РУТОКЕН

XIII международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи PKI-Форум Россия 2015

15–17 сентября 2015 г., Санкт-Петербург, гостиница Москва

Криптография для массового применения

Горелов Дмитрий Львович,
коммерческий директор компании «Актив»

PKI-FORUM
РОССИЯ `15

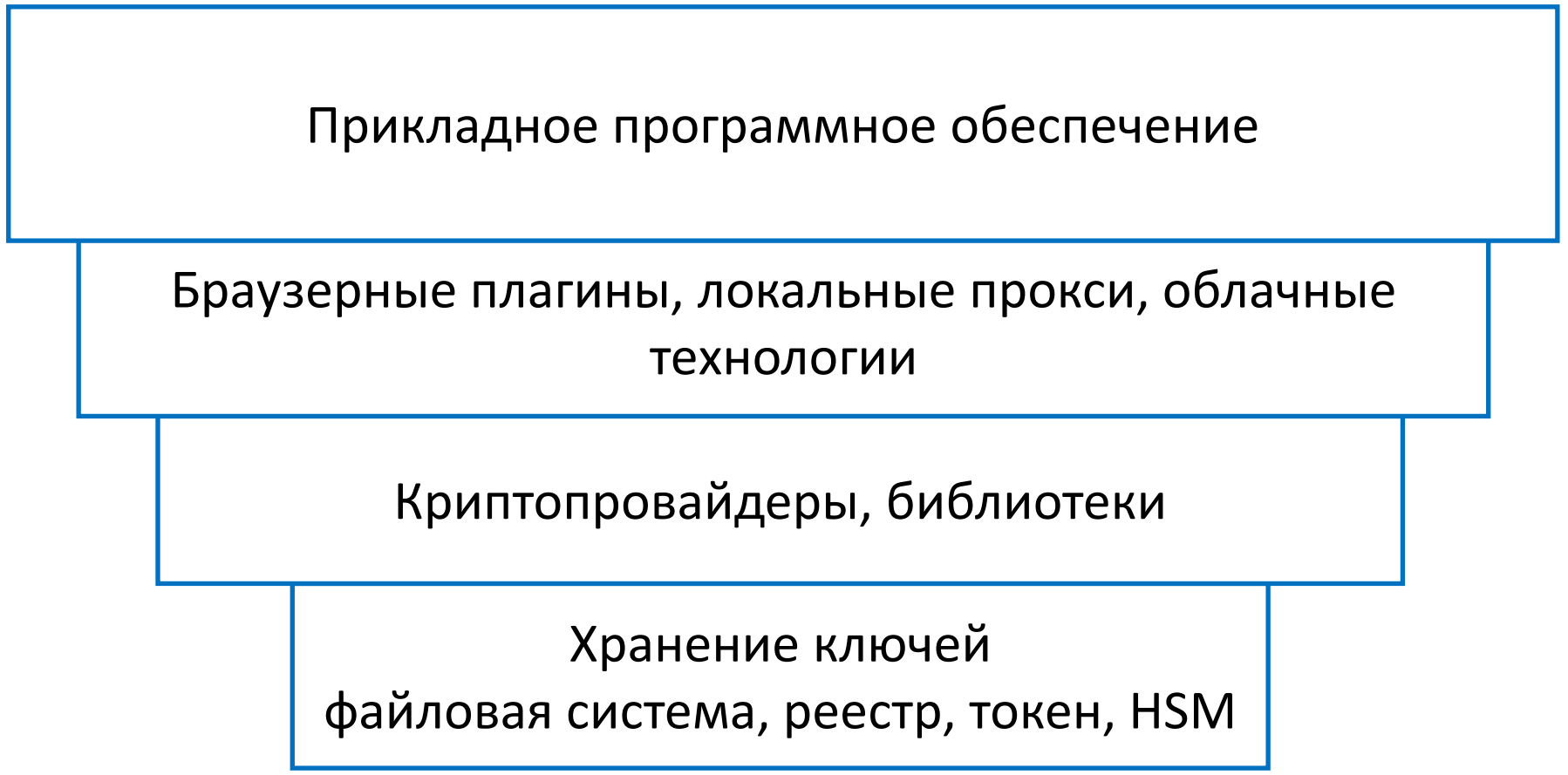
Введение

- Рассматривается архитектура решений использующих электронную подпись и инфраструктуру открытых ключей
- Рассматриваются информационные системы для массового пользователя

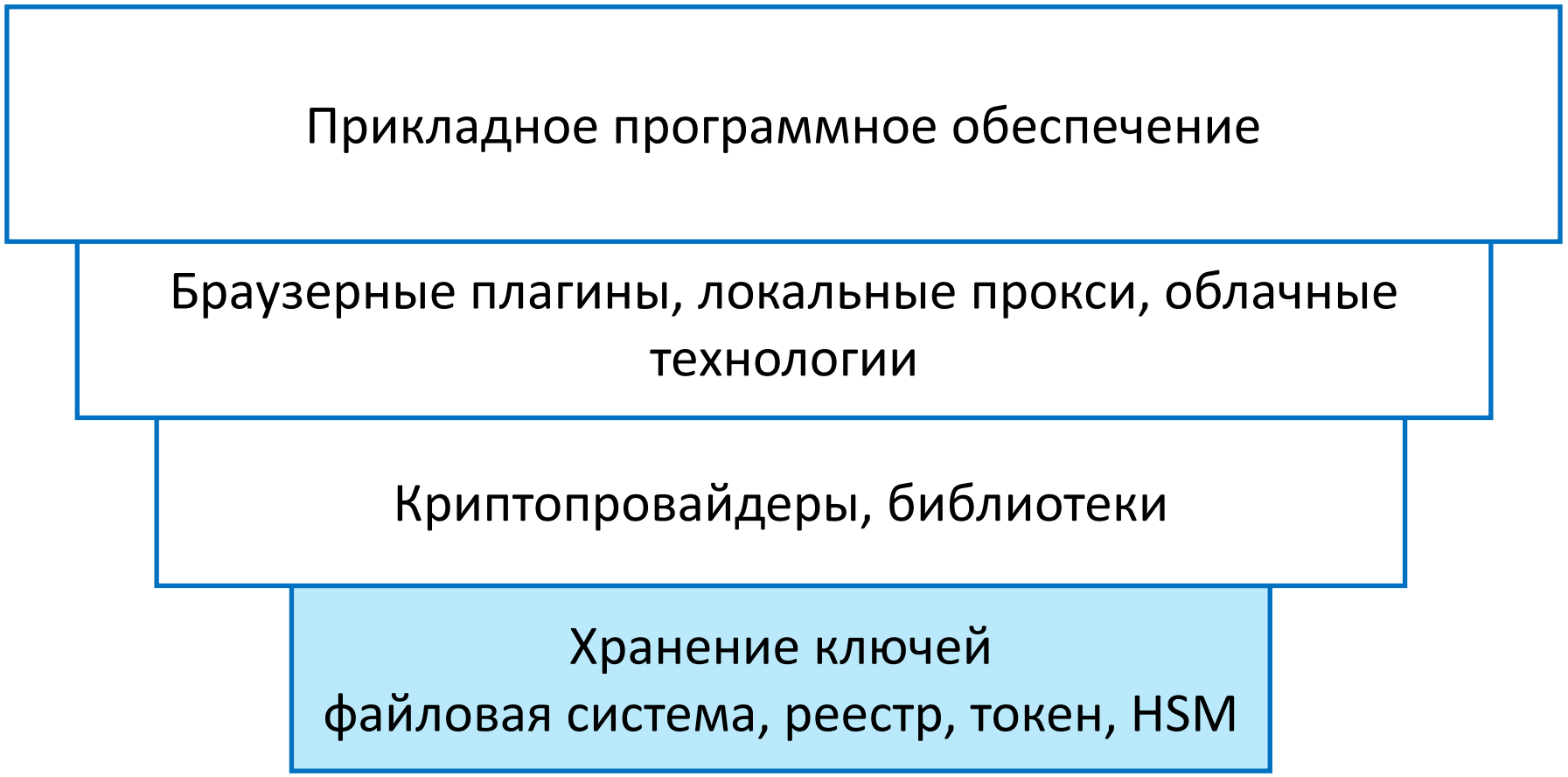
Определяющие факторы

- Невысокие требования к квалификации пользователя
- Удобство часто важнее безопасности
- Миграция информационных систем «в браузер»
- Увеличение доли мобильных платформ

Структура информационной системы



Структура информационной системы



Хранение ключей

Локальное хранение ключей пользователя:

- файловая система, реестр
- мобильные устройства.

В данном случае мобильные устройства представляют собой ключевое хранилище, к которому предъявляются те же требования безопасности, что и к отчуждаемому носителю.

Хранение ключей

Хранение ключей на отчуждаемых носителях

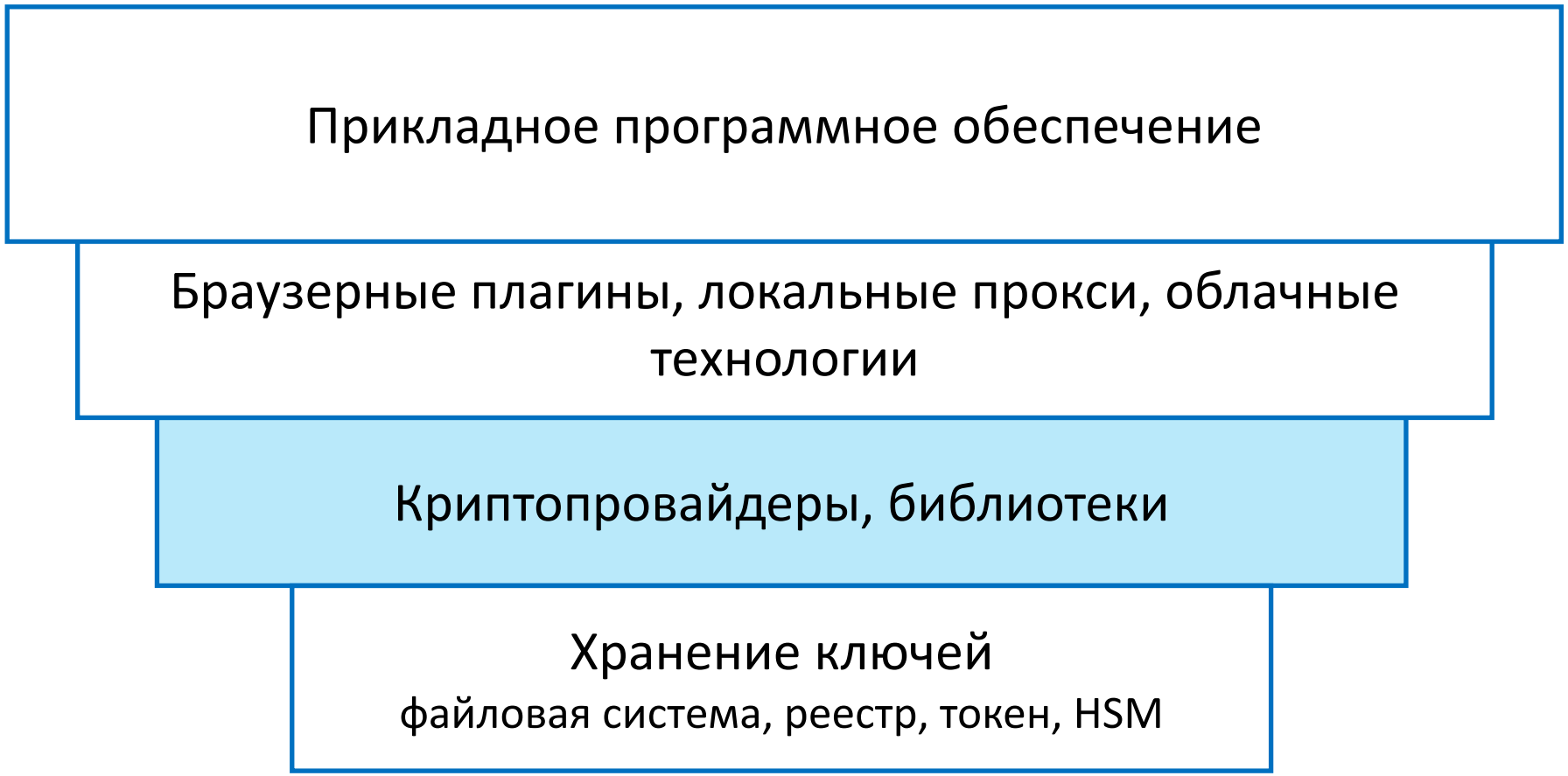
- Хранение ключа с возможностью экспорта.
- Носитель с криптографией «на борту» без возможности экспорта ключа.
- Автономные носители с возможностью ввода пин-кода на устройстве, устройства класса trustscreen.
- Носители с поддержкой технологии ФКН.

Хранение ключей

Хранение ключей на удаленном сервере.
Облачные технологии.

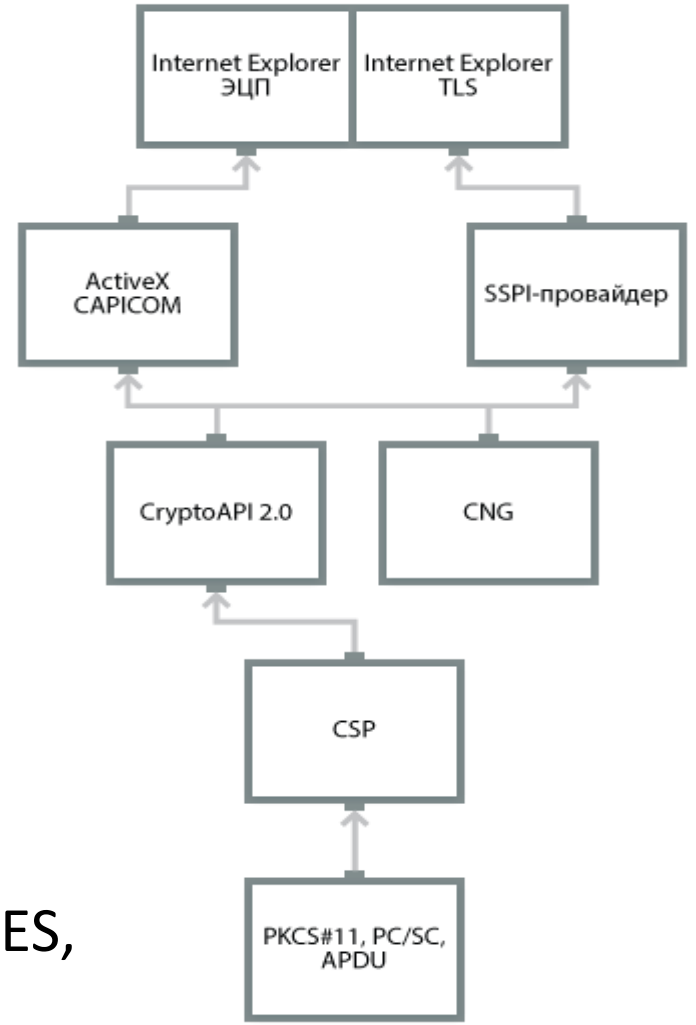
- HSM
- Защищенная БД

Структура информационной системы



Криптопровайдеры

- Служба хранения ключей
- Реализация криптографических алгоритмов
- Реализация криптографических протоколов
- Интерфейсы CryptoAPI 1.0, CryptoAPI 2.0, .COM
- Определяются стандартами: ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2012, RFC 4357, методическими рекомендациями ТК26, а также стандартами DH, RSA, AES, DSS, CYLINK_MEK, MD5, SHA, DES, Triple DES, Skipjack, KEA, CAST и другими.

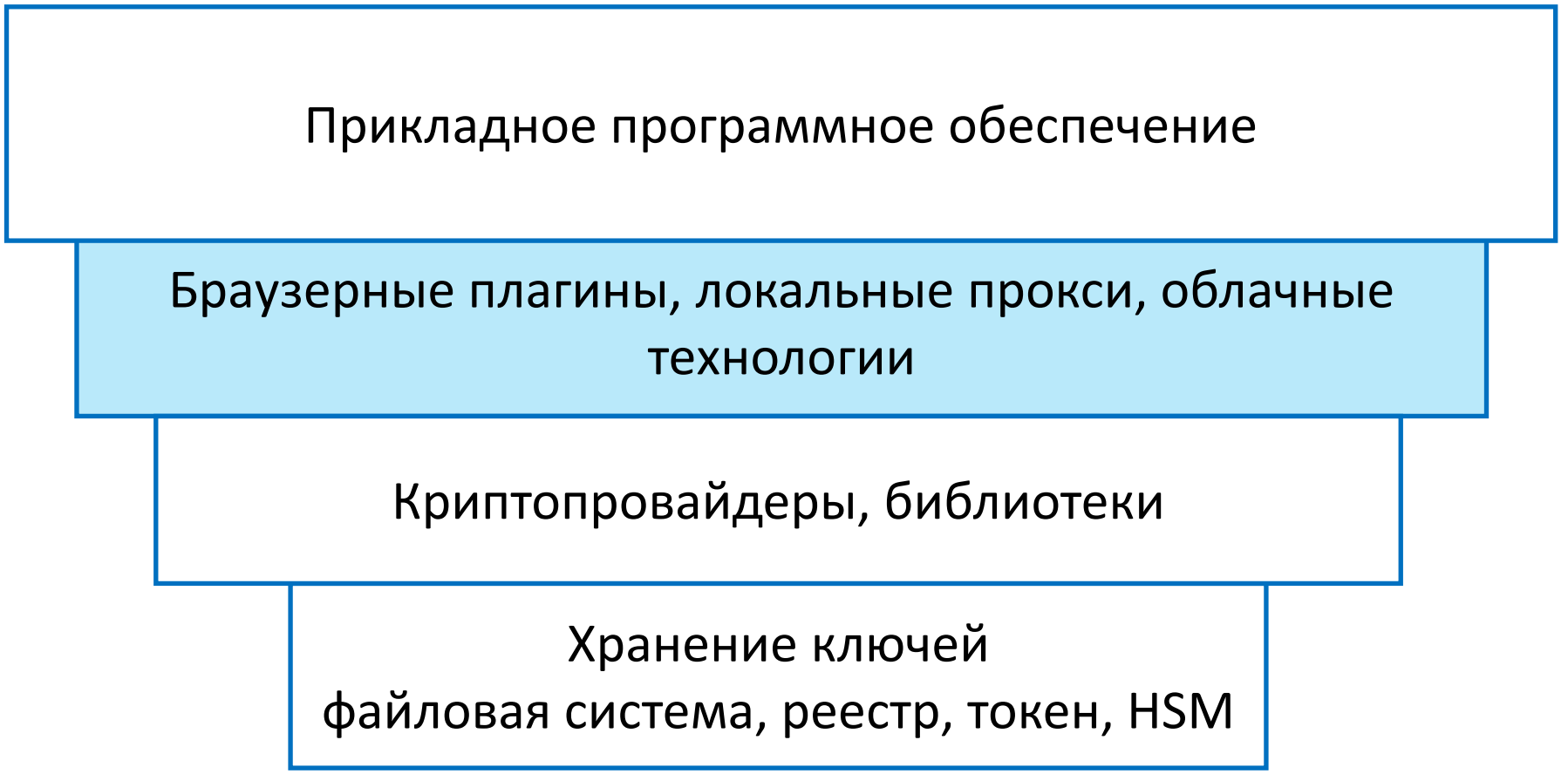


Криптографические библиотеки

* **Openssl-style**
* **PKCS#11**
* **NSS**
* **Проприетарные библиотеки**

- Обеспечивают доступ к криптографическим устройствам.
- Реализуют криптоалгоритмы, криптопротоколы.
- Обеспечивают доступ к ключам.
- Возможность как поддержки аппаратных устройств, так и только программной реализации.
- Поддержка стандартов
  Blowfish, Camellia, DES, RC2, RC4, RC5, IDEA, AES, ГОСТ 28147-8, MD5, MD2, SHA, MDC-2, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012, RSA, DSA,
  Diffie-Hellman key exchange, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 и других.

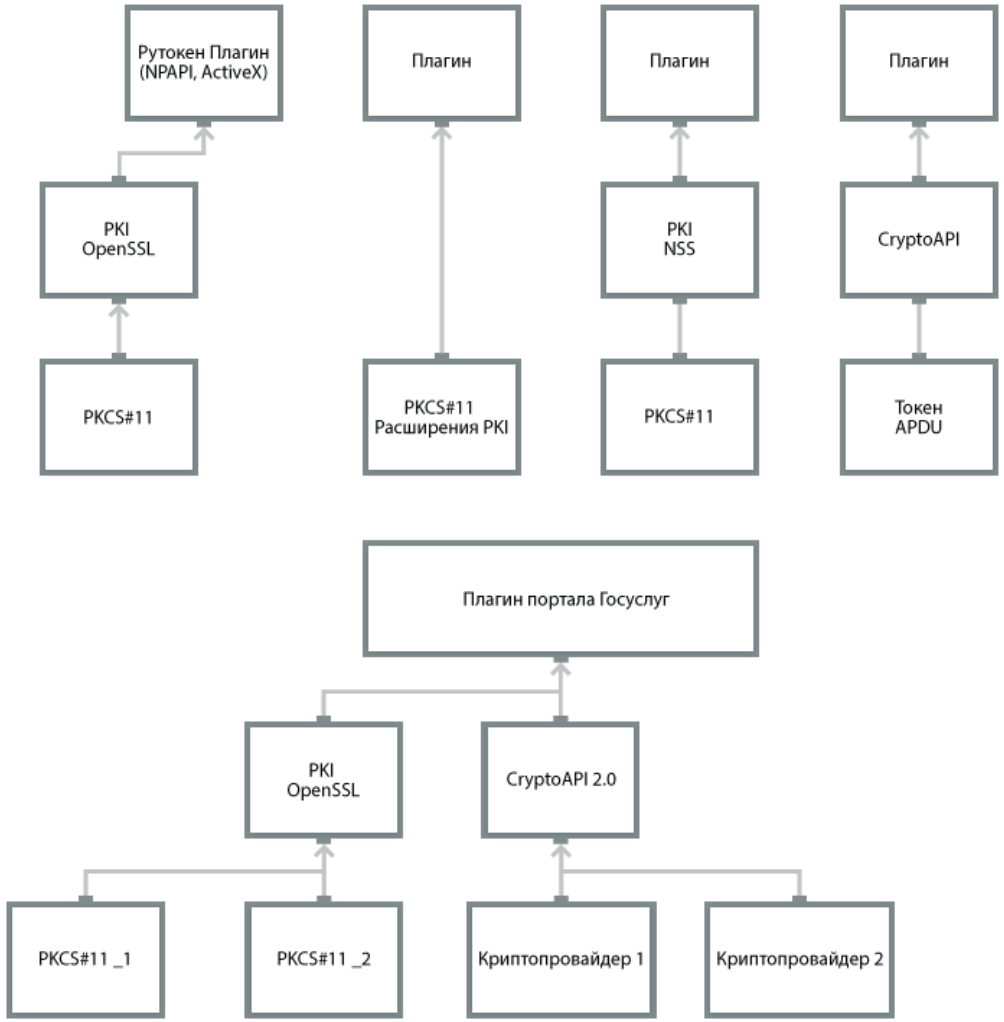
Структура информационной системы



Браузерные плагины

Браузерные плагины позволяют вызвать нативные библиотеки из скриптов Web-страницы.

- Используют в качестве криптоядра криптопровайдер, библиотеки PKCS#11, OpenSSL, аппаратные СКЗИ.
- Обеспечивают кроссплатформенность на базе PKCS#11.
- Могут поддерживаться различными браузерами.
- Прозрачное использование для пользователя.

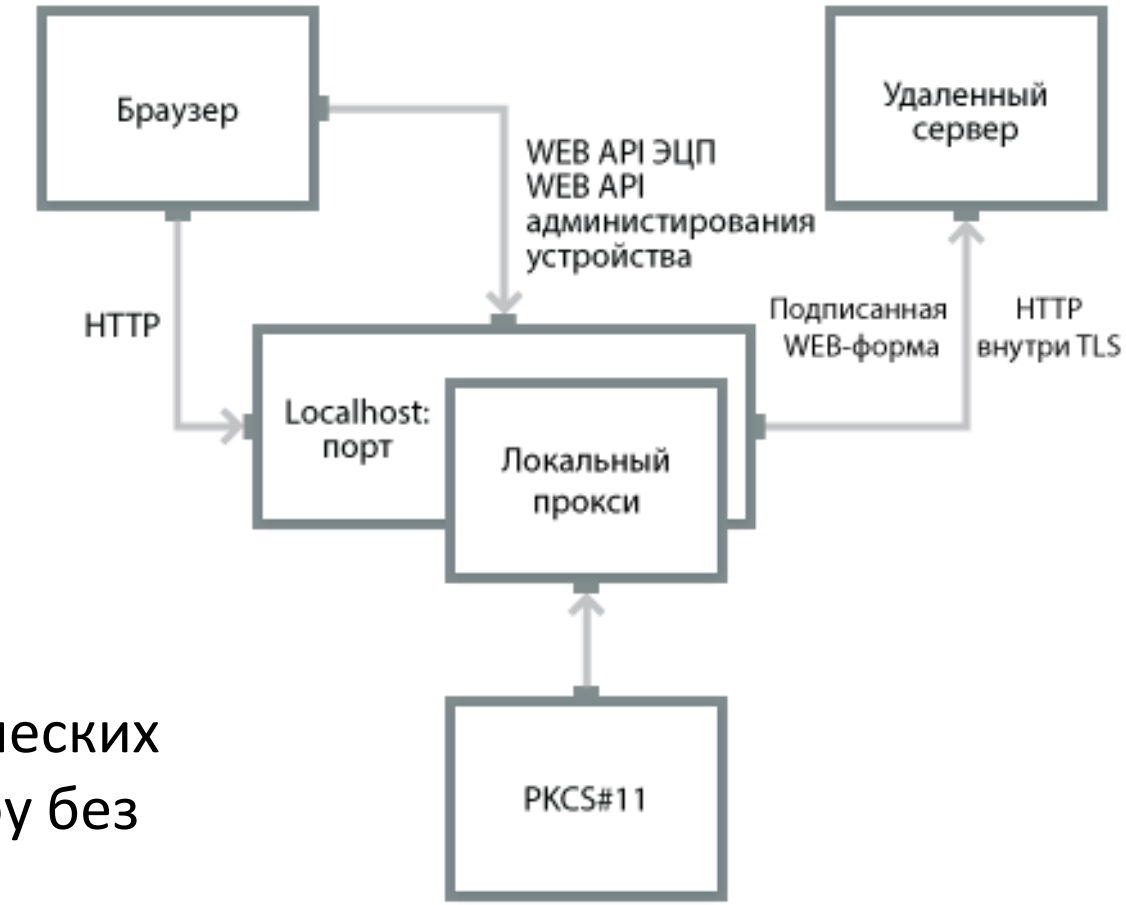


Смешанные браузерные решения

- Интерфес WebUSB позволяет реализовать драйверы USB-устройств на JavaScript, таким образом трасса вызовов из браузера проходит напрямую на уровень криптографического USB-устройства.
- Реализация при помощи встроенных в браузер JavaScript-функций форматов ЭП (XMLDSig, CMS) с вызовом функций электронной подписи из нативных библиотек
- JavaScript-библиотека с полноценной реализацией криптографических примитивов.
- Обращение из браузера как к локальному средству ЭП, так и к удаленному серверу для «упаковки» «сырой» подписи, вычисленной на рабочем месте пользователя.

Локальные прокси

- Установка TLS-туннеля с удаленным сервером.
- Передача прикладного уровня между приложением и удаленным сервером
- Применяется на различных платформах, в том числе мобильных.
- Не требует инсталляции.
- Возможность выполнения криптографических запросов (SOAP) через локальную службу без обращения к удаленному серверу



Электронная подпись в облаке

- Ключи электронной подписи пользователей хранятся на удаленном защищенном сервере (HSM).
- Подпись формируется на удаленном сервере, ключ подпись не покидает сервер.
- Могут использоваться различные варианты аутентификации.

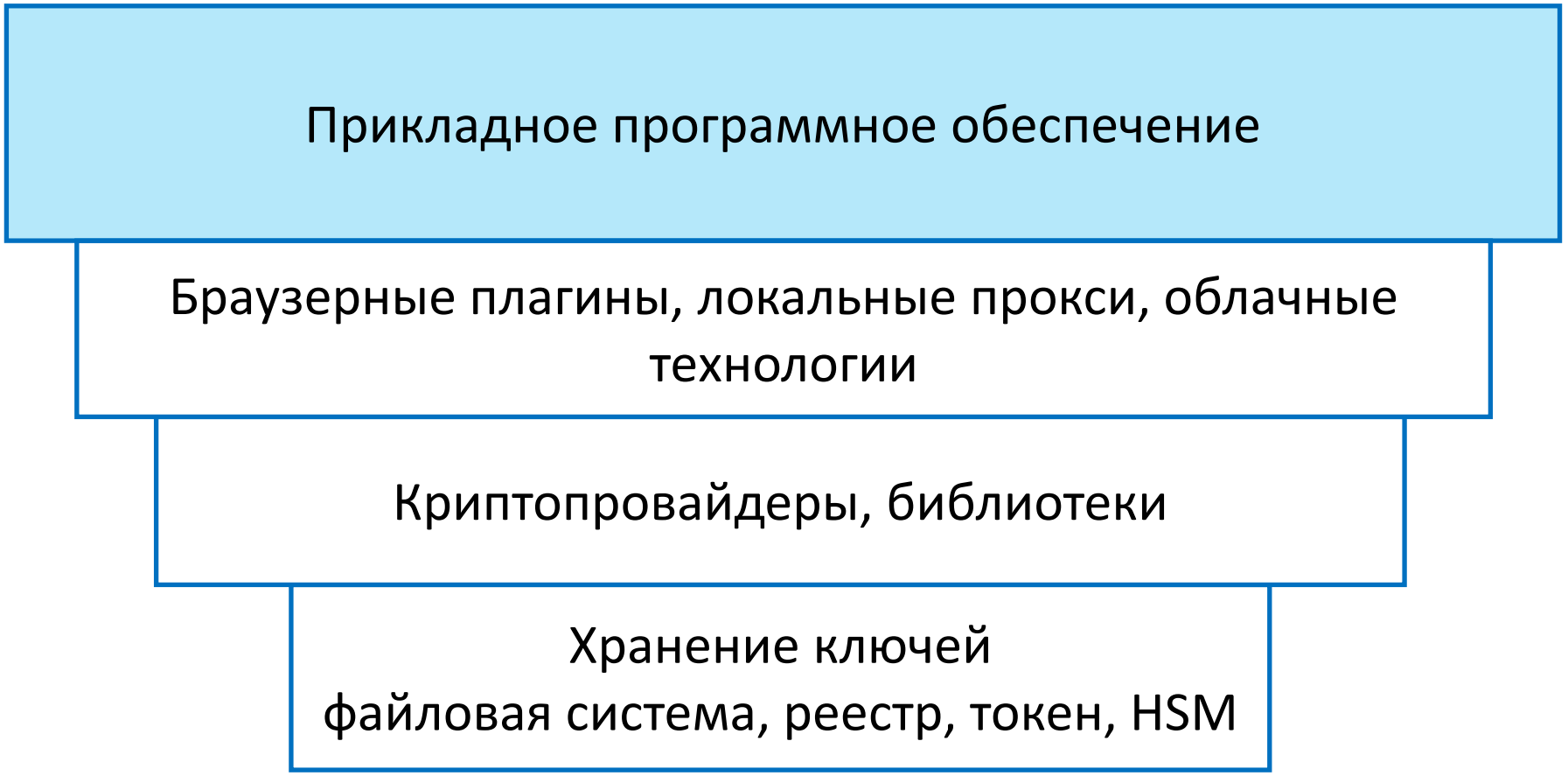
Плюсы:

- Надежная защита ключей ЭП пользователя.
- Поддержка мобильными устройствами.
- Не обязательна установка СКЗИ на рабочем месте пользователя.

Минусы:

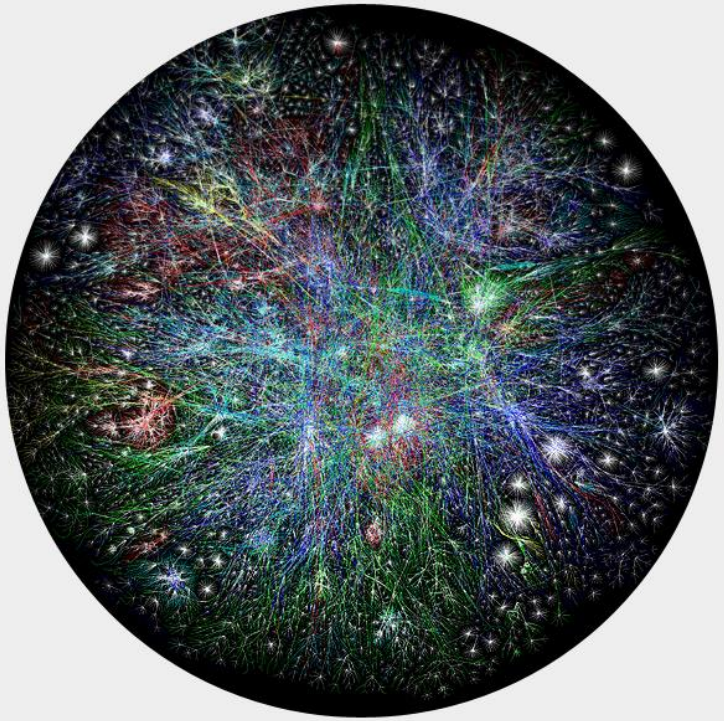
- Необходимость защиты канала, по которому передаются электронные документы.
- Сложный баланс между удобством и защищенностью системы.

Структура информационной системы



Прикладное программное обеспечение

- Системы электронного документооборота
- Системы дистанционного банковского обслуживания
- Online-сервисы с высокими требованиями к аутентификации пользователей

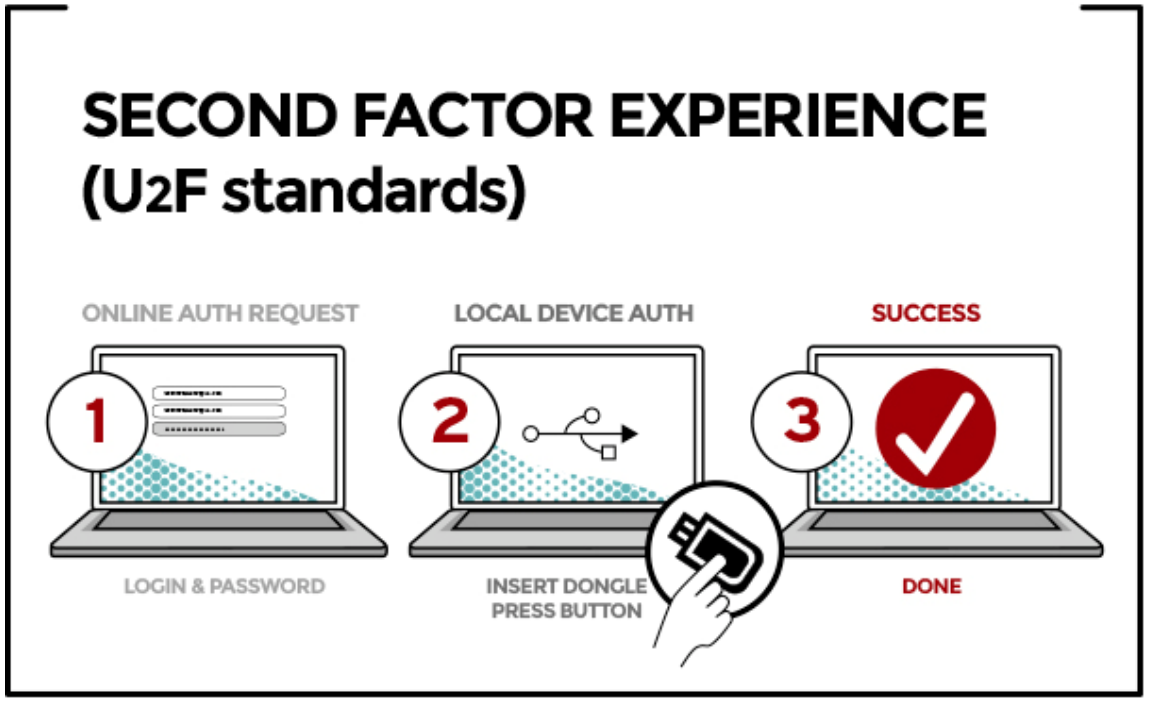


Участники FIDO Alliance

MasterCard

- Alibaba Group
- Nok Nok Labs
- NTT DOCOMO
- NXP
- Oberthur Technologies
- Qualcomm
- USAA
- Bank of America
- CruicialTec
- Discover
- Egis Technology
- IdentityX
- ING
- ARM
- Dell
- BlackBerry
- Aktiv-Soft Company
- Gemalto
- Goldman Sachs
- LG Electronics
- VASCO
- NIST

Двухфакторная аутентификация по протоколу U2F



- Аутентификация пользователя в онлайн-сервисах, на веб-сайтах при помощи физического U2F-устройства (USB-токен, NFC-брелок).
- Вся криптография на стороне сервера, браузера и U2F-устройства. Пользователю не приходится ставить дополнительное ПО.
- Операция аутентификации выполняется при помощи Javascript API встроенного в браузер, нативного API мобильных систем.
- Поддержка U2F в Google Chrome, YouTube, Linux PAM, OpenSSH, WordPress (software), Dropbox.

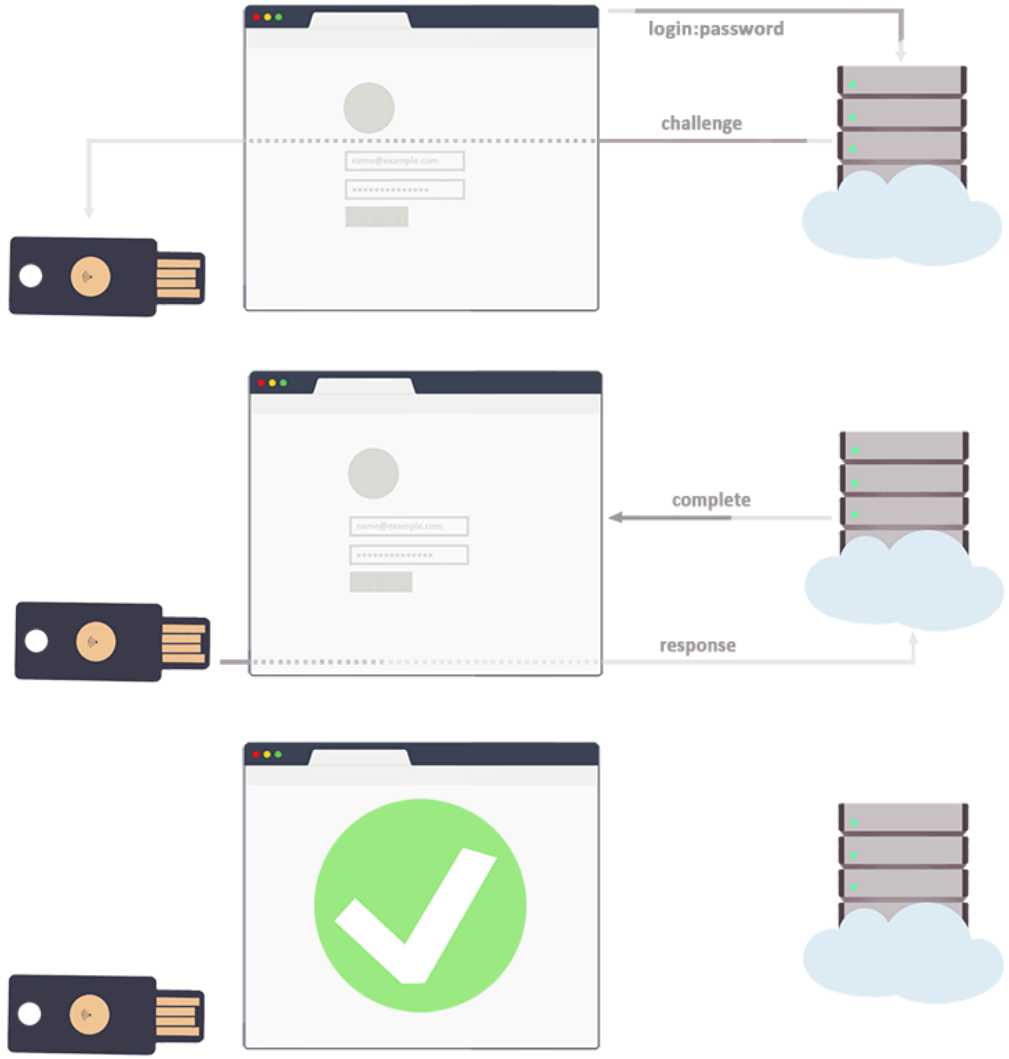
Двухфакторная аутентификация по протоколу U2F

Регистрация устройства

- Перевод U2F-устройства в активное состояния нажатием кнопки/касанием сенсора.
- Генерация ключевой пары на U2F-устройстве.
- Обмен открытыми ключами с браузером и сервером.

Аутентификация

- Перевод U2F-устройства в активное состояния нажатием кнопки/касанием сенсора.
- Подпись данных от сервера на U2F-устройстве.
- Проверка подписи на сервере.



Двухфакторная аутентификация по протоколу U2F

Протокол U2F обеспечивает защиту от следующих атак:

- Использование одной ключевой пары на нескольких онлайн-сервисах.
- Атака Man-In-The-Middle во время аутентификации.
- Копирование ключа ЭП на другое U2F-устройство.
- Выполнение аутентификации без согласия пользователя вредоносным ПО.

«PKI-FIDO»

- Каждое U2F-устройство обладает ключевой парой «аттестации», распределенной среди партии устройств одного вендора.
- Каждый открытый ключ U2F-устройства на шаге регистрации подписывается ключом ЭП «аттестации».
- При наличии инфраструктуры открытых ключей, онлайн-сервисы могут проверить, какому вендору принадлежит U2F-устройство, прошло ли оно сертификацию/аттестацию.
- Вендор может определять, с какими устройствами он готов работать.

Краткие выводы

- Активно развиваются технологии для работы с криптографией из контекста браузера
- Крупные проекты требуют, чтоб криптография и электронная подпись работали бесшовно, «из коробки»
- Массовый рынок требует простых, легких решений

Вопросы

Контактная информация

Электронная почта:

Общие вопросы – info@rutoken.ru

Тех.поддержка – hotline@rutoken.ru

Отдел продаж – sales@rutoken.ru

Сайты:

www.rutoken.ru

www.aktiv-company.ru

Телефон:

(495) 925-77-90