РУТОКЕН

PKI-Forum Россия 2014

16 – 18 сентября 2014 года

Обзор технологических подходов к построению СКЗИ и средств ЭП. Архитектуры и интерфейсы.

Горелов Дмитрий Львович

Коммерческий директор компании «Актив»

Компания Актив

Введение

- Рассматриваются СКЗИ для работы с ЭП, защиты клиент-серверных соединений (TLS) и шифрования передаваемых данных.
- Не включены в обзор: VPN, средства шифрования файловой системы, серверные решения и УЦ.

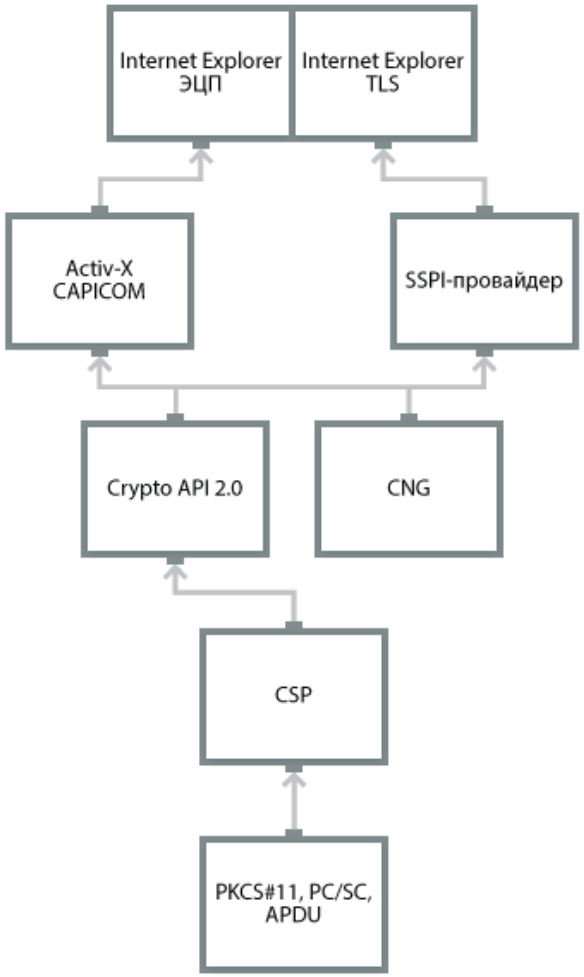
Классификация

- По технологиям интеграции в прикладные системы и архитектуре
- По интерфейсам, которые предоставляют СКЗИ для встраивания в приложения

Введение

- Криптопровайдеры
- Библиотеки
- Локальные прокси
- Браузерные плагины
- Браузеры
- Фреймворки, платформы, интерпретаторы
- Настольные криптографические приложения
- Аппаратные решения

Криптопровайдеры



Спецификации	Microsoft CSP, Microsoft CNG, Crypto API 1.0 -> Crypto API 2.0
Платформы	Семейство Windows. Есть порт на Linux, Mac OS X, iOS, Android
Алгоритмы и Протоколы	ЭЦП, шифрование, хэш-функция, имитозащита, HMAC, VKO, TLS, EAP-TLS и др.
Интеграция с PKI	X.509, PKCS#10, CMS, CRL, OCSP, TSP и др.
Механизмы ЭЦП	Нативный программный интерфейс (Си-style), встраивание в приложения
Механизмы аутентификации	Клиентская аутентификация в рамках TLS, KERBEROS-аутентификация в домене, механизмы на базе ЭЦП
TLS-ГОСТ	Встраивание в системный TLS

Криптопровайдеры

Форматы защищенных сообщений	PKCS#7, CMS, XMLDSig, CADES, PDF signature, MS Office Signature
Интеграция с браузером	ЭЦП в IE через ActiveX CAPICOM, TLS в IE через встраивание в SSPI-провайдер
USB-токены и смарт-карты	Хранилища ключей и сертификатов, использование аппаратной реализации алгоритмов, работа через PKCS#11 и PC/SC.
Поддержка приложений	IE, Microsoft Office, Microsoft Outlook Express, Microsoft Outlook, Microsoft Word/Excel, Microsoft Authenticode, Microsoft RDP, Microsoft Certification Authority, Microsoft IIS, Microsoft Exchange, Microsoft Terminal Server, Winlogon, Adobe Reader и т.д.

- КриптоПро CSP
- VipNet CSP
- Signal-COM CSP
- КриптоПро Рутокен CSP
- Валидата CSP

Криптопровайдеры

Вопросы, проблемы

- Отсутствие изначальной кроссплатформенности
- Установка с правами администратора, настройка
- Установка обновления ОС может потребовать обновления провайдера

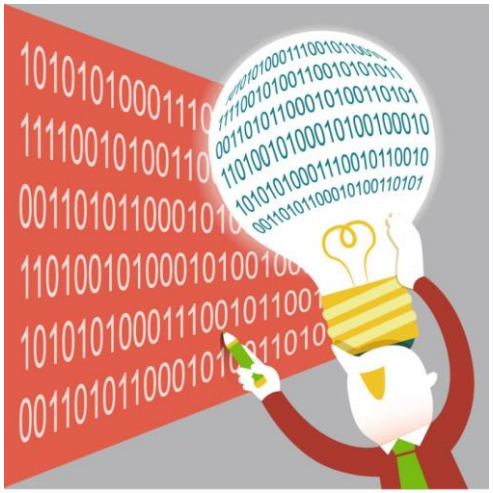
Криптопровайдеры

Плюсы

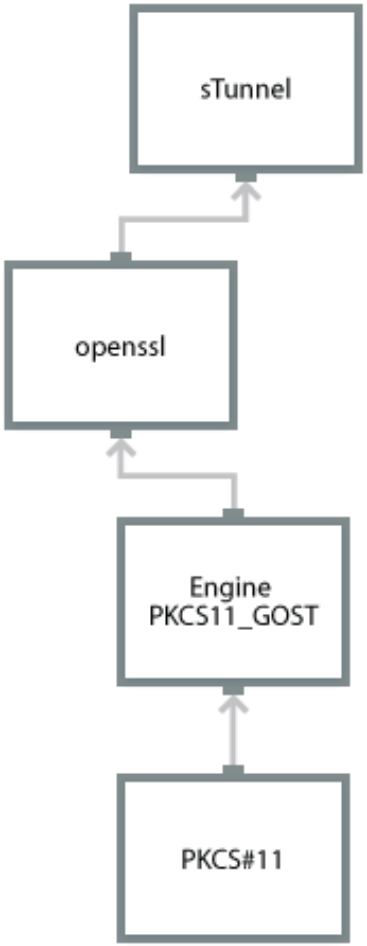
- Широчайший охват Windows-приложений
- Богатый инструментарий для разработчиков
- Апробированная на большом количестве проектов технология
- Стандарт de facto

Библиотеки

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



Openssl-style



Спецификации	Openssl API
Платформы	Семейство Windows, Linux, Mac OS X, iOS, Android
Алгоритмы и Протоколы	ЭЦП, шифрование, хэш-функция, имитозащита, HMAC, VKO , TLS
Интеграция с PKI	X.509, PKCS#10, CMS, CRL, OCSP, TSP и др.
Механизмы ЭЦП	Нативный программный интерфейс, Си-style
Механизмы аутентификации	Клиентская аутентификация в рамках TLS, собственные механизмы на базе ЭЦП
TLS-ГОСТ	TLS с российской криптографией поддержан в библиотеке (в случае использования openssl в качестве браузерного крипто-движка), TLS-прокси на базе openssl.

Openssl-style

Форматы защищенных сообщений	PKCS#7, CMS, XMLSec
Интеграция с браузером	Через TLS-прокси Через проприетарные плагины В Chromium openssl один из возможных криптодвижков
USB-токены и смарт-карты	Хранилища ключей и сертификатов, использование аппаратной реализации алгоритмов, работа через PKCS#11.
Приложения (с поддержкой ГОСТ)	OpenVPN, Apache, sTunnel, Nginx, Postgre SQL Проприетарные приложения

- МагПро КриптоПакет
- ЛирССЛ
- openssl + engine PKCS11_GOST + Рутокен ЭЦП
- openssl (несерт.)

Openssl-style

Вопросы, проблемы

- Openssl не поддерживается Windows-приложениями
- Необходимость патчить СПО, которое поддерживает openssl, для включения российской криптографии

Openssl-style

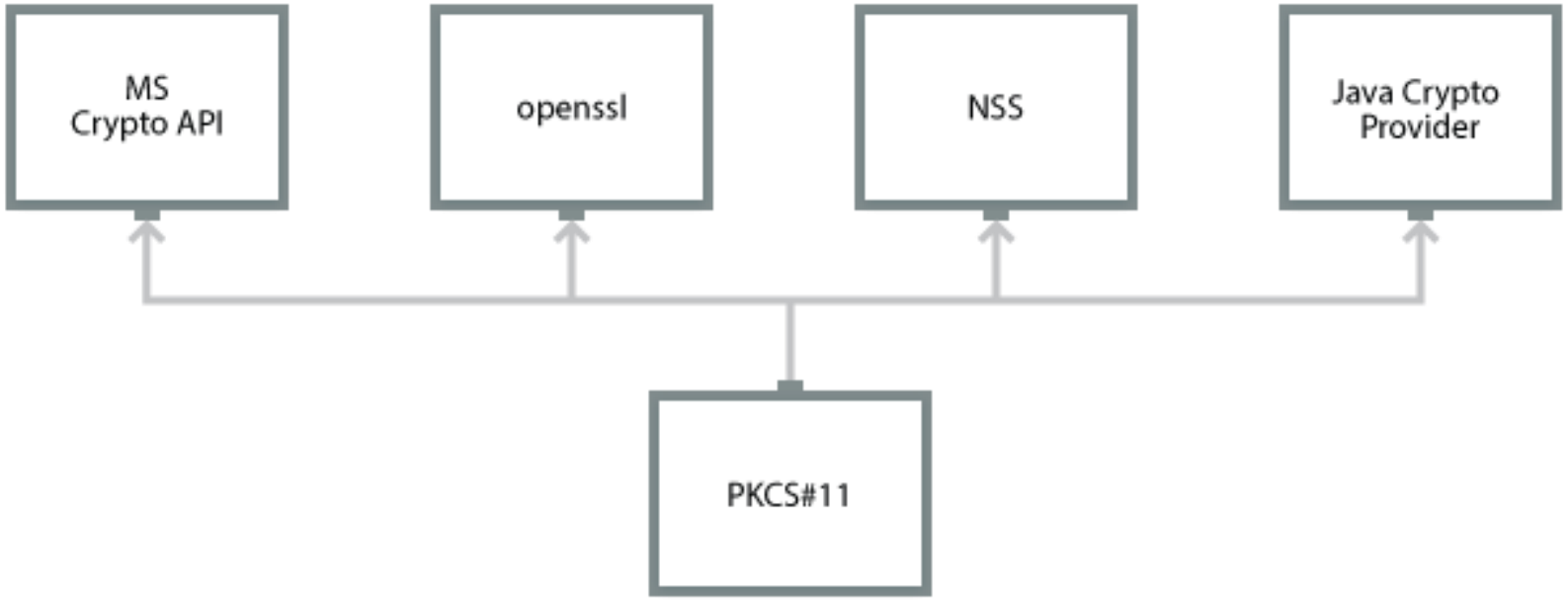
Плюсы

- Кроссплатформенность
- Использование в большом количестве проектов
- Можно делать приложения, не требующие инсталляции
- Широкий спектр приложений СПО, на базе которых можно делать защищенные сертифицированные продукты

PKCS#11

PKCS#11 платформонезависимый программный интерфейс доступа к криптографическим устройствам (USB-токены, смарт-карты и т.д).

С версии 2.30, поддерживаются ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94, ГОСТ 28147-89. Есть draft с поддержкой ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012.



PKCS#11

- Доступ к устройству
- Функции записи/чтения произвольных данных
- Работа с ключами (поиск, создание, удаление, импорт, экспорт)
- Функции работы с сертификатами (поиск, импорт, экспорт)
- Хэширование и подпись
- Функции шифрования
- Выработка ключей согласования
- Функции экспорта/импорта сессионного ключа

PKCS#11

- Стандарт PKCS#11 содержит полный набор криптопримитивов, пригодный для реализации форматов (PKCS#7/CMS, PKCS#10, X.509 и др.) и протоколов (TLS, IPSEC , openvpn и др.).
- Использование PKCS#11 обеспечивает совместимость ПО различных вендоров при работе с токенами (смарт-картами)
- Модули PKCS#11 бывают без поддержки аппаратных устройств, чисто программные.

Библиотеки

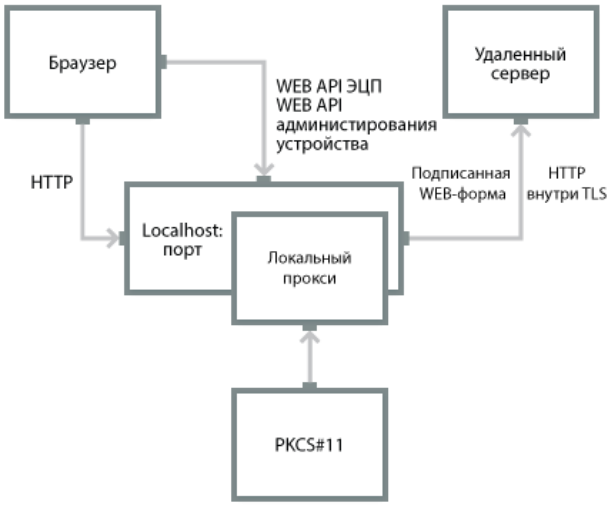
NSS

- Atoken (патч для NSS)
- NSS от «ЛИССИ-Софт»
- NSS от «Крипто-Про»

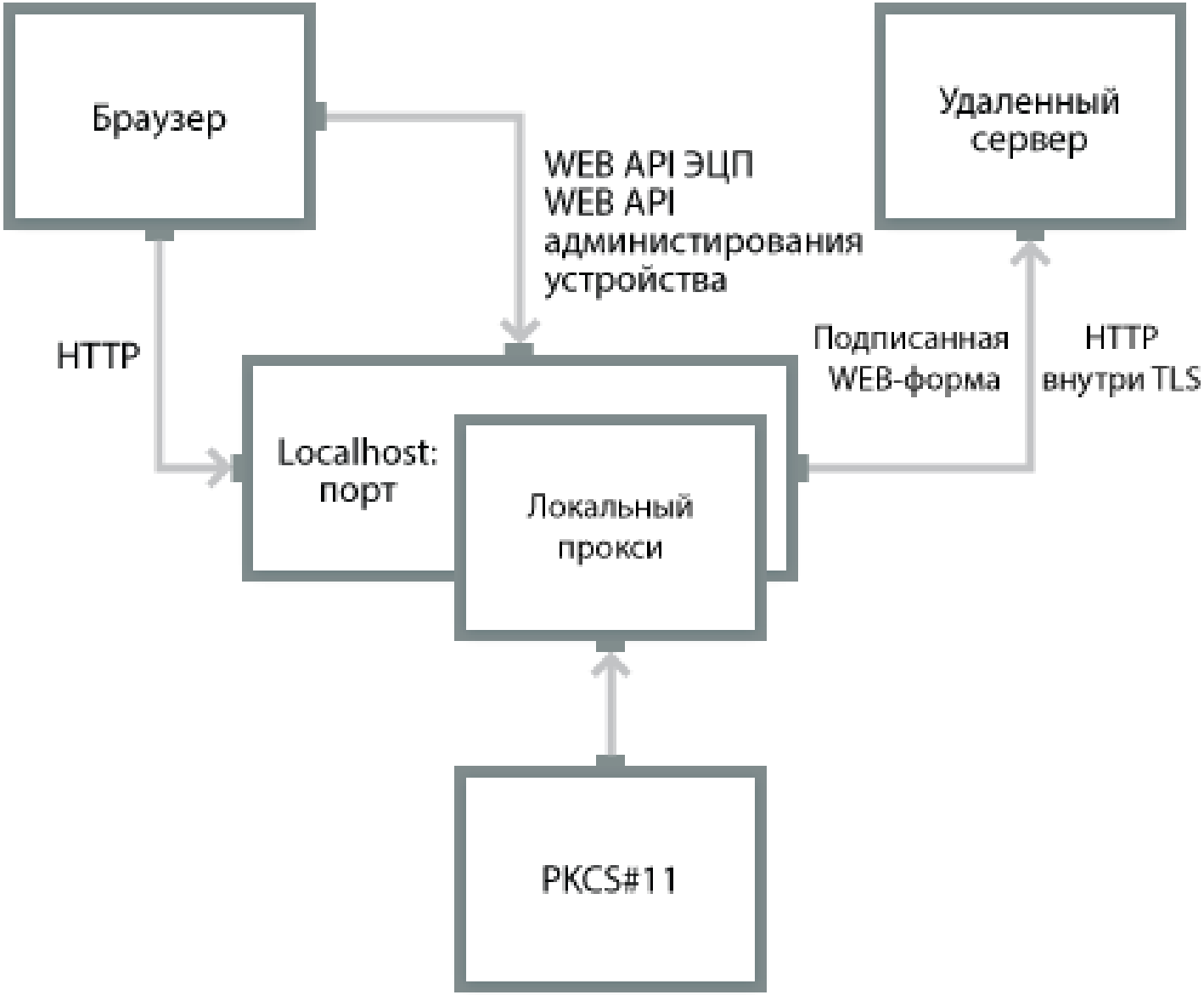
Проприетарные библиотеки

- Агава Си
- Крипто Си
- iCrypto
- Крипто-КОМ 3.3 и др.

Локальные прокси



Спецификации	-
Платформы	Семейство Windows, Linux, Mac OS X. На базе СПО iOS, Android
Алгоритмы и Протоколы	ЭЦП, шифрование, хэш-функция, имитозащита, HMAC, TLS.
Интеграция с PKI	X.509, PKCS#10, CMS, CRL, OCSP, TSP
Механизмы ЭЦП	Подпись WEB-форм при прохождении траффика WEB API
Механизмы аутентификации	Клиентская аутентификация в рамках TLS
TLS-ГОСТ	Через механизм проксирования


Браузер
Удаленный сервер
WEB API ЭЦП
WEB API
администирования
устройства
HTTP
Подписанная
WEB-форма
HTTP
внутри TLS
Localhost:
порт
Локальный
прокси
PKCS#11

Локальные прокси

Форматы защищенных сообщений	PKCS#7, CMS
Интеграция с браузером	Через механизм проксирования
USB-токены и смарт-карты	Хранилища ключей и сертификатов, использование аппаратной реализации алгоритмов, работа через PKCS#11 и PC/SC.
Поддержка приложений	Браузеры WEB-сервера RDP Почтовые клиенты и сервера

- МагПро КриптоТуннель
- Inter-PRO
- VPNKey-TLS
- LirTunnel
- КриптоПро sTunnel
- sTunnel

Локальные прокси

Вопросы, проблемы

- Прокси должен быть запущен и приложение должно «о нем знать»
- Использование нестандартных портов и http://localhost
- Ограничения на разработку web-сайта (относительные ссылки)
- Вопросы конфигурирования

Локальные прокси

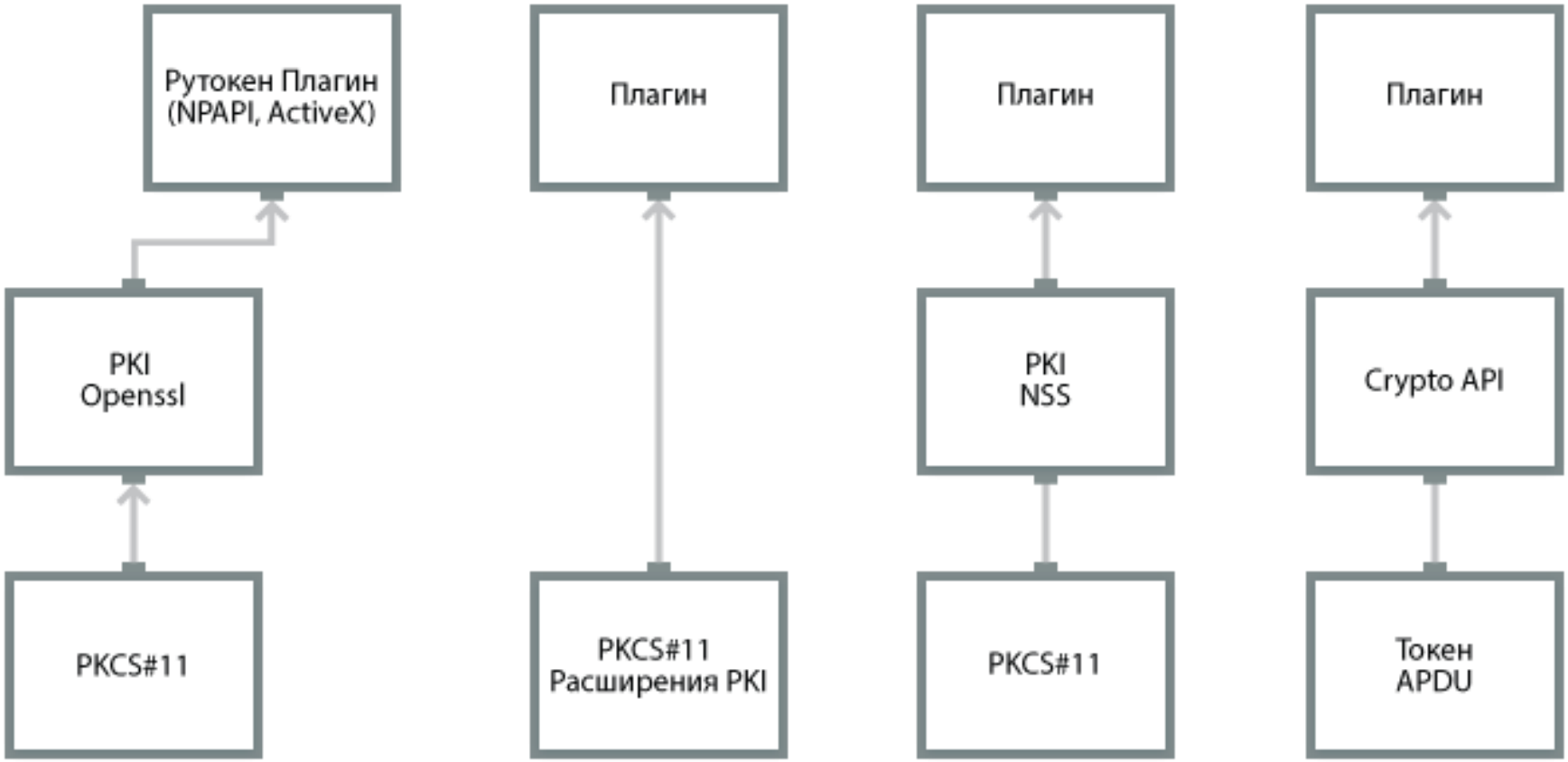
Плюсы

- универсальная технология, можно не бояться устаревания
- Кроссбраузерность, кроссплатформенность, поддержка всех WEB-серверов без модификации
- не требует инсталляции
- поддержка различных прикладных протоколов

Браузерные плагины

Спецификации	-
Платформы	Семейство Windows, Linux, Mac OS X.
Алгоритмы и Протоколы	ЭЦП, шифрование, хэш-функция, имитозащита, HMAC.
Интеграция с PKI	X.509, PKCS#10, CMS, CRL, OCSP*, TSP*
Механизмы ЭЦП	Программный интерфейс для использования в JavaScript
Механизмы аутентификации	ЭЦП случайных данных
TLS-ГОСТ	-

Браузерные плагины



Браузерные плагины

Форматы защищенных сообщений	PKCS#7, CMS, XMLDSig*, CADES*
Интеграция с браузером	ActiveX (для IE) NPAPI Native Messaging (Chromium)
USB-токены и смарт-карты	Хранилища ключей и сертификатов, использование аппаратной реализации алгоритмов, работа через PKCS#11, Crypto API.
Поддержка приложений	Браузеры

- КриптоПро ЭЦП Browser plugin
- eSign-PRO
- КриптоПлагин Лисси
- Плагин портала ГосУслуг
- JC-WebClient
- Рутокен Плагин
- КриптоАРМ Browser plugin

Браузерные плагины

Вопросы, проблемы

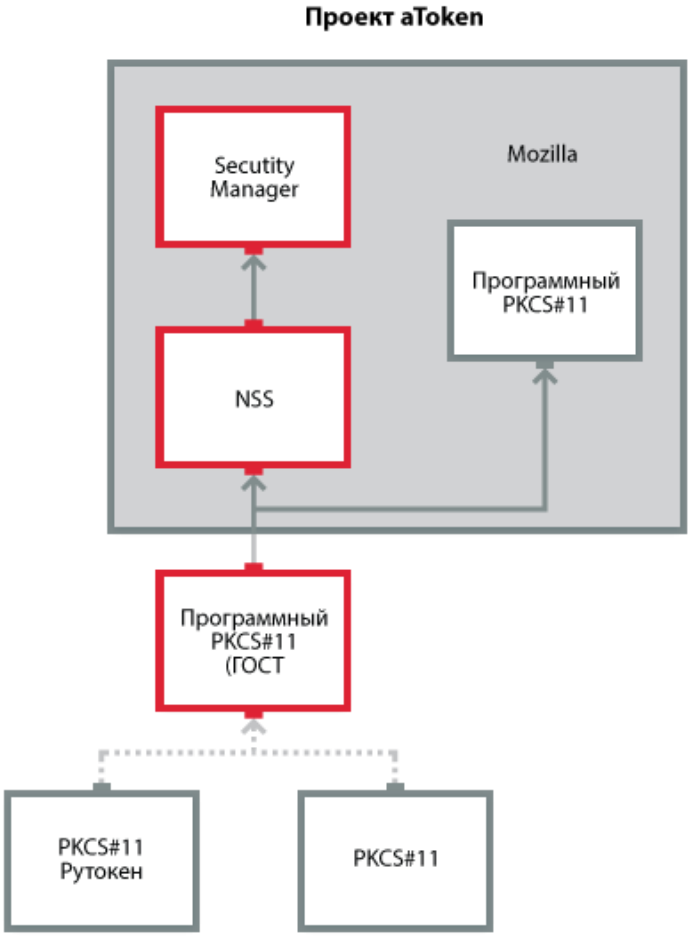
- отсутствие TLS
- удаление NPAPI из Chromium
- браузеры на мобильных платформах не поддерживают плагины
- настройки безопасности браузера могут блокировать исполнение плагина

Браузерные плагины

Плюсы

- кроссплатформенность для плагинов на базе PKCS#11
- кроссбраузерность
- плагины на базе PKCS#11 не требуют установки СКЗИ
- прозрачное использование для пользователя

Браузеры с российской криптографией



Спецификации	NSS с использованием PKCS11-токенов, программных и аппаратных, есть варианты на openssl
Платформы	Семейство Windows, Linux, Mac OS X, iOS, Android
Алгоритмы и Протоколы	ЭЦП, шифрование, хэш-функция, имитозащита, HMAC, VKO, TLS
Интеграция с PKI	X.509, PKCS#10, CMS, CRL
Механизмы ЭЦП	Вызов из JavaScript встроенных в браузер функций
Механизмы аутентификации	Клиентская аутентификация в рамках TLS, механизмы на базе ЭЦП
TLS-ГОСТ	Встроен в библиотеку и поддерживается браузером

Браузеры с российской криптографией

Форматы защищенных сообщений	PKCS#7, CMS
Интеграция с браузером	100%
USB-токены и смарт-карты	Хранилища ключей и сертификатов, использование аппаратной реализации алгоритмов, работа через PKCS#11 и PC/SC.
Поддержка приложений	-

- Mozilla FireFox, Chromium от Лисси
- Проект Atoken от R-Альфа (Mozilla FireFox)
- КриптоFox (на базе КриптоПро CSP)

Браузеры с российской криптографией

Вопросы, проблемы

- обновление браузера
- нужно переучивать пользователя на использование «нестандартного» браузера
- сертификация (нет прецедентов)

Браузеры с российской криптографией

Плюсы

- кроссплатформенность
- прозрачность использования для пользователя
- нет ограничений для разработчиков серверной части
- возможно создание Portable-версий

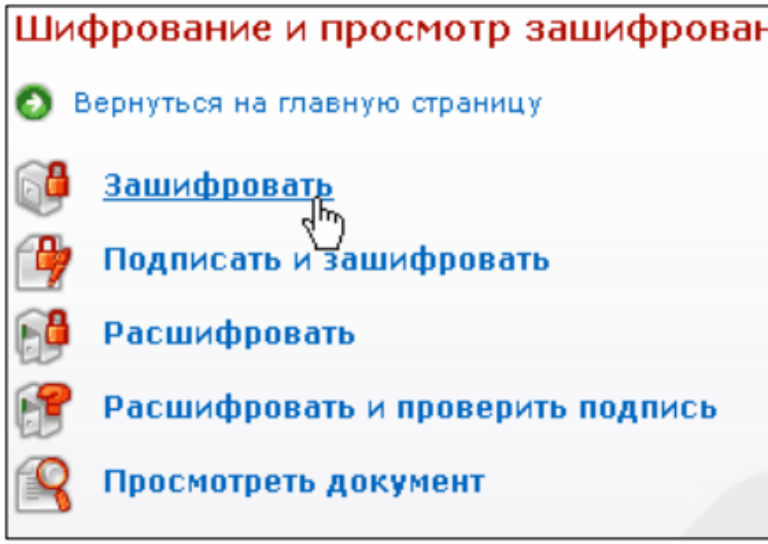
Фреймворки, платформы, интерпретаторы

- **Microsoft.NET**
  - КриптоПро .NET
- **Java**
  - КриптоПро JCP
  - Signal-COM JCP
  - Java-библиотеки
- **PHP**
- **JavaScript**

Настольные криптографические приложения

Программные средства предоставляющие пользовательский интерфейс для выполнения криптографических и сервисных операций:

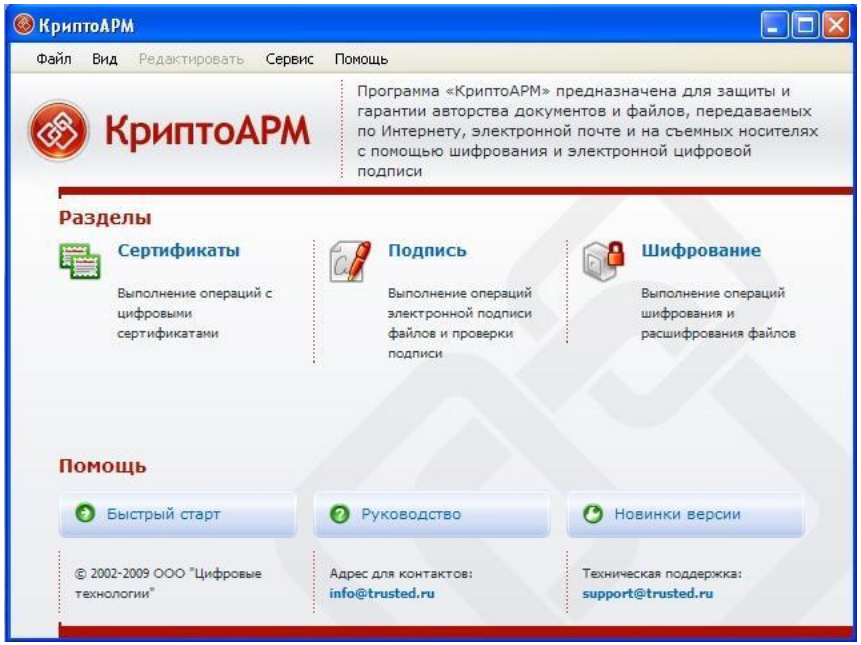
- подпись файла
- проверка подписи под файлом, построение цепочки и проверка списка отзыва и т.д.
- зашифрование файла
- расшифрование файла
- поиск и выбор сертификата пользователя
- просмотр сертификата
- ведение базы сертификатов респондентов
- генерация ключевой пары, формирование запроса на сертификат
- удаление ключевой пары
- импорт/экспорт сертификатов (корневых, пользовательских, респондентов)



Настольные криптографические приложения

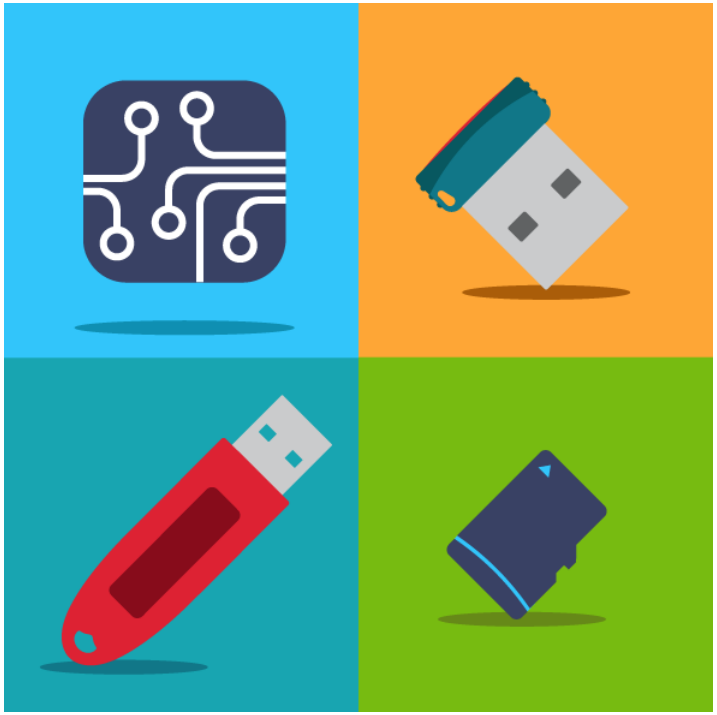
Примеры решений:

- КриптоАРМ
- КриптоНУЦ
- File-PRO, Admin PKI
- VipNet Crypto File
- Блокхост ЭЦП



Аппаратные средства

- **USB-токены**
- **Смарт-карты**
- SD-карты
- Trustscreen-решения
- Bluetooth-токены
- HSM



Заключение

- **Криптопровайдеры**
- **Библиотеки**
- **Локальные прокси**
- **Браузерные плагины**
- Настольные криптографическ ие приложения
- Фреймворки, платформы, интерпретаторы
- Браузеры
- **Аппаратные решения**

Контактная информация

Горелов Дмитрий

+7 (903) 729-29-23

gor@rutoken.ru

www.rutoken.ru