Программный комплекс «Блокхост-ЭЦП» 2.0 (ПК «Litoria Desktop»)

Описание применения

АННОТАЦИЯ

Настоящий документ содержит описание применения программного комплекса «Блокхост-ЭЦП» 2.0 (далее – ПК «Litoria Desktop», ПК или комплекс).

В разделе «Назначение ПК «Litoria Desktop» дан краткий обзор основных функций и возможностей комплекса.

В разделе «Условия применения комплекса» указаны аппаратные и программные требования к рабочему компьютеру пользователя, на котором будет использоваться комплекс.

В соответствующих разделах указаны задачи, которые решает комплекс, и функции, с помощью которых эти задачи решаются, а также описаны виды входных и выходных данных для основных функций комплекса.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПК «LITORIA DESKTOP»

Основным назначением ПК «Litoria Desktop» является создание, добавление, заверка и проверка электронной подписи (ЭП), а также шифрование и расшифровывание файлов. В ПК «Litoria Desktop» реализована возможность выполнения одновременных операций создания ЭП и шифрования, расшифровывания и проверки ЭП.

Кроме того, продукт позволяет выполнить функции просмотра хранилища сертификатов и списков отзыва сертификатов; создания запроса на выпуск и перевыпуск сертификата; установки сертификата на устройство; установки сертификата из устройства в реестр; просмотра установленных криптопровайдеров и их параметров; формирования DVCS-запросов и анализа DVC-квитанций в соответствии с рекомендациями RFC3029.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

Требования к рабочей станции, на которую устанавливается ПК «Litoria Desktop», обусловлены применением ОС.

ПК «Litoria Desktop» функционирует под управлением следующих ОС:

- Windows XP (32 бит/64 бит);
- Windows Sever 2003 (32 бит/64 бит);
- Windows Server 2008 (32 бит/64 бит);
- Windows Vista (32 бит/64 бит);
- Windows 7 (32 бит/64 бит);
- Windows Server 2008 R2;
- Windows 8 (32 бит/64 бит);
- Windows Server 2012 (64 бит);
- Windows 8.1 (32 бит/64 бит);
- Windows Server 2012 R2 (64 бит).

Дополнительно должно быть установлено следующее программное обеспечение:

1. Средство криптографической защиты информации, реализованное в соответствии с технологией Microsoft CSP. Например: либо программные СКЗИ – «ViPNet CSP» версии 3.2, «ВАЛИДАТА CSP» версии 4.0, «Крипто-Ком 3.2», «КриптоПро CSP» версий 3.6 и выше или ПК «ЛИССИ-CSP»; либо драйвера для аппаратных СКЗИ – «Криптотокен» в составе изделия «eToken ГОСТ» или «РУТОКЕН ЭЦП».

3. ОПИСАНИЕ ЗАДАЧИ

3.1. ОПРЕДЕЛЕНИЕ ЗАДАЧИ

Электронная подпись (ЭП) стала неотъемлемым атрибутом повседневной деятельности современного человека. Без ЭП в настоящее время уже невозможно представить функционирование большинства информационных систем от проведения электронных торгов до сдачи налоговой отчетности, от защищенного доступа к web-ресурсам через Интернет до корпоративного электронного документооборота.

Для работы с ЭП обычному пользователю необходим огромный набор средств, а именно: криптопровайдер, средство высокого уровня для создания ЭП, электронные ключи и драйвера к ним. При этом все средства не достаточно просто установить на компьютер пользователя, необходимо еще выполнить ряд действий для настройки работы с ЭП, что занимает много времени и сил.

3.2. МЕТОД РЕШЕНИЯ ЗАДАЧИ

При использовании ПК «Litoria Desktop» пользователю доступен весь комплект необходимых функций.

Для подготовки рабочего места к работе с ЭП ПК «Litoria Desktop» предоставляет пользователю возможность выполнить следующие функции:

- создание нового запроса на сертификат;
- создание запроса на основе имеющегося сертификата;
- установка сертификата на устройство;
- просмотр сертификатов в контейнерах;
- установка сертификата из устройства в хранилище «Личное»;
- управление сертификатами:
  - импорт;
  - экспорт;
  - удаление;
  - детальный просмотр;
  - проверка статуса по локальному и/или удаленному COC и по протоколу OCSP в реальном времени;
- управление списками отзыва сертификата:
  - импорт;
  - экспорт;
  - удаление;
  - детальный просмотр;
- просмотр списка криптопровайдеров;
- удаление контейнера закрытого ключа;
- управление настройками комплекса.

Для работы с ЭП комплекс обеспечивает выполнение следующих функций:

- создание ЭП для файлов произвольного типа;
- добавление ЭП для подписанных файлов;
- заверка ЭП для подписанных файлов;
- проверка ЭП для подписанных файлов с возможностью получения исходного документа;
- формирование DVCS-запросов и анализ DVC-квитанций в соответствии с рекомендациями RFC3029;
- шифрование файла произвольного типа;
- расшифровывание файла;
- гарантированное удаление файлов произвольно типа;
- универсальные операции:
  - создание ЭП и шифрование файла произвольного типа;

- расшифровывание файла и проверка ЭП с возможностью получения исходного документа.

3.2.1. СОЗДАНИЕ НОВОГО ЗАПРОСА НА СЕРТИФИКАТ

Для выполнения операций создания/добавления/заверки ЭП необходимо иметь личный цифровой сертификат.

Цифровой сертификат содержит идентификационную информацию о пользователе (в том числе его имя), открытый ключ и уникальную цифровую подпись, которая закрепляет сертификат за удостоверяющим центром (УЦ), который его создал. Закрытый ключ, соответствующий открытому ключу сертификата, должен находиться в контейнере на отчуждаемом носителе. В качестве отчуждаемого носителя может использоваться любой носитель (например, дискета 3,5", сменный носитель с интерфейсом USB и др.)

С помощью ПК «Litoria Desktop» можно создать запрос на новый личный сертификат. Для этого надо указать имя выходного файла, криптосистему, криптопровайдер, имя ключевого контейнера, личную идентификационную информацию пользователя и информацию о создаваемом сертификате, такую как использование ключа и назначение сертификата. При выполнении операции создания запроса осуществляется также создание ключевой пары открытый-закрытый ключ. Созданный запрос отправляется на рассмотрение в УЦ, и на основе него УЦ выпускает личный цифровой сертификат.

3.2.2. СОЗДАНИЕ ЗАПРОСА НА ОСНОВЕ ИМЕЮЩЕГОСЯ СЕРТИФИКАТА

ПК «Litoria Desktop» позволяет создать запрос на новый сертификат на основе имеющегося сертификата, у которого истекает или уже истек срок действия.

Для создания запроса на сертификат на основе имеющегося необходимо указать имя выходного файла, криптосистему, криптопровайдер, имя ключевого контейнера, и выбрать сертификат, на основе которого надо создать запрос на новый сертификат.

3.2.3. УСТАНОВКА СЕРТИФИКАТА НА УСТРОЙСТВО

ПК «Litoria Desktop» позволяет выполнить установку сертификата ключа подписи на устройство, которое ранее использовалось для создания запроса и содержит контейнер с парой открытый-закрытый ключ к этому сертификату.

3.2.4. ПРОСМОТР СЕРТИФИКАТОВ В КОНТЕЙНЕРАХ

С помощью ПК «Litoria Desktop» можно выполнить просмотр сертификатов, созданных на основе различных криптопровайдеров, во всех имеющихся контейнерах, и установить выбранный сертификат в хранилище «Личное».

3.2.5. УПРАВЛЕНИЕ СЕРТИФИКАТАМИ

ПК «Litoria Desktop» позволяет работать с системными хранилищами сертификатов. Существуют возможности импорта, экспорта и удаления сертификатов, а также просмотра хранилища сертификатов.

Хранилище сертификатов – это область системы, предназначенная для хранения сертификатов.

Импорт – это копирование сертификатов, списков сертификации удостоверяющего центра и списков отзыва сертификатов с локального диска в хранилище сертификатов.

Экспорт – это копирование сертификатов, списков сертификации удостоверяющего центра и списков отзыва сертификатов из хранилища сертификатов на локальный диск.

С помощью ПК «Litoria Desktop» можно выполнить операции установки корневого сертификата, актуального списка отзыва и сертификатов других пользователей.

Также с помощью функции *Импорт* можно установить личный сертификат из файла, полученного от УЦ в ответ на отправленный запрос, в хранилище сертификатов «Личное».

3.2.6. УПРАВЛЕНИЕ СПИСКАМИ ОТЗЫВА СЕРТИФИКАТОВ

ПК «Litoria Desktop» позволяет работать со списками отзыва сертификатов. Существуют возможности импорта, экспорта, удаления и просмотра списков отзыва.

3.2.7. ПРОСМОТР СПИСКА КРИПТОПРОВАЙДЕРОВ

С помощью ПК «Litoria Desktop» можно выполнить просмотр установленных на компьютере криптопровайдеров и информацию о них.

3.2.8. УДАЛЕНИЕ КОНТЕЙНЕРА ЗАКРЫТОГО КЛЮЧА

ПК «Litoria Desktop» позволяет удалить контейнер закрытого ключа с ключевого отчуждаемого носителя.

3.2.9. УПРАВЛЕНИЕ НАСТРОЙКАМИ КОМПЛЕКСА

ПК «Litoria Desktop» предоставляет возможность создать настройки для всех типовых операций.

Для каждой ситуации можно настроить профиль работы программы: установить кодировку выходных файлов операций, указать информацию для подключения к прокси-серверу, установить адрес службы штампов времени, указать имя рабочей директории, выбрать сертификат подписчика, указать параметры создания и проверки ЭП, выбрать сертификаты получателей и другое.

Благодаря таким настройкам возможна автоматизация всех операций – выполнение любой операции за один клик мыши.

3.2.10. СОЗДАНИЕ ЭП

Электронная подпись (ЭП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки и полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭП. С помощью ЭП можно идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Для создания ЭП должен быть осуществлен выбор сертификата ключа подписи, криптосистемы (программный или аппаратный криптопровайдер) и параметров создания ЭП.

К параметрам создания ЭП относятся:

- создание отделенной или совмещенной ЭП;
- создание ЭП с вложенным внутренним штампом времени;
- создание усовершенствованной ЭП.

Процесс создания усовершенствованной ЭП делится на следующие этапы:

- создание ЭП;
- получение штампа времени на значение ЭП;
- сбор доказательств действительности сертификата ключа подписи и присоединение этих доказательств и их хэш-кодов к подписанному документу;
- получение штампа времени на сформированные доказательства действительности сертификата ключа.

3.2.11. ДОБАВЛЕНИЕ ЭП

В случае, когда в подписании документа участвует несколько лиц, и каждый должен поставить в нем свою подпись (например, в листе согласования), используется операция добавления ЭП. В отличие от

операции создания ЭП добавление ЭП производится в уже подписанный ранее документ.

В ПК «Litoria Desktop» существует возможность добавления подписи, созданной на криптографическом алгоритме, отличном от ГОСТ, например, RSA.

3.2.12. ЗАВЕРКА ЭП

ПК «Litoria Desktop» позволяет формировать заверяющую ЭП. С помощью этого типа подписи можно заверить ЭП другого пользователя, сформировав ЭП на значении ЭП другого пользователя, тем самым косвенно подписывая сами данные.

Перед созданием заверяющей подписи производится проверка ЭП, чтобы было достоверно известно, какие подписи уже существуют в документе, и их статус.

Дальнейшая операция по заверке подписи аналогична созданию ЭП.

Заверка ЭП возможна лишь для подписанных ранее файлов.

3.2.13. ПРОВЕРКА ЭП

Проверка ЭП подразумевает подтверждение подлинности электронной подписи в электронном документе, то есть:

- принадлежности электронной подписи в электронном документе владельцу сертификата ключа подписи;
- отсутствия искажений в подписанном данной электронной подписью электронном документе;
- подтверждение момента подписи;
- подтверждение действительности сертификата ключа подписи на момент проверки либо на момент создания электронной подписи при наличии в ЭП доказательств, определяющих этот момент.

Проверка усовершенствованной ЭП файла с отделенной подписью – проверка корректности самого файла подписи.

3.2.14. ФОРМИРОВАНИЕ DVCS-ЗАПРОСОВ И АНАЛИЗ DVC-КВИТАНЦИЙ

ПК «Litoria Desktop» позволяет формировать DVCS-запросы 2-х типов:

- подтверждение электронной подписи (ЭП) электронного документа (Validation of Digitally Signed Document – VSD);
- подтверждение действительности сертификата ключа подписи (Validation of Public Key Certificates – VPKC).

Подписанный указанным личным сертификатом DVCS-запрос отправляется для проверки на сервер службы ДТС. Ответ сервера приходит в виде квитанции.

При формировании DVCS-запроса типа VSD можно отправить внутри запроса не документ, а его хэш-значение (применяется, когда недопустима передача содержания конфиденциального документа в канал связи).

Комплекс позволяет создать анонимный DVCS-запрос, но в таком случае квитанция не имеет юридического значения. Анонимный DVCS-запрос используется только в демонстрационных целях.

Более подробное описание функций формирования DVCS-запросов и анализа DVC-квитанций смотрите в документе «ПК «Litoria Desktop». Руководство пользователя. ДТС клиент».

3.2.15. ШИФРОВАНИЕ ФАЙЛА

Шифрование производится с использованием открытого ключа, содержащегося в сертификате получателя. Закрытый ключ есть только у владельца использованного сертификата открытого ключа.

Таким образом, при шифровании файла никто, кроме владельца закрытого ключа, не сможет расшифровать файл.

ПК «Litoria Desktop» может производить шифрование файла сразу для нескольких будущих получателей файла, при этом их сертификаты должны быть созданы с помощью криптографического алгоритма, относящегося к стандарту (например, ГОСТ или RSA), единому для всех участников операции. Для каждого сертификата получателей пользователь может просмотреть статус, чтобы на его основании сделать вывод о пригодности данного сертификата к шифрованию.

Возможность гарантированного удаления файла после шифрования позволяет безвозвратно удалить конфиденциальную информацию. Необходимо заметить, что файл подкачки ОС Windows может хранить в себе остатки содержимого файла, но без знания примерного содержимого файла найти их не представляется возможным.

3.2.16. РАСШИФРОВЫВАНИЕ ФАЙЛА

При получении зашифрованного документа расшифровывание пройдет успешно при наличии закрытого ключа, связанного с одним из открытых ключей, на которых производилось шифрование файла.
Если существует несколько закрытых ключей, которым соответствуют несколько открытых ключей, участвующих при шифровании, то расшифровывание произойдет на первом из закрытых ключей. После расшифровывания можно получить информацию о том, на каком сертификате была произведена операция расшифровывания.

3.2.17. ГАРАНТИРОВАННОЕ УДАЛЕНИЕ ФАЙЛОВ

Гарантированное удаление можно выполнить для любого выбранного пользователем файла.

Удаление файлов происходит трехкратным затиранием содержимого по специальному алгоритму, исключающему считывание остаточной информации на диске после удаления.

3.2.18. УНИВЕРСАЛЬНАЯ ОПЕРАЦИЯ СОЗДАНИЯ ЭП И ШИФРОВАНИЯ ФАЙЛА

Программный комплекс предоставляет возможность одновременного создания ЭП и шифрования. Все действия, выполняемые при этом, аналогичны одиночным операциям создания ЭП и шифрования.
С помощью этой функции достигается универсальность в интерфейсе и удобство для пользователя.

3.2.19. УНИВЕРСАЛЬНАЯ ОПЕРАЦИЯ РАСШИФРОВЫВАНИЯ ФАЙЛА И ПРОВЕРКИ ЭП

Функциональность проверки идентична отдельным проверкам – вначале выполняется расшифровывание, потом проверка ЭП.

После расшифровывания пользователю становится доступна следующая информация:

- для расшифровывания – сертификат открытого ключа, на связанном с которым закрытом ключе файл был расшифрован;
- для проверки ЭП – все сертификаты подписи, их статусы.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1. ВХОДНЫЕ ДАННЫЕ

Входные данные для ПК «Litoria Desktop» отличаются друг от друга в зависимости от выполняемой операции. В таблице 4.1 приведены входные данные для основных функций комплекса.

Таблица 4.1

Функция	Входные данные	Примечание
Создание нового запроса на сертификат	1. Название файла-запроса и его расположение; 2. Криптосистема (указанная вручную); 3. Криптопровайдер (указанный вручную), с помощью которого будет создан ключевой контейнер; 4. Информация о ключевом контейнере (имя, заданное автоматически или вручную; pin-код); 5. Параметры ключевой пары (алгоритм, длина открытого ключа и параметры применения); 6. Идентификационная информация о пользователе (указанная вручную); 7. Параметры ключа и сертификата (указанная вручную).	Для выполнения данной функции необходимо иметь в наличии чистый ключевой носитель[1].
Создание запроса на основе имеющегося сертификата	1. Название файла-запроса и его расположение; 2. Криптосистема (указанная вручную); 3. Криптопровайдер (указанный вручную), с помощью которого будет создан ключевой контейнер; 4. Информация о ключевом контейнере (имя, заданное автоматически или вручную; pin-код); 5. Параметры ключевой пары (алгоритм, длина открытого ключа и параметры применения); 6. Сертификат подписчика, на основе которого будет создан запрос.	Для выполнения данной функции необходимо иметь в наличии ключевой носитель с закрытым ключом сертификата подписчика, на основе которого будет создан запрос.
Установка сертификата на устройство	1. Файл сертификата, полученный в ответ на ваш запрос из удостоверяющего центра; 2. Криптосистема (указанная вручную).	Для выполнения данной функции необходимо иметь ключевой носитель, с использованием которого создавался запрос.
Просмотр сертификатов в контейнерах	1. Криптосистема (указанная вручную); 2. Криптопровайдер (указанный вручную), на основе которого были созданы ключевые контейнеры с сертификатами; 3. Информация о ключевом контейнере.	Для выполнения данной функции необходимо иметь носитель с ключевыми контейнерами.

[1] В качестве ключевого носителя может использоваться любой носитель, например, дискета 3,5", сменный носитель с интерфейсом USB и др.

Функция	Входные данные	Примечание
Импорт сертификата	1. Файл сертификата, который необходимо скопировать в хранилище сертификатов; 2. Хранилище сертификатов (указанное автоматически или вручную), в которое необходимо скопировать сертификат.	
Экспорт сертификата	1. Сертификат (указанный вручную в хранилище), который необходимо скопировать на локальный диск; 2. Формат файла сертификата (указанный вручную).	
Удаление сертификата	1. Сертификат (указанный вручную в хранилище).	
Детальный просмотр сертификата	1. Сертификат (указанный вручную в хранилище).	
Проверка статуса сертификата	1. Сертификат (указанный вручную в хранилище).	
Импорт списка отзыва сертификатов	1. Файл списка отзыва, который необходимо скопировать в хранилище; 2. Хранилище (указанное автоматически или вручную), в которое необходимо скопировать список отзыва.	
Экспорт списка отзыва сертификатов	1. Список отзыва (указанный вручную в хранилище), который необходимо скопировать на локальный диск; 2. Формат файла списка отзыва (указанный вручную).	
Удаление списка отзыва сертификатов	1. Список отзыва (указанный вручную в хранилище).	
Детальный просмотр списка отзыва	1. Список отзыва (указанный вручную в хранилище).	
Создание ЭП	1. Файл произвольного типа[2]; 2. Сертификат подписчика (указанный вручную); 3. Криптосистема (указанная вручную); 4. Параметры подписи (указанные вручную).	Для выполнения данной функции необходимо иметь в наличии ключевой носитель с закрытым ключом сертификата подписчика.
Добавление ЭП Заверка ЭП	1. Подписанный файл; 2. Сертификат подписчика (указанный вручную); 3. Криптосистема (указанная вручную); 4. Параметры подписи (указанные вручную).	Для выполнения данной функции необходимо иметь в наличии ключевой носитель с закрытым ключом сертификата подписчика.

[2] ПК «Litoria Desktop» работает с файлами форматов, поддерживаемых ПО Microsoft Office и соответствующими приложениями, установленными в ОС. При подписании таких файлов ЭП не встраивается в сам файл, а создается в формате CAdES.
При создании квалифицированной ЭП допустимыми форматами файлов являются только odf, pdf, xml.

Функция	Входные данные	Примечание
Проверка ЭП	1. Подписанный файл; 2. Параметры проверки подписи (указанные вручную).	
Формирование DVCS-запроса VSD типа	1. Подписанный файл в формате pkcs#7[3]; 2. Параметры запроса (указанные вручную); 3. Криптосистема (указанная вручную); 4. Сертификат подписчика (указанный вручную); 5. Адрес ДТС сервера (указанный автоматически).	
Формирование DVCS-запроса VPKC типа	1. Сертификат ключа подписи; 2. Параметры запроса (указанные вручную); 3. Криптосистема (указанная вручную); 4. Сертификат подписчика (указанный вручную); 5. Адрес ДТС сервера (указанный автоматически).	
Шифрование	1. Файл произвольного типа[4]; 2. Сертификаты получателей (указанные вручную).	
Расшифровывание	1. Зашифрованный файл.	
Гарантированное удаление	1. Файл произвольного типа[4].	
Создание ЭП и шифрование файла.	1. Файл произвольного типа[4]; 2. Сертификат подписчика (указанный вручную); 3. Сертификаты получателей (указанные вручную); 4. Параметры подписи (указанные вручную).	
Расшифровывание файла и проверка ЭП	1. Подписанный и зашифрованный файл; 2. Параметры проверки подписи (указанные вручную).	

4.2. ВЫХОДНЫЕ ДАННЫЕ

В результате выполнения операций шифрования и создания ЭП на выходе ПК «Litoria Desktop» формируются файлы с расширениями, указанными в настройках. Расширения, которые указаны по умолчанию, приведены в таблице 4.2.

Таблица 4.2

Иконка	Тип файла	Расширение файла	Описание
	Подписанный файл	.p7s	подписан в DER-кодировке или в BASE64-кодировке
	Зашифрованный файл	.p7m	зашифрован в DER-кодировке или в BASE64-кодировке
	Подписанный и зашифрованный файл	.p7s.p7m	подписан и зашифрован в DER-кодировке или в BASE64-кодировке

[3] base64 формат и отделенная подпись временно не поддерживаются

[4] ПК «Litoria Desktop» работает с файлами форматов, поддерживаемых ПО Microsoft Office и соответствующими приложениями, установленными в ОС. При подписании таких файлов ЭП не встраивается в сам файл, а создается в формате CAdES.

Новое расширение файлу назначается в зависимости от типа операции.

Идентификатор создаваемого после выполнения операций шифрования и создания файла формируется по следующей схеме:

Идентификатор файла до выполнения операций шифрования и/или создания ЭП: **<Имя файла>.<расширение файла до выполнения операции>.**

Идентификатор файла после выполнения операций шифрования и/или создания ЭП: **<Имя файла>.<расширение файла до выполнения операции>.<Новое расширение>**.

Аналогично происходит восстановление старого идентификатора файла после выполнения обратных операций расшифровывания и снятия ЭП.

Примечание: ПК «Litoria Desktop» не встраивает ЭП в файлы форматов PDF, XML и ODF, а создает для них подпись в формате CAdES.