РУТОКЕН

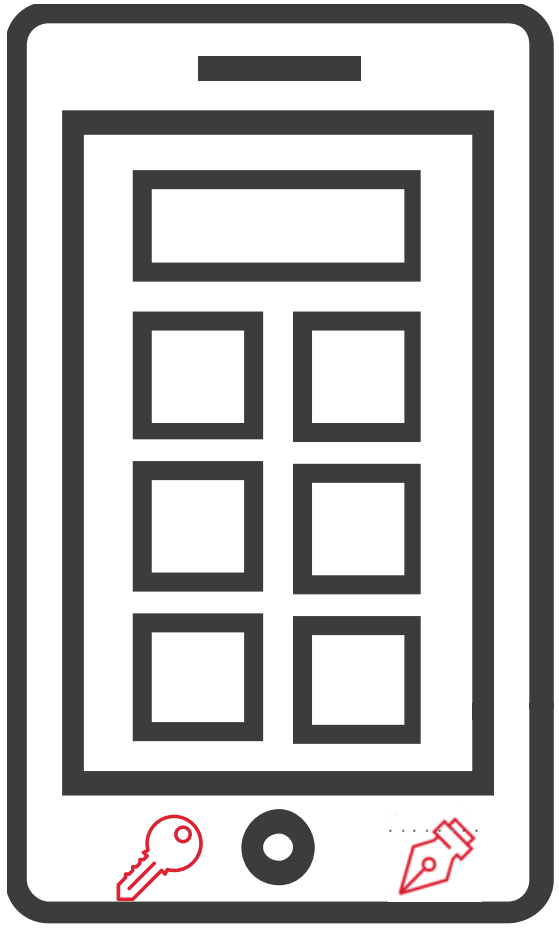
PKI Форум Россия 2020

Электронная подпись на мобильных устройствах и облачные решения: секреты должны оставаться секретами

Владимир Иванов
Директор по развитию
Компания «Актив»

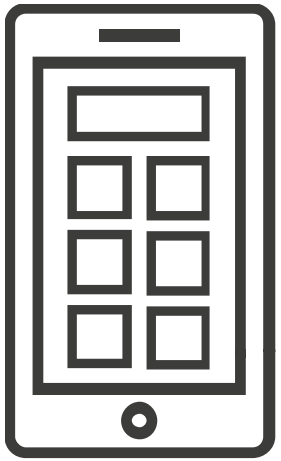
Мобильная подпись

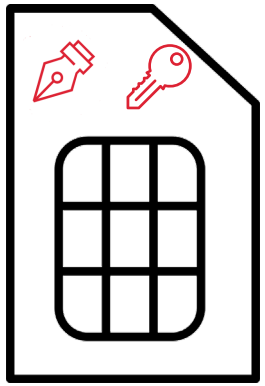
Мобильная подпись: в приложении



- Ключи хранятся в памяти недоверенного устройства
- Криптография реализована программно
- Сложно доверять генератору случайных чисел
- Приложение распространяется через сторонние сервисы
- Пользоваться можно только на мобильном устройстве
- Аутентификация средствами мобильной платформы
- При удалении приложения, как правило, удаляется ключ подписи

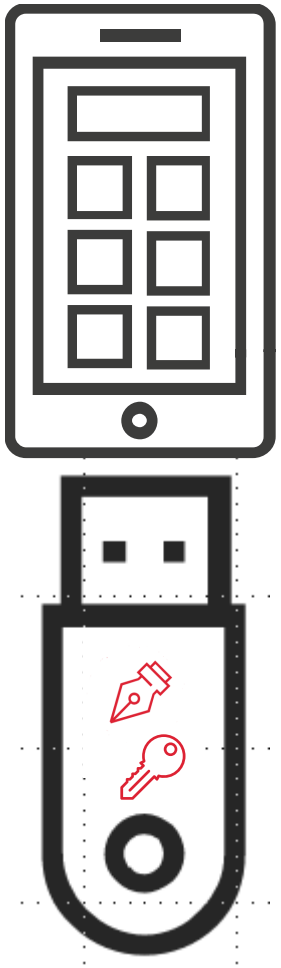
Мобильная подпись: на SIM-карте





- Специальная SIM-карта с криптографическими функциями
- Проблемы с идентификацией пользователя и выпуском сертификата. Нужно два раза идентифицировать заявителя.
- Коммуникации – нельзя обращаться из ОС. Передача данных только через SMS
- Пользоваться можно только на мобильном устройстве
- Практически невозможно визуализировать документ
- Требует подключения к мобильной сети
- Фактически нельзя отделить ключи от мобильного устройства
- Наступление eSIM – нет перспектив

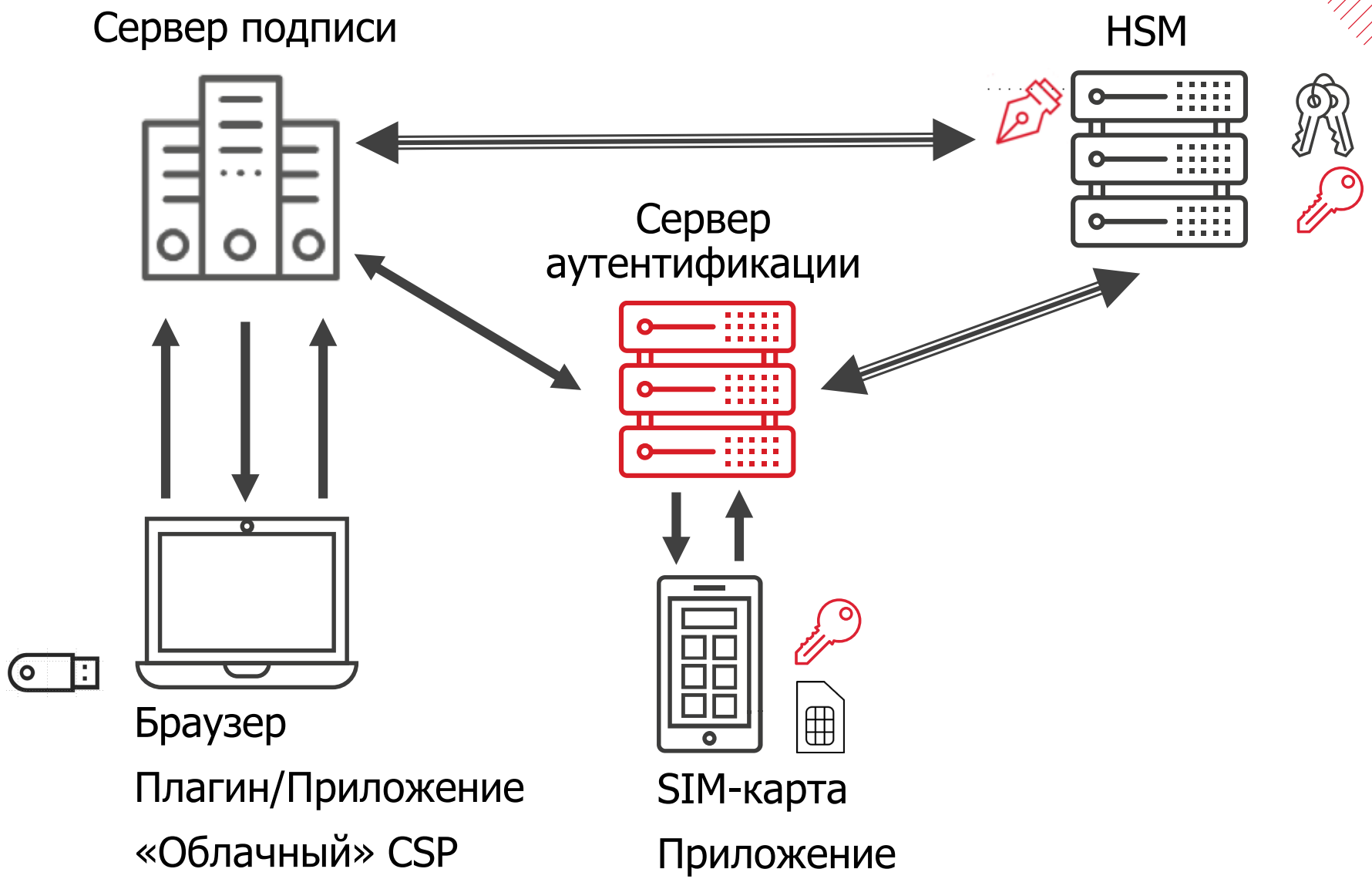
Мобильная подпись: на токене



- Токен с контактным интерфейсом – разнообразие портов
- Bluetooth токен – требует процедуры сопряжения. Высокая цена
- Эксплуатируется только с приложением

Облачная подпись

Облачная подпись

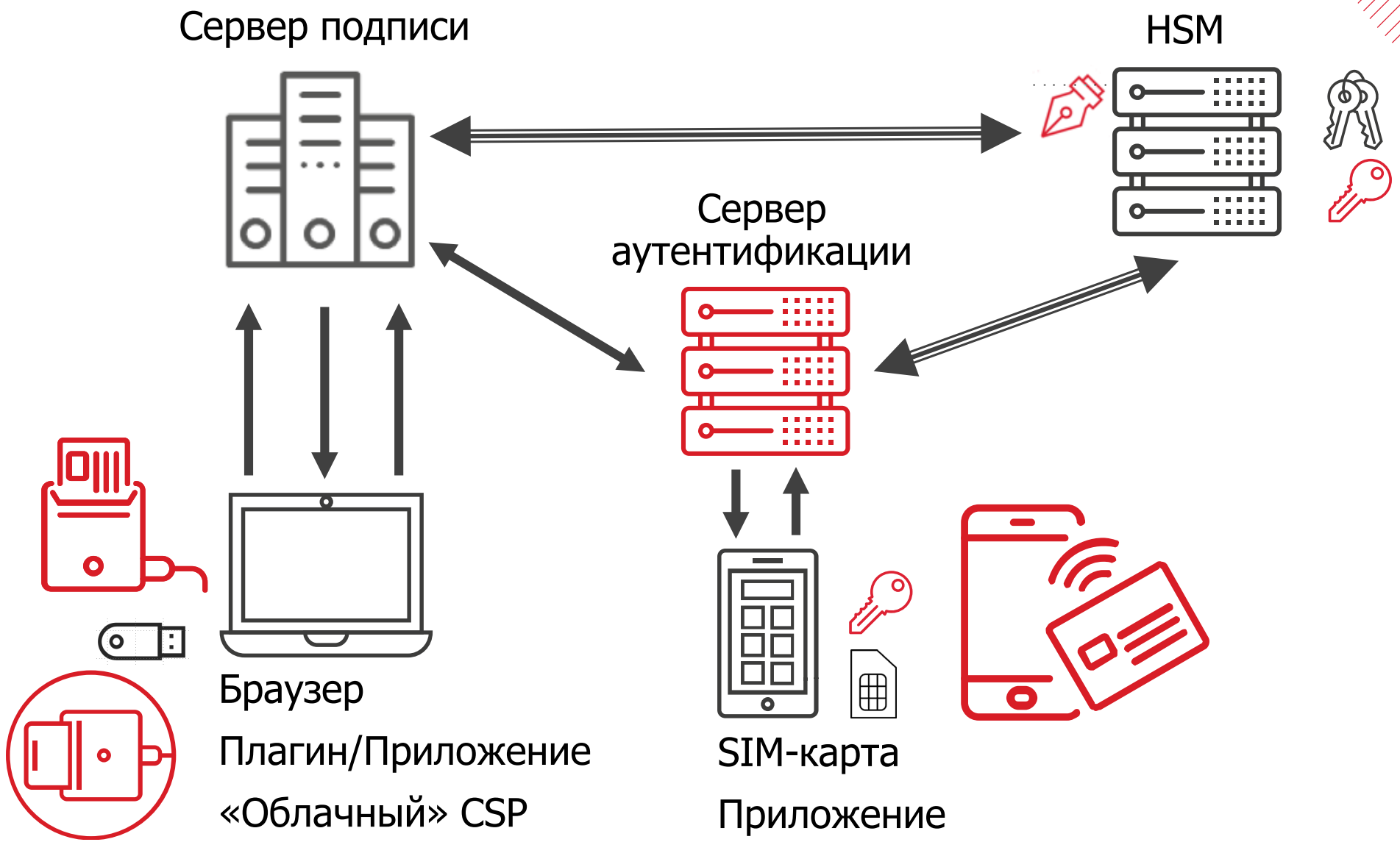


Как отделить ключи от мобильного устройства?

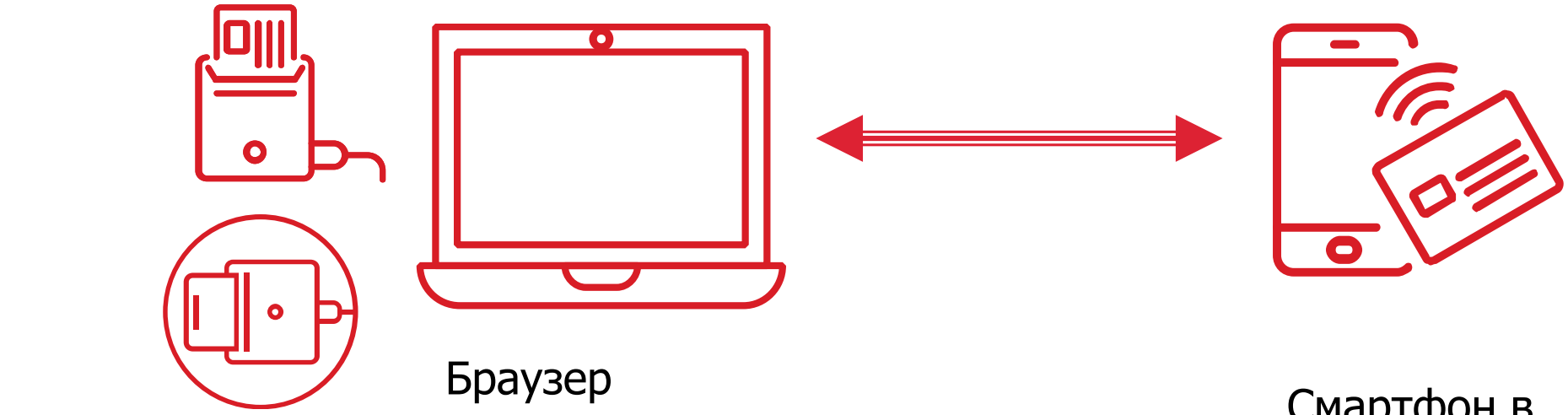
Дуальная смарт-карта
Рутокен ЭЦП 3.0 NFC

- Подпись касанием карты к мобильному устройству или считывателю
- Криптография на борту на неизвлекаемых ключах
- Производительность через NFC канал не хуже, чем через контактный интерфейс
- Не требует процедуры сопряжения
- Питание через интерфейсы
- Использование на мобильных устройствах (Android, iOS, Аврора) бесконтактно
- Использование на ПК бесконтактно и контактно
- Секреты хранятся отдельно от приложений и документов

Облачная подпись



Локальная и мобильная подписи
на Рутокен ЭЦП 3.0 NFC



Контактный или
NFC считыватель

Браузер

Плагин/Приложение

«Облачный» CSP

Смартфон в
качестве NFC
считывателя


XXXX
XXX
01001
10110
01011
РУТОКЕН

Контактная информация

Владимир Иванов

info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90

РУТОКЕН

Характеристики
Рутокен ЭЦП 3.0 NFC

- Аппаратная реализация криптографии:
  - ГОСТ 34.10-2012 (256/512 бит)
  - ГОСТ 34.11-2012
  - VKO GOST
  - Магма
  - Кузнечик
  - RSA
  - ECDSA
- Совместимость с современными ОС, включая отечественные и мобильные
- Совместимость с криптопровайдерами
- Защита NFC канала (SESPAKE)
- Высокая производительность
- SDK для встраивания в приложения