|  |  |
| --- | --- |
| согласовано | Утверждаю |
| Заместитель Председателя  Высшего Арбитражного  Суда Российской Федерации | Генеральный директор  ЗАО «КРОК инкорпорейтед» |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_С.М. Амосов | \_\_\_\_\_\_\_\_\_\_\_\_\_ Б.Л. Бобровников |
| «\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 2013 г. | «\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 2013 г. |

Присоединение ВАС РФ к СМЭВ, разработка электронных сервисов для информационного взаимодействия с федеральными органами исполнительной власти с использованием инфраструктуры СМЭВ, подключение к ЕСИА и обеспечение использования усиленной квалифицированной электронной подписи в информационных системах арбитражных судов РФ

Плагин по работе со СКЗИ LCSignPlugin

Web-плагин LCSignPlugin

Частное техническое задание

17404049.5081000.132-01 93 01

На 17 листах

Действует с \_\_\_\_\_\_\_\_\_\_\_

Аннотация

Настоящее Частное техническое задание (далее - ЧТЗ) определяет назначение, общие и специальные требования к плагину по работе с СКЗИ LCSIGNPLUGIN.

**Конфиденциальный документ ЗАО «КРОК инкорпорейтед».** Любая информация, представленная в настоящем документе и имеющая отношение к сотрудничеству сторон, хозяйственно-коммерческой деятельности или техническим возможностям ЗАО «КРОК инкорпорейтед», а также к изделиям, услугам, фактическим и аналитическим данным, заключениям и материалам, кроме информации, которая в соответствии с действующим законодательством и иными правовыми актами Российской Федерации не может быть отнесена к конфиденциальной информации, является конфиденциальной. Не разрешается копирование и распространение информации без письменного разрешения ЗАО «КРОК инкорпорейтед».

Содержание

[1 Введение 4](#_Toc369809996)

[2 Общие сведения 5](#_Toc369809997)

[2.1 Наименование программы 5](#_Toc369809998)

[2.2 Наименования Разработчика и Заказчика работ и их реквизиты 5](#_Toc369809999)

[2.3 Основание для проведения работ 5](#_Toc369810000)

[2.4 Сроки начала и окончания работ 5](#_Toc369810001)

[2.5 Документы, на основании которых ведется проектирование 5](#_Toc369810002)

[2.6 Порядок оформления и предъявления Заказчику результатов работ 6](#_Toc369810003)

[3 Назначение и область применения разработки 7](#_Toc369810004)

[3.1 Назначение программы 7](#_Toc369810005)

[3.2 Область применения 7](#_Toc369810006)

[3.3 Объект, в котором используют программу 7](#_Toc369810007)

[4 Требования к программе 8](#_Toc369810008)

[4.1 Требования к функциональным характеристикам 8](#_Toc369810009)

[4.2 Требования к надежности 10](#_Toc369810010)

[4.3 Условия эксплуатации 11](#_Toc369810011)

[4.4 Требования к составу и параметрам технических средств 11](#_Toc369810012)

[4.5 Требования к информационной и программной совместимости 11](#_Toc369810013)

[4.6 Требования к маркировке и упаковке 12](#_Toc369810014)

[4.7 Требования к транспортированию и хранению 12](#_Toc369810015)

[5 Требования к программной документации 13](#_Toc369810016)

[6 Технико-экономические показатели 14](#_Toc369810017)

[7 Стадии и этапы разработки 15](#_Toc369810018)

[8 Порядок контроля и приемки 16](#_Toc369810020)

# Введение

Web-плагин LCSignPlugin разработан для платформ MS Windows, MAC OS, Linux и может использоваться в различных браузерах – Internet Explorer, Mozilla Firefox, Safari, Opera, Google Chrome, Seamonkey.

Web-плагин LCSignPlugin соответствует требованиям Федерального закона от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» и «Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи», утвержденным приказом ФСБ России от 27.12.2011 г. № 795.

В качестве средств криптографической защиты (далее - СКЗИ) может использоваться любой MS CSP с поддержкой российской криптографии, программные и аппаратные токены с поддержкой интерфейса PKCS#11.

# Общие сведения

## Наименование программы

**Полное наименование программы:**

Плагин по работе со СКЗИ LCSignPlugin.

**Условное обозначение программы:**

Web-плагин LCSignPlugin.

## Наименования Разработчика и Заказчика работ и их реквизиты

**Разработчик**

Закрытое акционерное общество «КРОК инкорпорейтед»

Адрес: 105082, Москва, ул. Большая Почтовая, д.26В, стр.2

Тел.: (495) 974-22-74

Факс: (495) 974-22-77

**Заказчик**3

Высший Арбитражный Суд Российской Федерации

Адрес: 101000 г. Москва, Малый Харитоньевский пер., д.12

Тел.: (495) 608-11-00

Факс: (495) 608-11-62

## Основание для проведения работ

Основанием для проведения работ по созданию web-плагина LCSignPlugin является Государственный контракт № ВАС-А-И33-13 от 30.08.2013 г.

## Сроки начала и окончания работ

Дата начала работ: 30.08.2013 г.

Дата окончания работ: 20.12.2013 г.

## Документы, на основании которых ведется проектирование

* Федеральный закон от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»;
* «Требования к форме квалифицированного сертификата ключа проверки электронной подписи», утвержденные приказом ФСБ России от 27.12.2011 г. № 795.

## Порядок оформления и предъявления Заказчику результатов работ

Работы по созданию должны осуществляться в соответствии с ГОСТ 34.601-90 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

По окончанию выполнения работ Разработчик должен представить Заказчику:

* дистрибутив web-плагина на оптических носителях;
* исходные коды web-плагина с комментариями и пояснениями;
* эксплуатационную документацию на web-плагина;
* неисключительные права на программное обеспечение web-плагина;
* акт сдачи-приемки работ.

# Назначение и область применения разработки

## Назначение программы

Web-плагин LCSignPlugin предназначен для:

* выполнения криптографических операций (формирование и проверка электронной подписи по стандарту PKCS#7;
* шифрование данных на открытом ключе по стандарту PKCS#7;
* извлечение исходных данных из зашифрованных контейнеров PKCS#7 и контейнеров с присоединенной подписью;
* установка защищенного соединения с сервером по протоколу TLS;
* формирование запроса на сертификат в формате PKCS#10;
* просмотр сертификатов;
* импорт/экспорт сертификатов в формате PKCS#12;
* расшифровка почтовых сообщений (SMIME) в web-приложении с использованием средств и возможностей различных СКЗИ.

## Область применения

Областью применения web-плагина LCSignPlugin является обеспечение формирования и проверки отсоединенной ЭП следующих ИС АС РФ:

* системы автоматизации судебного делопроизводства;
* информационная система «Мой арбитр»;
* информационная система «Картотека арбитражных дел».

## Объект, в котором используют программу

Браузеры – Internet Explorer, Mozilla Firefox, Safari, Opera, Google Chrome, Seamonkey.

ОС – MS Windows, MAC OS, Linux.

Прикладное ПО – MS Word.

# Требования к программе

## Требования к функциональным характеристикам

### Web-плагин LCSignPlugin должен реализовывать следующий набор функций:

1. HRESULT PKCS7SignFile(String InFile, String OutFile, bool IsAttached).

Выполняет подписание файла InFile с помощью личного сертификата. Результат – подпись в формате PKCS#7, – сохраняется в файле OutFile. Если значение параметра IsAttached равно true, то создается присоединенная подпись – контейнер PKCS#7 содержит не только электронную цифровую подпись, но и исходные данные целиком. Если же IsAttached равен false, то выходной файл будет содержать только подпись, без исходных данных.

Коды ошибок:

* 0x20040000 – успех;
* 0xA0040005 - не удалось открыть файл;
* 0xA0040003 - недостаточно памяти;
* 0xA0040006 - не удалось создать файл для записи;
* 0xA0040011 – нет сертификатов;
* 0xA0040004 - пользователь отменил выбор сертификата;
* 0xA0040010 - не найден сертификат;
* 0xA0040017 - не удалось построить цепочку сертификата;
* 0xA0040018 - истек срок действия сертификата;
* 0xA0040020 - корневой сертификат цепочки не доверенный;
* 0xA0040021 - неполная цепочка сертификата;
* 0xA0040022 – не установлен криптопровайдер;
* 0xA0040016 – не удалось получить доступ к хранилищу сертификатов.

1. HRESULT PKCS7VerifyFile(String Content, String Signature).

Функция выполняет проверку электронной цифровой подписи. Исходные данные берутся из файла Content, подпись – из файла Signature. Если проверка подписи прошла успешно, возвращается значение - 0.

Коды ошибок:

* 0x20040000 – успех;
* 0xA0040005 - не удалось открыть файл данных;
* 0xA0040003 - недостаточно памяти;
* 0xA0040006 - не удалось открыть файл подписи;
* 0xA0040022 – не установлен криптопровайдер;
* 0xA0040009 – подпись неверна, неверный формат подписи;
* 0xA0040008 – подпись неверна, не совпадают данные;
* 0xA0040007 – подпись неверна.

1. HRESULT TLSClientSession(String Host, int Port, String Data, String DataOut).

Данная функция позволяет отправлять и принимать данные по защищенному протоколу TLS с поддержкой российской криптографии. Открывается защищенное соединение с сервером Host на порте Port. Затем серверу предоставляется сертификат пользователя, после чего устанавливается авторизованное соединение. Если в системе нет установленных сертификатов, в таком случае устанавливается анонимное соединение. Затем функция отправляет на сервер данные, содержащиеся в параметре Data, и ждет ответа от сервера. После получения ответа соединение разрывается. В случае успешного выполнения в строку DataOut записываются данные, полученные от сервера.

Коды ошибок:

* 0x20040000 – успех;
* 0xA0040022 – не установлен криптопровайдер;
* 0xA0040023 – сервер не доступен;
* 0xA0040004 - пользователь отменил выбор сертификата;
* 0xA0040024 – неверный сертификат;
* 0xA0040025 – ошибка чтения данных с сервера.

### При работе с устройствами через интерфейс PKCS#11 Web-плагин LCSignPlugin должен реализовывать следующие функции:

1. INT ADDMODULEPKCS11(STRING MODULE, STRING LIBRARY).

Регистрирует во внутренней базе данных новый модуль под именем Module, работающий через подключаемую библиотеку, находящуюся в файле Library.

Коды ошибок:

* 0 – успех;
* -1 – ошибка загрузки модуля PKCS#11.

1. ARRAY LISTTOKEN()

Функция возвращает массив имен всех подключенных к плагину токенов. Помимо модулей, подключенных через функцию AddModulePKCS11, функция всегда возвращает виртуальные токены all и internal.

1. ARRAY PRIVCERT(STRING MODULE).

Возвращает список (по одному имени на строку) личных сертификатов (таких, для которых имеется закрытый ключ), хранящихся на подключенном токене Module. Если указан виртуальный токен all, то плагин последовательно переберет все подключенные к нему модули без необходимости у пользователя ввод PIN-кода для каждого токена. Вызов данной функции с указанием виртуального токена internal возможен, но результатом всегда будет пустой массив.

Коды ошибок:

NULL – нет сертификатов.

1. INT P7SIGNFILE(STRING NICKNAME, STRING INFILE, STRING OUTFILE, BOOL ISATTACHED).

Выполняет подписание файла InFile с помощью личного сертификата NickName. Результат – подпись в формате PKCS#7, – сохраняется в файле OutFile. Если значение параметра IsAttached равно true, то создается присоединенная подпись – контейнер PKCS#7 содержит не только электронную цифровую подпись, но и исходные данные целиком. Если же IsAttached равен false, то выходной файл будет содержать только подпись, без исходных данных.

Коды ошибок:

* 0 – успех;
* 5 - не удалось открыть файл;
* 3 - недостаточно памяти;
* 6 - не удалось создать файл для записи;
* 10 - не найден сертификат;
* 17 - не удалось построить цепочку сертификата;
* 18 - истек срок действия сертификата;
* 20 - корневой сертификат цепочки не доверенный;
* 21 - неполная цепочка сертификата.

1. STRING TLSCLIENT(STRING NICKNAME, STRING HOST, INT PORT, STRING DATA).

Данная функция позволяет отправлять и принимать данные по защищенному протоколу TLS с поддержкой российской криптографии. Открывается защищенное соединение с сервером Host на порте Port. Затем серверу предоставляется сертификат, указанный в параметре Nickname, после чего устанавливается авторизованное соединение. Параметр Nickname может являться пустой строкой (“”) – в таком случае устанавливается анонимное соединение. Затем функция отправляет на сервер данные, содержащиеся в параметре Data, и ждет ответа от сервера. После получения ответа соединение разрывается. В случае успешного выполнения возвращается строка, содержащая данные, полученные от сервера.

Коды ошибок:

NULL – ошибка.

## Требования к надежности

Требования не предъявляются.

## Условия эксплуатации

Эксплуатация web-плагина LCSignPlugin должна соответствовать требованиям к эксплуатирующей ее системе в целом:

* требованиям к режимам функционирования системы;
* требованиям по диагностированию системы;
* требования к численности и квалификации персонала системы.

## Требования к составу и параметрам технических средств

Web-плагин LCSignPlugin должен функционировать на технических средствах эксплуатирующей ее системы.

## Требования к информационной и программной совместимости

### Web-плагин LCSignPlugin должен функционировать в операционных системах Windows XP(x86, x64), Vista(x86, x64), 7(x86, x64), 8(x86, x64), Apple OS X, Linux x86, x64 (Debian, Mandriva, Ubuntu, Mint).

### Web-плагин LCSignPlugin должен функционировать в web-браузерах Internet Explorer, Firefox, Safari, Opera, Google Chrome.

### Функционирование web-плагина LCSignPlugin в системах автоматизации судопроизводства должно осуществляться посредством прикладного ПО MS Word. Для этого web-плагин должен быть реализован в виде 32/64-х битного COM-объекта.

### В качестве средств электронной подписи web-плагином должны поддерживаться:

1. Средства электронной подписи программного обеспечения «КриптоПро CSP» версии 3.6.
2. Программные средства электронной подписи, реализующие интерфейс MS Crypto API:
   1. VipNet CSP;
   2. Лисси-CSP;
   3. SignalCom CSP.
3. Аппаратные средства электронной подписи, реализующие интерфейс PKCS#11:
   1. eToken ГОСТ;
   2. Rutoken ЭЦП;
   3. MS\_KEY\_K.

## Требования к маркировке и упаковке

Требования к маркировке и упаковке не предъявляются.

## Требования к транспортированию и хранению

Требования к транспортированию и хранению не предъявляются.

# Требования к программной документации

5.1 В процессе разработки web-плагина LCSignPlugin должна быть разработана следующая эксплуатационная документация:

* «Описание программы»;
* «Описание применения»;
* «Исходные тексты программ с комментариями»;
* «Формуляр»;
* «Ведомость эксплуатационных документов»;
* «Руководство оператора»;
* «Руководство программиста».

5.2 Эксплуатационная документация должна разрабатываться с учетом требований комплекса государственных стандартов «Единая система программной документации»:

* ГОСТ 19.001-77. ЕСПД. Общие положения;
* ГОСТ 19.004-80. ЕСПД. Термины и определения;
* ГОСТ 19.101-77. ЕСПД. Виды программ и программных документов;
* ГОСТ 19.201-78. ЕСПД. Техническое задание. Требования к содержанию и оформлению;
* ГОСТ 19.301-79. ЕСПД. Программа и методика испытаний. Требования к содержанию и оформлению;
* ГОСТ 19.401-78. ЕСПД. Текст программы. Требования к содержанию и оформлению;
* ГОСТ 19.402-78. ЕСПД. Описание программы. Требования к содержанию и оформлению;
* ГОСТ 19.501-78. ЕСПД. Формуляр. Требования к содержанию и оформлению
* ГОСТ 19.502-78. ЕСПД. Описание применения. Требования к содержанию и оформлению;
* ГОСТ 19.503-79. ЕСПД. Руководство системного программиста. Требования к содержанию и оформлению;
* ГОСТ 19.504-79. ЕСПД. Руководство программиста. Требования к содержанию и оформлению;
* ГОСТ 19.505-79. ЕСПД. Руководство оператора. Требования к содержанию и оформлению;
* ГОСТ 19.507-79. ЕСПД. Ведомость эксплуатационных документов.

# Технико-экономические показатели

Ориентировочная экономическая эффективность не рассчитываются.  
Предполагаемая годовая потребность web-плагина LCSignPlugin – 2 млн. экземпляров в год. Зарубежных и отечественных аналогов нет.

# Стадии и этапы разработки

|  |  |  |
| --- | --- | --- |
| №  п/п | Наименование этапа | Сроки  выполнения |
| 1 | Разработка ТЗ на проведение тематических исследований по оценке влияния программного обеспечения «Web-плагин LCSignPlugin на СКЗИ» | До 1 октября 2013 г. |
| 2 | Разработка плагина для web-браузеров для обеспечения возможности подачи документов с использованием электронной подписи. | До 21 октября 2013 г. |
| 3 | Разработка эксплуатационной документации на web-плагин | До 1 ноября 2013 г. |
| 4 | Проведение испытаний разработанного web-плагина на соответствующих ОС и с использованием соответствующих СКЗИ | До 1 декабря 2013 г. |
| 5 | Осуществление комплексного тестирования программного обеспечения, разработанного по результатам этапа 1. | До 20 декабря 2013 г. |

# Порядок контроля и приемки

Испытания должны обеспечить проверку как минимум успешного функционирования разработанного web-плагина на соответствующих операционных системах и с использованием соответствующих СКЗИ.

По результатам испытаний разработанный web-плагин и эксплуатационная документация (в соответствии с разделом 5) должны быть переданы Заказчику для проведения комплексных испытаний в составе ИС Заказчика. По результатам проведения комплексных испытаний при обнаружении недостатков в ходе них должна быть выполнена доработка web-плагина и проведены повторные комплексные испытания.

Результатами проведения испытаний разработанного web-плагина являются следующие отчетные документы:

1. Программа и методика испытаний.
2. Протокол испытаний.

Каждый этап работ оформляется промежуточным актом сдачи-приемки работ по этапам, определенным в разделе 7.

Перечень условных обозначений, сокращений и терминов

|  |  |
| --- | --- |
| Термин | Определение |
| ГОСТ | Государственный стандарт |
| ЕСПД | Единая система программной документации |
| ИС | Информационные системы |
| Модуль | Web-плагин LCSignPlugin |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| СКЗИ | Средство криптографической защиты информации |
| ЧТЗ | Частное техническое задание |
| ЭЦП | Электронная цифровая подпись |
| PKCS | Криптографические стандарты открытого ключа (Public Key Cryptography Standards). |