ИИТ Агент подписи vs Сайфер Персональный сервис ЭЦП

Сокращения

АП - ИИТ Агент подписи
ПС - Персональный сервис ЭЦП
ВР - ИИТ web-розширення та NMH-модуль
ВП - NPAPI плагин

Установка и обновление

ПС	Веб-библиотеки	
	АП	ВР
Приложение персонализируется для отдельно взятой площадки и распространяется по защищенному соединению используя протокол HTTPS + SSL сертификат площадки.	Загрузка инсталяционных пакетов происходит через незащищенное соединение по протоколу HTTP, ресурс http://iit.com.ua не поддерживает протокол HTTPS.	Загрузка расширения производится через веб-магазин chrome, который гарантирует целостность и подлинность кода. NMH-модуль загружается через незащищенное соединение по протоколу HTTP, ресурс http://iit.com.ua не поддерживает протокол HTTPS.
Исходный код подписан, его целостность и подлинность проверяется виртуальной Java машиной при загрузке приложения.	Исходный код приложения не подписан.Для Linux систем Проверка целостности и подлинности deb пакетов не производится автоматически и является нетривиальной задачей для рядового пользователя.	Исходный код NMH-модуля не подписан. Для Linux систем Проверка целостности и подлинности deb пакетов не производится автоматически и является нетривиальной задачей для рядового пользователя.
Не требует установки и дополнительных настроек.	Необходимо установить и произвести настройки.	Необходимо отдельно выполнить установку и настройки веб-разширения и отдельно установку NMH-модуля.
Проверка обновленной версии происходит каждый раз при запуске приложения, приложение обновляется автоматически.	Необходимо контролировать наличие обновлений на сайте производителя. Обновление устанавливается вручную.	Необходимо контролировать наличие обновлений отдельно для NMH-модуля и отдельно для веб-расширения. Обновления устанавливается вручную.
Требует установки Java.	Не требует установки Java.	Не требует установки Java.

Использование

Персональный сервис	Веб библиотеки
Не требует дополнительных JavaScript библиотек для работы. Реализация ПС основана на подмножестве требований REST, содержит встроенный веб сервер для унификации взаимодействия по протоколу HTTPS.	Для работы требует JavaScript библиотеку-обертку, которая унифицирует взаимодействие с тремя различными в технологическом плане внешними компонентами. С каждым из внешних компонентов взаимодействие происходит с использованием отдельного протоколов: АП - JSON-RPC, ВР - Native Messaing Protocol, NPAPI.

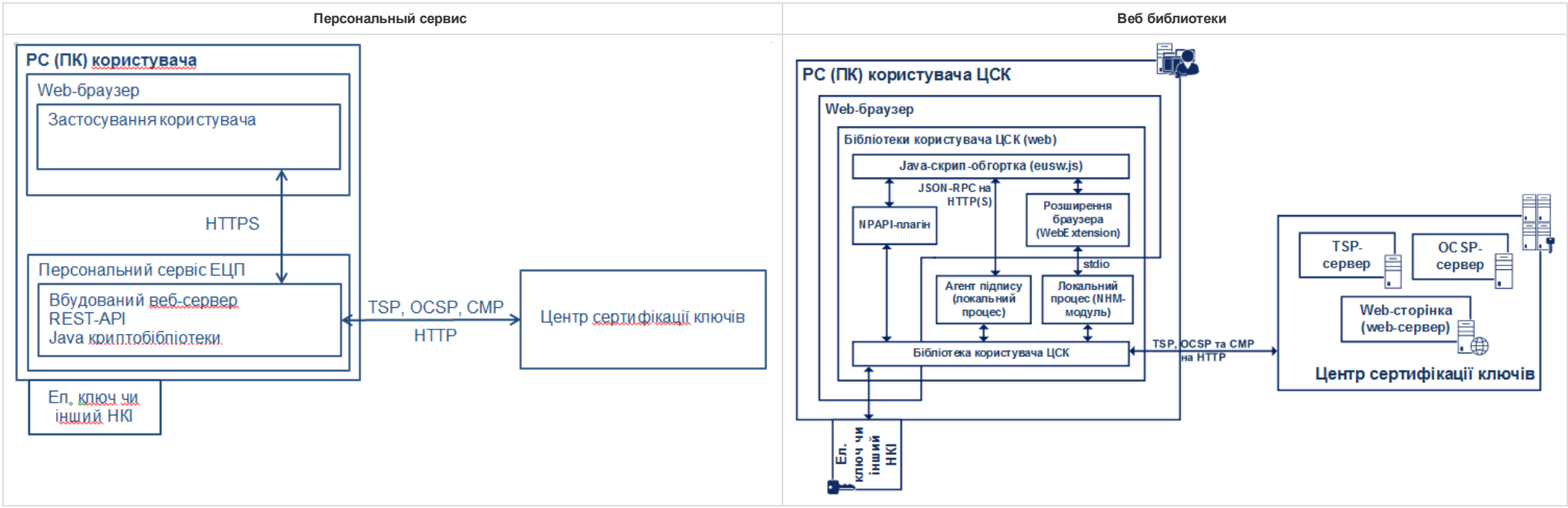

Таблица 1. Совместимость с операционными системами

Персональный сервис ЭЦП	Веб-библиотеки		
Все ОС, для которых существует реализация виртуальной машины Java	АП	ВР	ВП
	Только Windows	Linux (производные от Debian), Windows, OS X	Linux, Windows, OS X

Таблица 2. Совместимость с браузерами

Персональный сервис ЭЦП	Веб-библиотеки		
Все браузеры с поддержкой AJAX	АП	ВР	ВП
	Все браузеры с поддержкой AJAX	Chrome, Opera	Firefox

Таблица 3. Сводная таблица совместимости ОС+браузер

Персональный сервис ЭЦП	Веб-библиотеки
Одна и та же версия приложения используется для всех операционных систем и браузеров.	3 (три) различных подхода могут быть использованы. Вариант использования зависит от операционной системы и версии браузера.

	Chrome	Firefox	Opera	IE 10	Edge	Safari
Windows	Персональный сервис ЭЦП, выполненный в виде Java Web Start Appication					
Linux						

	Chrome	Firefox	Opera	IE 10	Edge	Safari
Windows	АП або ВР	в ОС Microsoft Windows XP та 2003 Server АП або NPAPI-плагіну з 40 до 52, в ОС Microsoft Windows Vista та вище АП з версії 22 та вище	АП або ВР з версії 35 та вище	АП	АП	

	Chrome	Firefox	Opera	IE 10	Edge	Safari
Linux (производние от Debian)	ВР	з версії 40 до 52 з використанням NPAPI-плагіну	ВР з версії 35 та вище			
OS X	АП або ВР	з версії 40 та вище АП або NPAPI-плагіну з версії 40 до 52	АП або ВР з версії 35 та вище			АП

Персональный сервис	Веб-библиотека	
	АП	ВР
Загрузка данных, которые подлежат проверке (выработки) цифровой подписи, а также получение самой цифровой подписи поддерживается как в двоичном виде, так и в формате Base64.	Только Base64.	Только Base64.
Ограничение на максимальный объем загружаемых (получаемых) данных зависит от фактического объема памяти, которым оперирует операционная система и которое выделено приложению. Объем выделенной памяти возможно указывать при старте приложение.	Поскольку используется только формат Base64, то, в случае необходимости подписать большой объем данных, например **50Мб** и выше, процесс кодировая-декодирования будет занимать длительное время и может привести к "зависанию" JavaScript VM браузера.	Поскольку используется только формат Base64, то, в случае необходимости подписать большой объем данных, например 50Мб и выше, процесс кодировая-декодирования будет занимать длительное время и может привести к "зависанию" JavaScript VM браузера. **Технологические ограничение** на объем данных, которые могут быть получены с NMH приложения, равно **1Мб**.

Безопасность

ПС	АП	ВР	NPAPI
Защищенный обмен между web-страницей и ПС строится посредством HTTPS-соединения посредством SSL-сертификата, изданного доверенным ЦСК.	Защищенный обмен между web-страницей и ПС строится на **недоверенном** HTTPS-соединении, для построения которого используется **самоизданный** SSL-сертификат. Указанный сертификат следует самостоятельно регистрировать в ОС.	Для взаимодействия JavaScript библиотеки и приложения, которое выступает в роли Native messaging host (NMH) используется **незащищенный** Native messaging protocol. Описание уязвимости здесь.	Не поддерживается современными версиями браузеров в виду серьезных проблем с безопасностью.
При запуске приложение оповещает пользователя о занятости необходимого для работы порта, предотвращая возможность подмены приложения вредоносным ПО.	При запуске приложение оповещает пользователя о занятости необходимого для работы порта, предотвращая возможность подмены приложения вредоносным ПО.	Достоверное приложение, которое выступает в роли Native messaging host, **может быть подменено вредоносным ПО**. У пользователя **отсутствует возможность контроля** за процессом регистрации и использования приложений, которые выполняют роль Native messaging host.	
Пользователь в интерактивном режиме дает разрешение на использование своей цифровой подписи.	Отсутствует контроль со стороны пользователя за использованием его цифровой подписи.	Отсутствует контроль со стороны пользователя за использованием его цифровой подписи.	

Поддержка и сопровождение

Персональный сервис	Веб-библиотеки
Специалистам службы поддержки необходимо освоить порядок работы с одним приложениям.	Специалистам службы поддержки необходимо освоить порядок работы с тремя отдельными приложениями.

Персональный сервис	Веб-библиотеки
В случае возникновения ошибок и сбоев в процесс отладки будет вовлечены 2 компонента: Персональный сервис и браузер. Пользователь имеет возможность предоставить службе поддержки дополнительную информацию как о работе персонального сервиса (журнал событий), так и взаимодействия сервиса с браузером (встроенные инструменты разработчика браузера) Для локализации неисправности службе поддержки достаточно записей журнала Персонального сервиса и информации, которую предоставляет средства разработчика браузера.	В случае возникновения ошибок и сбоев, в процесс отладки будет вовлечены 4 компонента: браузер, JavaScript-библитека, агент подписи, веб-расширение (плагин). У пользователя нет простой возможности определить, с каким компонентом в котретный момент времени работает JavaScript-библитека. У пользователя нет возможности предоставить информацию (состав запросов) о взаимодействии Веб-расширения и приложения, которое выполняет роль NMH.