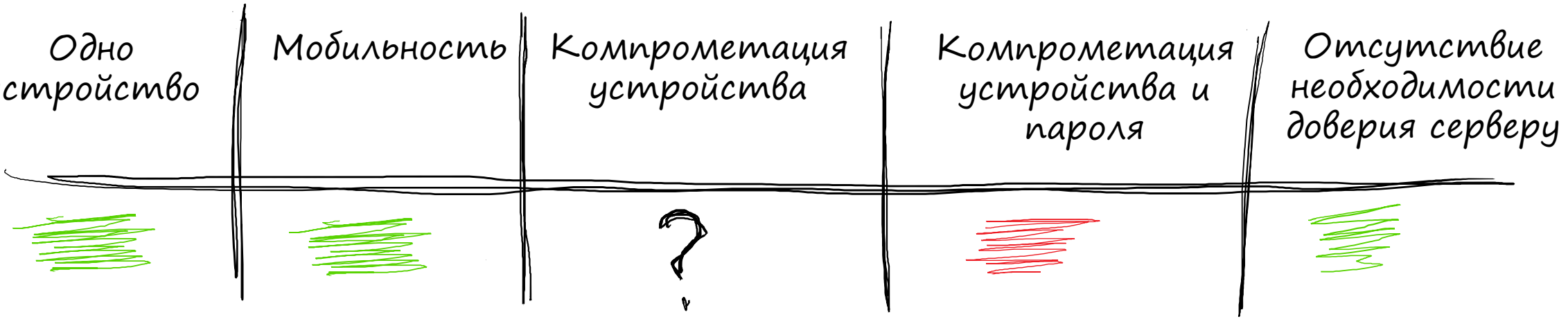
Ключ на смартфоне под защитой пароля



пароль

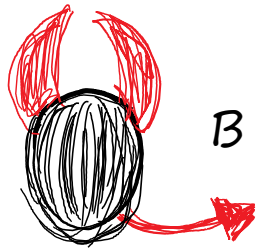


для доступа к ключу нужно ввести пароль



Ключ на смартфоне под защитой пароля

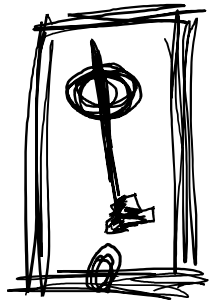
пароль



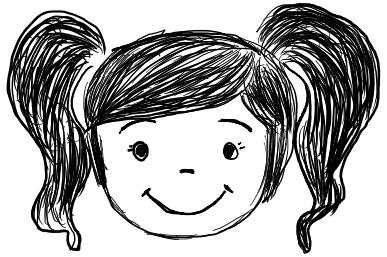
В случае кражи устройства нарушитель сможет перебрать пароль

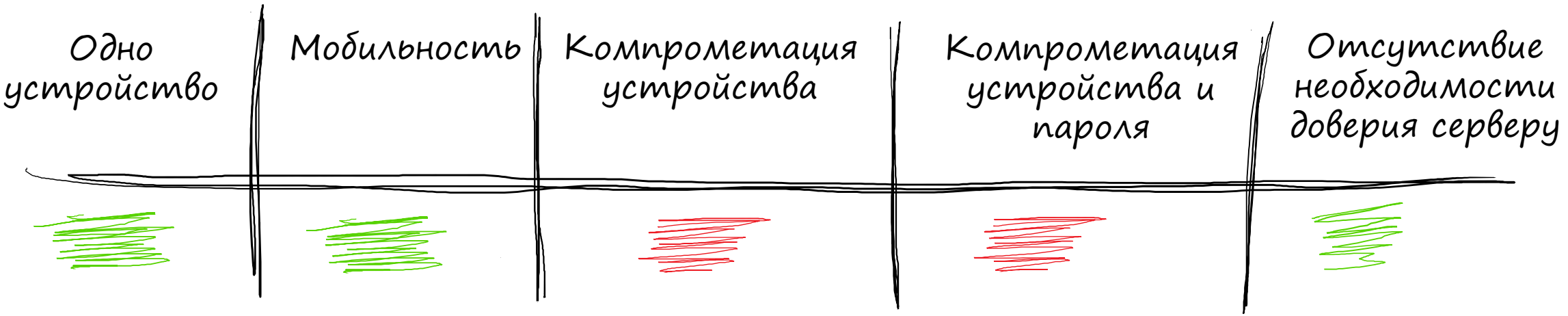
Критерии: имитовставка, открытый ключ

Ключ на смартфоне под защитой пароля

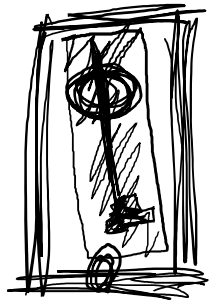


пароль

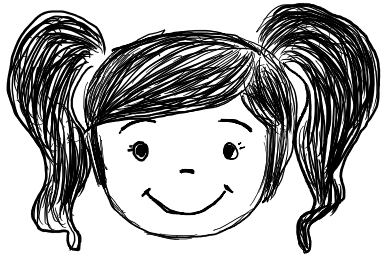


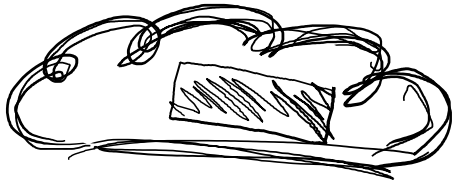


Ключ на смартфоне под защитой с помощью сервера

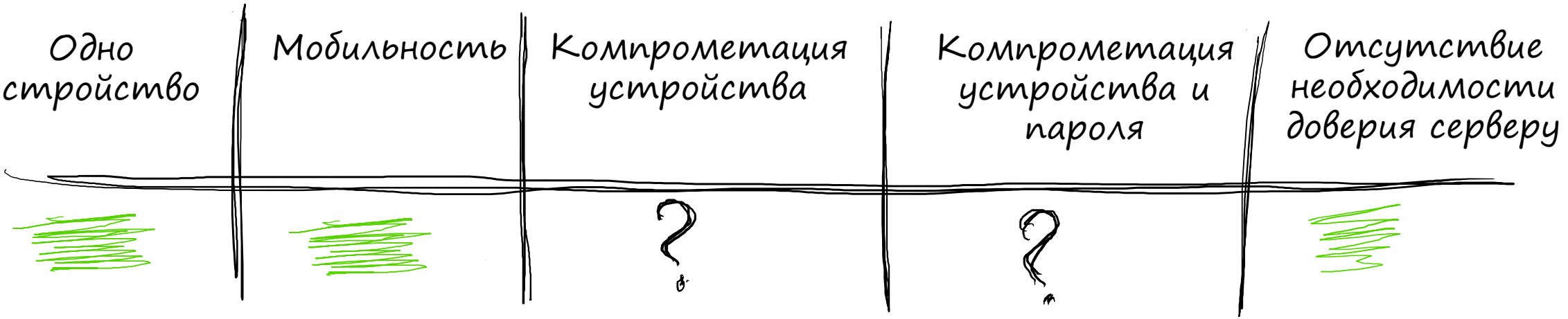


пароль

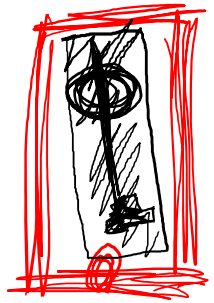




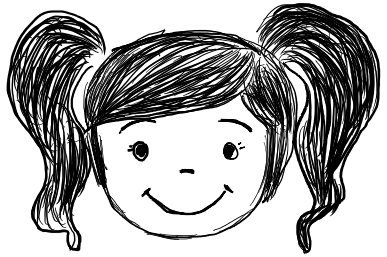
для доступа к вектору защиты ключа нужно ввести пароль

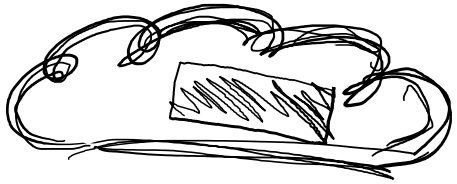


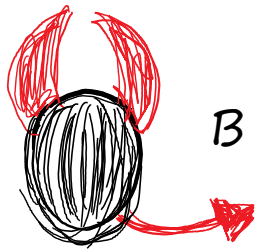
Ключ на смартфоне под защитой с помощью сервера



пароль





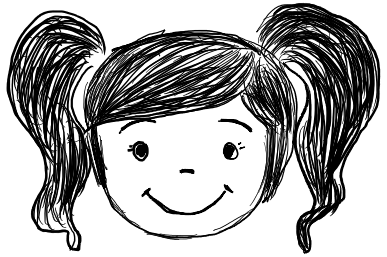


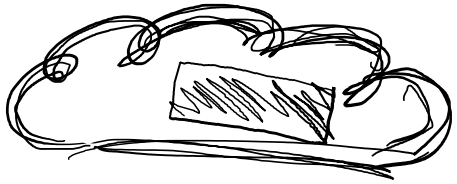
В случае кражи устройства нарушитель не сможет перебрать пароль

Ограничение на количество попыток за счёт сервера

Ключ на смартфоне под защитой с помощью сервера

пароль

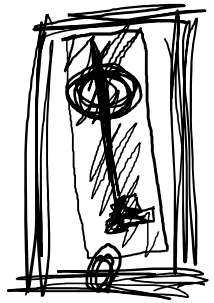




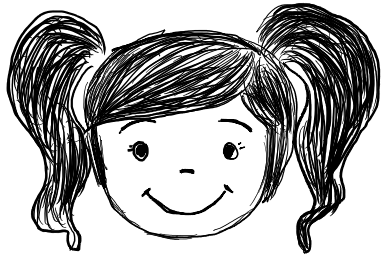
В случае кражи устройства и компрометации пароля нарушитель сможет получить доступ к ключу и подписывать неограниченное количество раз

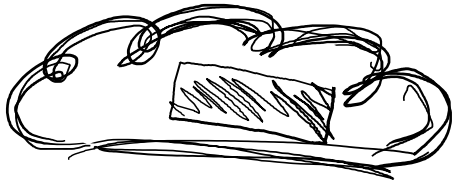
НО сервер может уведомить пользователя о том, что был осуществлён доступ к вектору защиты. Пользователь может среагировать на уведомление и отозвать сертификат

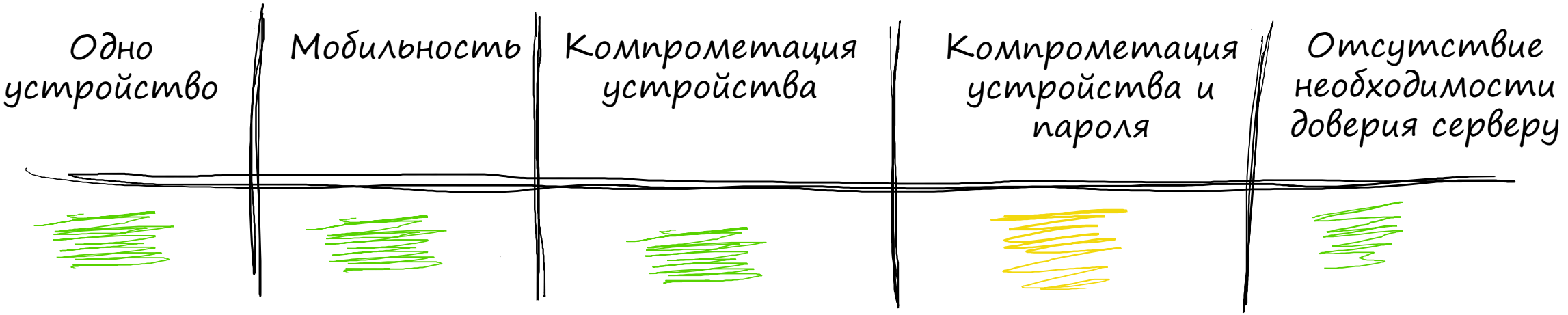
Ключ на смартфоне под защитой с помощью сервера



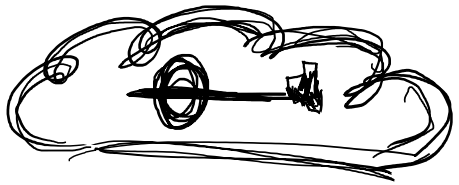
пароль







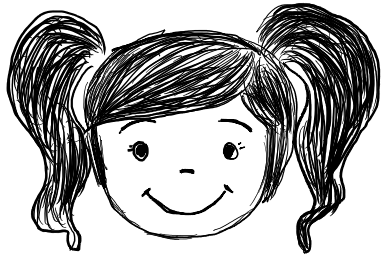
Ключ на сервере



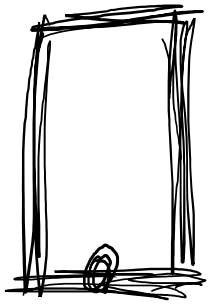
хранится ключ

производятся все операции с ключом

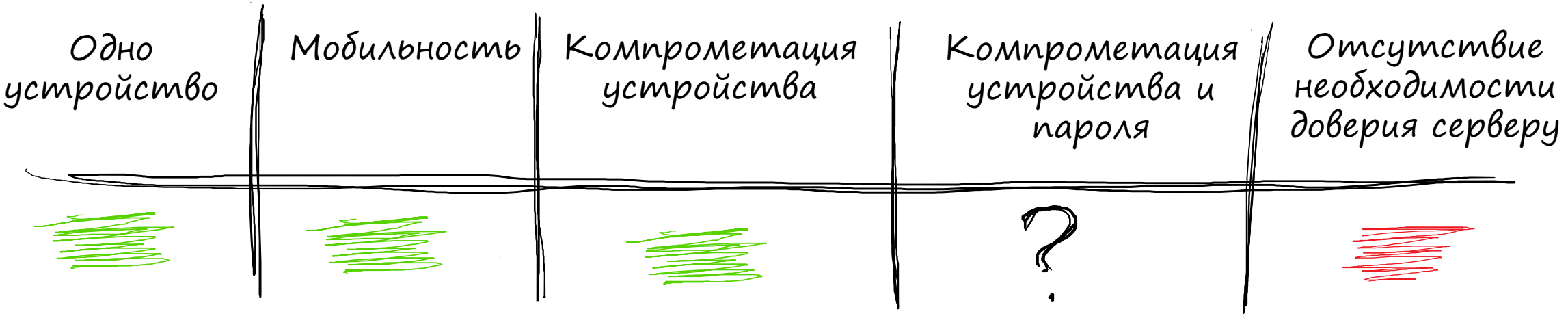
пароль



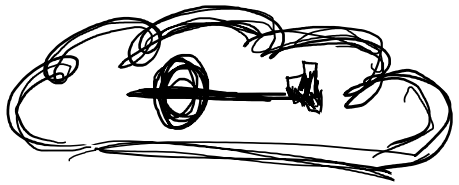
для доступа к ключу нужно ввести пароль



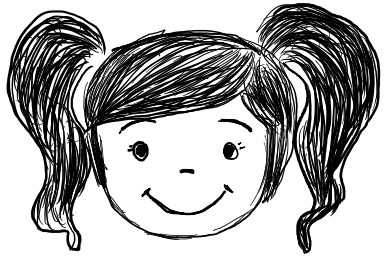
второй фактор аутентификации на сервере

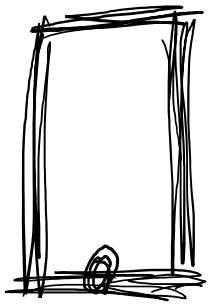


Ключ на сервере



пароль

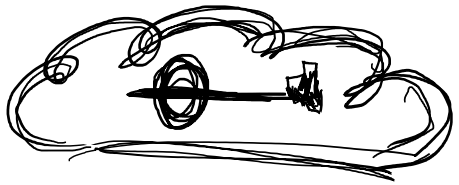




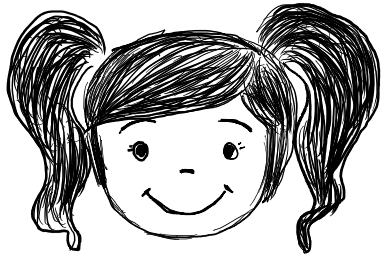
В случае кражи устройства и компрометации пароля нарушитель сможет подписывать, ТОЛЬКО СОВЕРШАЯ ЗАПРОСЫ К СЕРВЕРУ

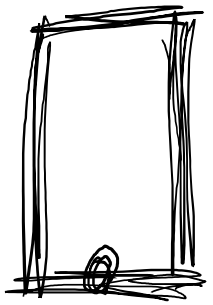
Отслеживаемость: сервер знает все документы, которые были подписаны с помощью данного ключа подписи

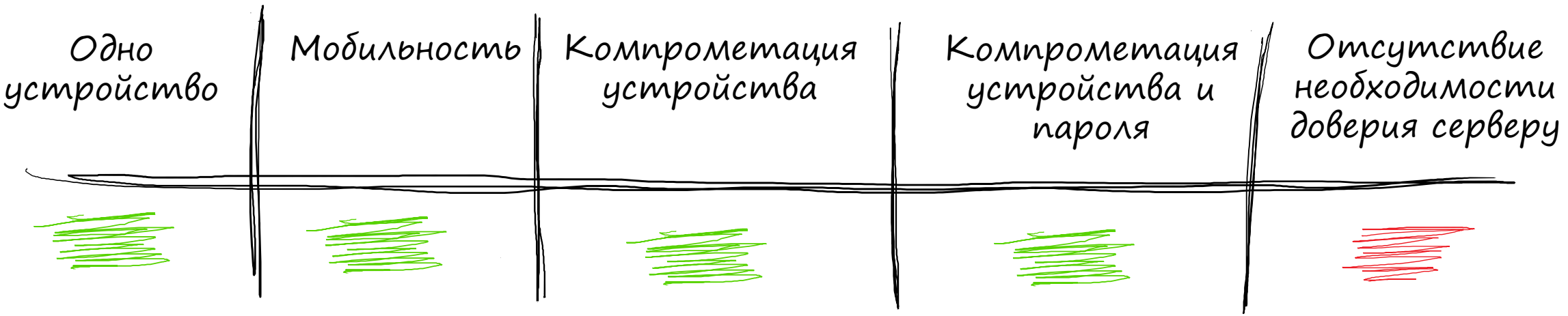
Ключ на сервере



пароль



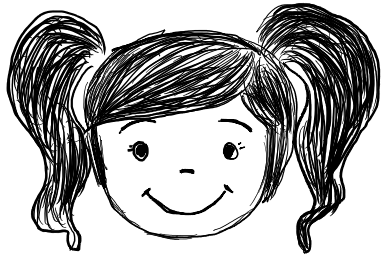




Часть ключа на смартфоне, часть ключа на сервере

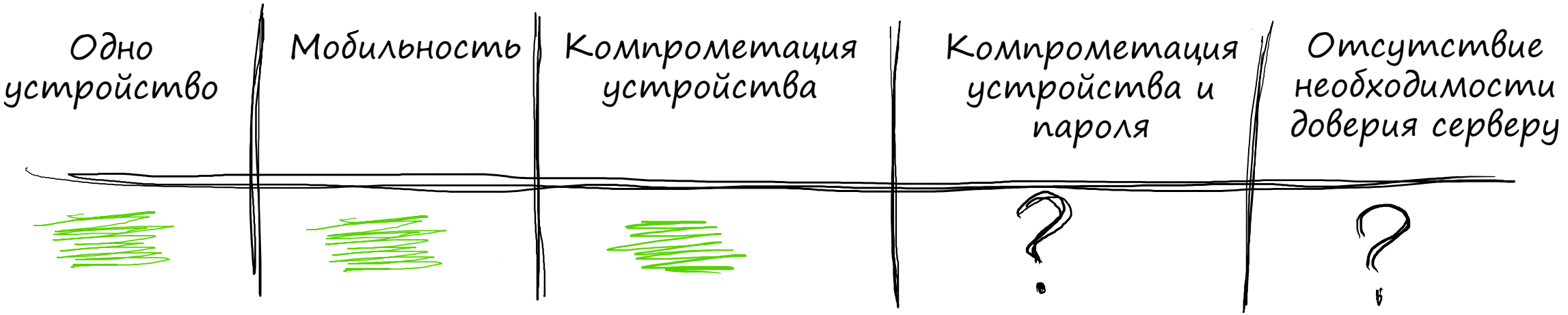
хранится часть ключа

пароль



для доступа к вектору защиты нужен пароль

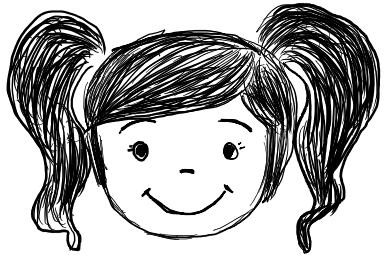
хранится вторая часть ключа



Часть ключа на смартфоне, часть ключа на сервере

хранится часть ключа

пароль



для доступа к вектору защиты нужен пароль

хранится вторая часть ключа

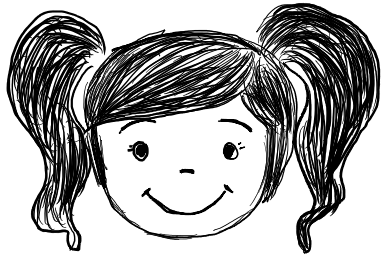
Используется специальная двусторонняя схема подписи – ни одна сторона не сможет подписать без взаимодействия со второй стороной.

CTCrypt 2023. «Two-party GOST in two parts: fruitless search and fruitful synthesis»

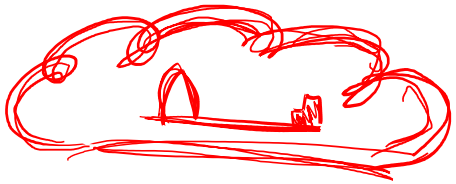
Часть ключа на смартфоне, часть ключа на сервере

хранится часть ключа

пароль



для доступа к вектору защиты нужен пароль



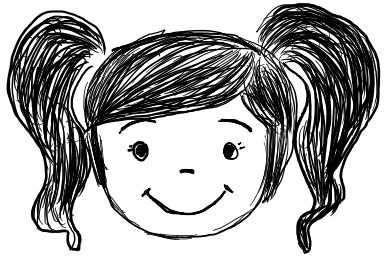
хранится вторая часть ключа

Сервер не сможет подписывать без клиента

Часть ключа на смартфоне, часть ключа на сервере

хранится часть ключа

пароль



для доступа к вектору защиты нужен пароль

хранится вторая часть ключа

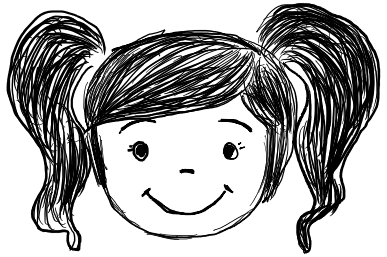
В случае кражи устройства и компрометации пароля нарушитель сможет подписывать, ТОЛЬКО СОВЕРШАЯ ЗАПРОСЫ К СЕРВЕРУ

Отслеживаемость: сервер знает все документы, которые были подписаны с помощью данного ключа подписи

Часть ключа на смартфоне, часть ключа на сервере

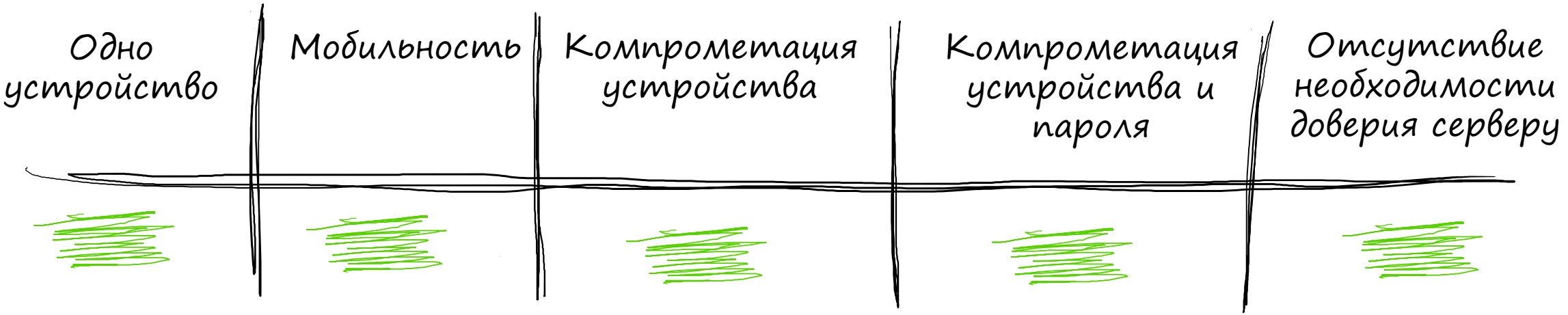
хранится часть ключа

пароль

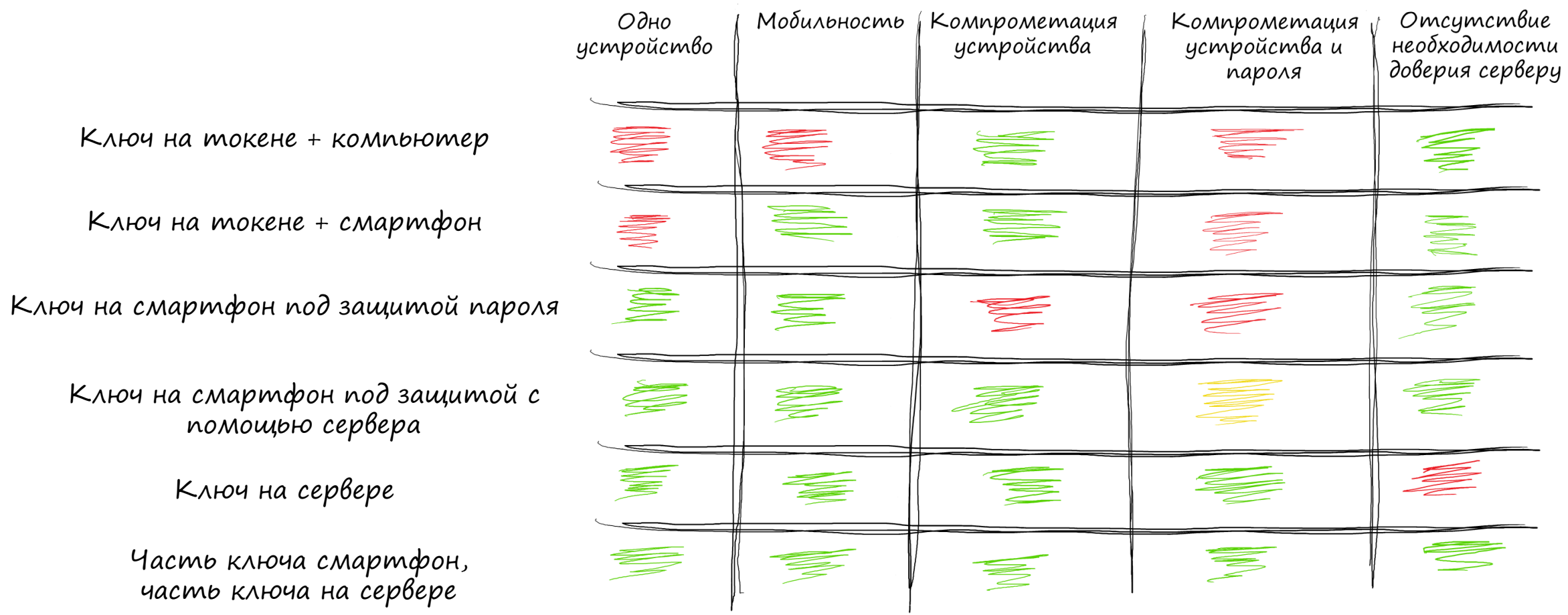


для доступа к вектору защиты нужен пароль

хранится вторая часть ключа



Итог


Одно устройство
Мобильность
Компрометация устройства
Компрометация устройства и пароля
Отсутствие необходимости доверия серверу
Ключ на токене + компьютер
Ключ на токене + смартфон
Ключ на смартфон под защитой пароля
Ключ на смартфон под защитой с помощью сервера
Ключ на сервере
Часть ключа смартфон, часть ключа на сервере