

СКЗИ «Шифр-Х.509»

Отказ от NРAPI в современных web-браузерах. Подходы к решению

ООО «Сайфер БИС», к.т.н. Влад Ковтун

Содержание

- Суть проблемы
- Известные походы и их особенности
- Выбранный подход

В чем суть проблемы*

| Платформа | Время отказа от NPAPI |
|--|-------------------------|
| Web-браузер | |
| Google Chrome | Сентябрь 2015 |
| Mozilla FireFox | Декабрь 2016 |
| Opera | Сентябрь 2015 |
| Microsoft Internet Explorer 11 (ActiveX) | с 2020 (для Windows 10) |
| Microsoft Edge | Не поддерживает |
| Среда исполнения | |
| Oracle JRE | С выпуска JDK 9, 2017 |

*- «лицензионная война» между Google и Oracle

Известные походы

1. Javascript библиотека в web-странице
 - ЧАО ИИТ
2. Javascript библиотека в расширении в web-браузере
 - ООО Бифит
3. Native библиотека в расширении в web-браузере
 - ПАО ПриватБанк+ЧАО ИИТ

Известные походы

4. Отдельное Java приложение

- Интернет банкинг (ООО Сайфер БИС, ООО Бифит, ООО НОКК и другие)

5. Native локальный web-сервис

- ЧАО ИИТ

6. Java локальный web-сервис

- ООО Сайфер БИС

Особенности

1. Javascript библиотека в web-странице

- JSVM и сам стандарт находится в развитии
- Различные реализации в web-браузерах
- Невозможно использовать защищенные носители
- Невозможно обеспечить целостность библиотеки
- Большой размер библиотеки, загружаемый каждый раз вместе с web-страницей
- Ограничение на размер обрабатываемых данных
- Технология Local Storage в web-браузере накладывает ограничение на использование лишь одного ключа и лишь одного web-приложения

Особенности

2. Javascript библиотека в расширении в web-браузере

- JSVM и сам стандарт находится в развитии
- Различные реализации в web-браузерах
- Поддержка расширений для разных браузеров и разных их версий
- Невозможно использовать защищенные носители
- **Возможно** обеспечить целостность библиотеки
- Расширение устанавливается и обновляется независимо от страницы
- Ограничение на размер обрабатываемых данных

Особенности

2. Javascript библиотека в расширении в web-браузере

- Технология Local Storage в web-браузере накладывает ограничение на использование лишь одного ключа и лишь одного web-приложения
- Необходимость дополнительного контроля версий расширения, т.к. данная возможность может быть отключена в браузере

Особенности

3. Native библиотека в расширении в web-браузере

- Поддержка расширений для разных web-браузеров и их версий
- Поддержка расширений для разных платформ (Windows, Linux, MacOS X и т.д.)
- **Возможно** использовать защищенные носители
- **Возможно** обеспечить целостность библиотеки
- Расширение устанавливается и обновляется независимо от страницы

Особенности

3. Native библиотека в расширении в web-браузере

- Нет ограничений на размер обрабатываемых данных
- Высокая производительность

Особенности

4. Отдельное Java приложение

- Необходимость разработки отдельного Java приложения для разных задач
- **Возможно** использовать защищенные носители
- **Возможно** обеспечить целостность библиотеки
- Нет ограничений на размер обрабатываемых данных

Особенности

5. Native локальный web-сервис

- Поддержка разных приложений для разных платформ (Windows, Linux, MacOS X и др.)
- **Возможно** использовать защищенные носители
- **Возможно** обеспечить целостность библиотеки
- Приложение устанавливается и обновляется независимо от web-страницы
- Нет ограничений на размер обрабатываемых данных
- **Не доверенное** и защищенное HTTPS-соединение
- Высокая производительность

Особенности

5. Native локальный web-сервис

- Журналирование операций сервиса
- Возможность работы с ЦСК напрямую и через Proxy
- Возможность взаимодействовать из любых приложений запущенных локально

Особенности

6. Java локальный web-сервис

- Единое приложение для разных платформ
- **Возможно** использовать защищенные носители
- **Возможно** обеспечить целостность библиотеки
- Приложение **загружается** и обновляется независимо от страницы
- Нет ограничений на размер обрабатываемых данных
- Доверенное и защищенное HTTPS-соединение
- Высокая производительность
- Работа в разовом и пакетном режимах
- Журналирование операций сервиса

Особенности

6. Java локальный web-сервис

- Асинхронное выполнение задач в несколько потоков
- Просмотр информации о сущности, для которой вычисляется ЭЦП и МВ
- Взаимодействие с ЦСК напрямую (OCSP, TSP, LDAP) и через HTTP(s)-проxy
- Взаимодействие из любых приложений запущенных локально
- Высокий потенциал для развития

Java локальный web-сервис

ОБЩАЯ ИДЕЯ

Функции

- Формирование и проверка ЭЦП
 - Разовый
 - Пакетный
- Формирование и проверка МВ
 - Разовый
 - Пакетный
- Получение информации о сущности для которой вычисляется МВ и ЭЦП

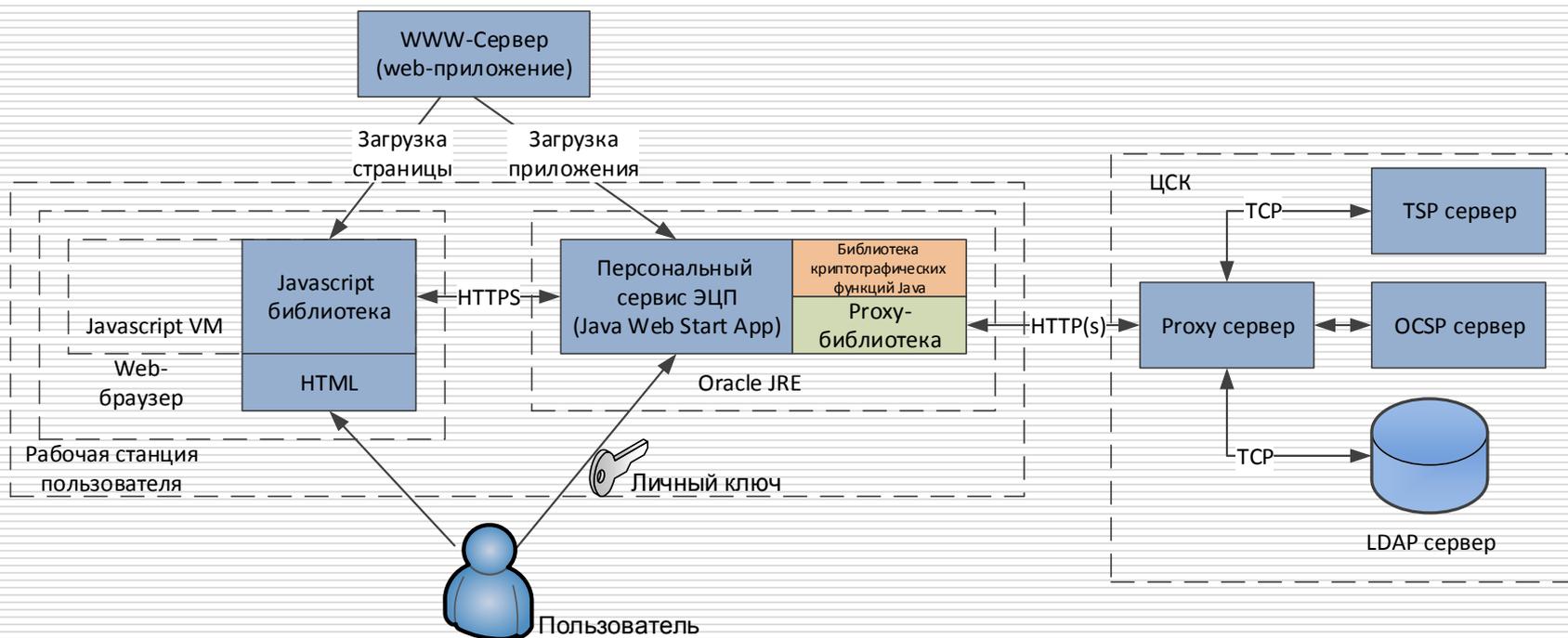
Функции

- Оперлируемые данные:
 - Файлы
 - Данные на странице
- Ведение журнала операций сервиса
- Наличие настроек:
 - Предустановленные (защиты)
 - Модифицируемые (через REST API)
- Просмотр сертификата

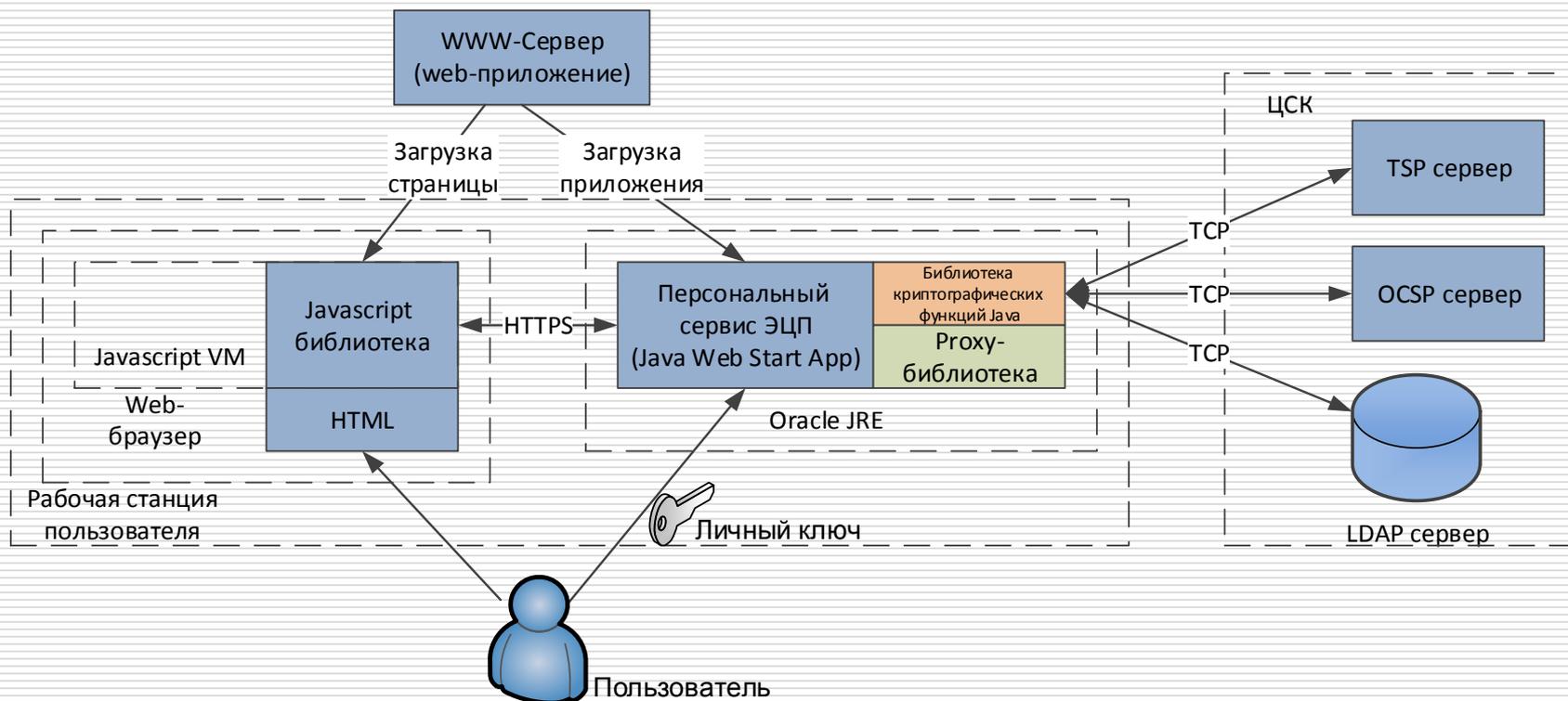
Функции

- Ввод в действие ключей

Архитектура (с proxy)



Архитектура (без проху)



Возможности

- Запрос разрешения на доступ к ключу
 - Разовый
 - Пакетный (указанное число или неограниченно)
- Конечное время действия разрешения доступа к ключу
- Конечное время бездействия сервиса (требуется ввод пароля)

Возможности

- ❑ Реальный HTTPS с использованием ключей доверенного ЦСК (web-страница <-> web-сервис)
- ❑ Асинхронное вычисление ЭЦП и МВ
- ❑ Многопоточный режим работы
- ❑ Ведение журнала операций
- ❑ Работа в отладочном режиме

Возможности

- Работа с ЦСК
 - Напрямую
 - Режим проксирования
- Поддержка разных платформ (поддерживаемые Oracle JRE)

Настройки (фиксированы)

- Создание контекста (proxy):
 - HTTP(s)-proxy: IP & Port
 - Создание контекста (без proxy):
 - OCSP: IP & Port
 - TSP: IP & Port
 - LDAP: IP & Port, Base DB, User, Pwd
 - Порт HTTPS для подключения
 - Число параллельно работающих потоков (для асинхронности)
-

Настройки (фиксированы)

- Время с момента последней активности, для ввода пароля доступа к ключу

Настройки (через REST API)

- ❑ Время действия разрешения на доступ ключу для выполнения операции
- ❑ Число обращений к ключу в рамках одного разрешения
- ❑ Время с момента последней активности, для ввода пароля доступа к ключу

Настройки (через REST API)

- Время действия разрешения доступа к ключу

Алгоритм (пакетный режим)

Формирование ЭЦП

- Проверка состояния сервиса
- Получение разрешения
- Получение сессии
- Загрузка данных в рамках сессии
- Вычисление ЭЦП
- Получение состояния операции
- Получение ЭЦП
- Завершение сессии*
- Завершение разрешения*

Проверка ЭЦП

- Проверка состояния сервиса
- Получение сессии
- Загрузка данных в рамках сессии
- Загрузка ЭЦП
- Проверка ЭЦП
- Получение состояние операции
- Завершение сессии*

Алгоритм (разовый режим)

Формирование ЭЦП

- Проверка состояния сервиса
- Получение сессии
- Загрузка данных в рамках сессии
- Вычисление ЭЦП
- Получение состояния операции
- Получение ЭЦП
- Завершение сессии*

Проверка ЭЦП

- Проверка состояния сервиса
- Получение сессии
- Загрузка данных в рамках сессии
- Загрузка ЭЦП
- Проверка ЭЦП
- Получение состояние операции

Производительность

- Условия эксперимента (web-сервис, без проху)
 - Рабочая станция:
 - CPU: Intel Core i5-4670 (4 cores)
 - RAM: 8 Gb
 - ОС: Windows 7 SP1 x86-64
 - JRE: Oracle JRE 1.8_091 x86-64
 - Длина ключа 257 бит

Производительность

- Условия эксперимента (ЦСК)
 - Виртуальная машина:
 - CPU: Intel Xeon X5550 (4 cores)
 - RAM: 4 Gb
 - ОС: Windows Server 2012 R2
 - СОС содержит 45 тыс. записей
 - LDAP: 1,5 млн. сертификатов

Производительность

| Размер данных | Постановка ЭЦП, с | Проверка ЭЦП, с |
|---------------|-------------------|-----------------|
| 1 кб | 0,037 | 0,134 |
| 10 кб | 0,138 | 0,164 |
| 100 кб | 0,146 | 0,177 |
| 1 Мб | 0,220 | 0,270 |
| 10 Мб | 1,078 | 1,093 |
| 50 Мб | 4,269 | 4,800 |

Производительность

| Размер данных | Постановка МВ, с | Проверка МВ, с |
|---------------|------------------|----------------|
| 1 кб | 0,023 | 0,200 |
| 10 кб | 0,033 | 0,240 |
| 100 кб | 0,056 | 0,283 |
| 1 Мб | 0,133 | 0,354 |
| 10 Мб | 0,998 | 1,095 |
| 50 Мб | 4,673 | 4,781 |

ДЕМОНСТРАЦИЯ

Перспективы

- ❑ Генерация ключей (PKCS#10)
- ❑ Смена ключей с последующей отправкой запроса (PKCS#7) в ЦР ЦСК (плановая и принудительная)
- ❑ Генерация запроса (PKCS#7) на отзыв/блокирование сертификата

Вопросы?

Спасибо за внимание!

ООО «Сайфер БИС»

Влад Ковтун

email: vlad.kovtun@cipher.kiev.ua

www: <http://www.cipher.kiev.ua>