ГАЗИНФОРМ СЕРВИС

Программный комплекс «Litoria Desktop 2»
Описание применения

Санкт-Петербург, 2018

Аннотация

Настоящий документ содержит сведения о применении программного комплекса «Litoria Desktop 2» (далее – ПК «Litoria Desktop 2», ПК или комплекс).

В разделе «Назначение ПК «Litoria Desktop 2» дан краткий обзор основных функций и возможностей комплекса.

В разделе «Условия применения» 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 2»

Основным назначением ПК «Litoria Desktop 2» является создание, добавление, заверение и проверка электронной подписи (ЭП), а также шифрование и извлечение файлов. В ПК «Litoria Desktop 2» реализована возможность выполнения одновременных операций создания ЭП и шифрования, извлечения и проверки ЭП.

Кроме того, продукт позволяет выполнить функции просмотра хранилища сертификатов; создания запроса на выпуск и перевыпуск сертификата; установки сертификата на устройство; установки сертификата из устройства в реестр; просмотра установленных криптопровайдеров и их параметров; использования службы DVCS для проверки ЭП и действительности сертификата ключа проверки подписи, в том числе для электронных документов длительного архивного хранения.

Интеграция в различные системы документооборота, порталы и на серверы приложений с использованием российских и иностранных криптографических алгоритмов с возможностью трансграничного взаимодействия возможна с помощью криптографической платформы «Litoria Crypto Platform».

2 Условия применения

2.1 Требования к программному обеспечению

ПК «Litoria Desktop 2» функционирует под управлением следующих ОС:

- Windows 7 с пакетом обновления 1 (SP1) (32 бит/64 бит);
- Windows Server 2012 (64 бит);
- Windows Server 2012 R2 (64 бит);
- Windows 10 (32 бит/64 бит).

Дополнительно должно быть установлено следующее программное обеспечение:

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

Минимальные требования к рабочей станции, на которую устанавливается ПК «Litoria Desktop 2», обусловлены применением ОС.

Рекомендуется на рабочей станции, на которую устанавливается ПК «Litoria Desktop 2» использование монитора с разрешением экрана не менее 1280x800

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 недостаточно 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 2» пользователю доступен весь комплект необходимых функций.

Для подготовки рабочего места к работе с ЭП ПК «Litoria Desktop 2» 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 СОС и по протоколу OCSP в реальном времени;
- просмотр списка криптопровайдеров;
- удаление контейнера ключа ЭП;
- управление настройками комплекса.

Для работы с ЭП комплекс обеспечивает выполнение следующих функций:

- создание ЭП для файлов произвольного типа;
- добавление ЭП для подписанных файлов;
- заверение ЭП для подписанных файлов;

- создание, добавление, заверение ЭП для файлов PDF в формате CAdES/PAdES;
- проверка ЭП для подписанных файлов с возможностью получения исходного документа;
- использование службы DVCS для проверки ЭП и действительности сертификата ключа проверки подписи;
- шифрование файла произвольного типа;
- извлечение файла;
- универсальные операции:
  - создание ЭП и шифрование файла произвольного типа;
  - извлечение файла и проверка ЭП с возможностью получения исходного документа.

3.2.1 Создание нового запроса на сертификат

Для выполнения операций создания/добавления/заверения ЭП необходимо иметь личный сертификат ключа проверки ЭП.

Сертификат ключа проверки ЭП содержит уникальный номер сертификата ключа проверки ЭП, даты начала и окончания срока действия сертификата, идентификационную информацию о пользователе (в том числе его имя), уникальный ключ проверки ЭП, наименование используемого средства ЭП и наименование удостоверяющего центра (УЦ), который выдал сертификат ключа проверки ЭП.

Ключ ЭП, соответствующий ключу проверки ЭП должен находиться в контейнере на отчуждаемом носителе. В качестве отчуждаемого носителя может использоваться любой носитель (например, сменный носитель с интерфейсом USB и др.).

С помощью ПК «Litoria Desktop 2» можно создать запрос на новый личный сертификат. Для этого надо указать имя выходного файла, 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 так же создание ключевой пары: ключ ЭП – ключ проверки ЭП. Созданный запрос отправляется на рассмотрение в УЦ и на основе него УЦ выпустит сертификат ключа проверки ЭП.

3.2.2 Создание запроса на основе имеющегося сертификата

ПК «Litoria Desktop 2» 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, 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 2» позволяет выполнить установку сертификата ключа проверки подписи на устройство, которое ранее использовалось для создания запроса и содержит контейнер с парой: ключ ЭП – ключ проверки ЭП к этому сертификату.

3.2.4 Просмотр сертификатов в контейнерах

С помощью ПК «Litoria Desktop 2» 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 2» 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 и списков сертификации удостоверяющего центра с локального диска в хранилище сертификатов.

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

С помощью ПК «Litoria Desktop 2» можно выполнить операции установки корневого сертификата 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 Просмотр списка криптопровайдеров

С помощью ПК «Litoria Desktop 2» можно выполнить просмотр установленных на компьютере криптопровайдеров и информацию о них.

3.2.7 Удаление контейнера ключа ЭП

ПК «Litoria Desktop 2» позволяет удалить контейнер ключа ЭП с ключевого отчуждаемого носителя.

3.2.8 Управление настройками комплекса

ПК «Litoria Desktop 2» предоставляет возможность создать настройки для типовых операций: 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.

3.2.9 Создание ЭП

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

Для создания ЭП должен быть осуществлен выбор сертификата ключа проверки подписи 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 проверки подписи и присоединение этих доказательств и их хэш-кодов к подписанному документу;
- получение штампа времени на сформированные доказательства действительности сертификата ключа проверки ЭП.

3.2.10 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 2» существует возможность добавления подписи, созданной на криптографическом алгоритме, отличном от ГОСТ, например, RSA.

3.2.11 Заверение ЭП

ПК «Litoria Desktop 2» 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 заверению подписи аналогична созданию ЭП.

Заверению ЭП возможна лишь для подписанных ранее файлов.

3.2.12 Проверка ЭП

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

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

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

3.2.13 Использование службы DVCS для проверки ЭП и действительности сертификата ключа проверки ЭП

ПК «Litoria Desktop» позволяет получать подтверждение корректности ЭП электронного документа (Validation of Digitally Signed Document – VSD) и подтверждение действительности сертификата ключа проверки подписи (Validation of Public Key Certificates – VPKC) от службы DVCS.

Для обращения к службе необходимо наличие личного сертификата ключа проверки ЭП, зарегистрированного ранее на сервере ДТС. Подписанный указанным личным сертификатом DVCS-запрос отправляется для проверки на сервер службы ДТС. В ответ сервер присылает информацию о действительности ЭП документа или сроке действия сертификата ключа проверки ЭП.

Формирование запросов к службе DVCS происходит в прозрачном для пользователя режиме. При этом отображение результатов проверок пользователю как с использованием службы DVCS, так и без нее, осуществляется в обычном режиме.

Использование службы DVCS для проверки ЭП и действительности сертификата ключа проверки подписи позволяет пользователю не устанавливать списки отзывов сертификатов на локальный компьютер. Проверка ЭП и действительности сертификата ключа проверки ЭП осуществляется на сервере ДТС с выдачей доказательств действительности в виде квитанции. Таким образом, пользователи осуществляют перечисленные проверки в единой точке, контролируемой администратором безопасности, с сохранением всех результатов операций и статистических выборок.

Настройка включения/выключения режима использования службы DVCS для проверки ЭП и действительности сертификата ключа проверки ЭП осуществляется пользователем с правами администратора. Более подробное описание настройки смотрите в документе «ПК «Litoria Desktop». Руководство администратора».

3.2.14 Поддержка электронных документов длительного архивного хранения

Необходимым условием архивного хранения электронных документов является использование усовершенствованной ЭП (УЭП). Формат усовершенствованной электронной подписи предусматривает обязательное включение в реквизиты подписанного документа доказательства момента создания подписи (штамп времени) и действительности сертификата в момент создания подписи. Такую подпись можно успешно проверять в течение срока действия ключа проверки подписи службы штампов времени.

При истечении срока действия ключа проверки подписи службы штампа времени, для длительного архивного хранения электронных документов, подписанных УЭП, к подписи добавляется архивный штамп времени, повышая значимость подписи до формата CAdES-A.

В ПК «Litoria Desktop 2» реализована поддержка электронных документов длительного архивного хранения включая доказательство момента подписи документа и действительность сертификата ключа подписи при создании ЭП и проверке ее корректности и возможность доказательства корректности подписи и целостности файла после истечения срока действия сертификата подписи.

3.2.15 Шифрование файла

Шифрование производится с использованием ключа проверки ЭП, содержащегося в сертификате получателя. Ключ ЭП есть только у владельца использованного сертификата ключа проверки ЭП. Таким образом, при шифровании файла никто, кроме владельца ключа ЭП, не сможет расшифровать файл.

ПК «Litoria Desktop 2» 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.

3.2.16 Извлечение файла

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

3.2.17 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. Таким образом достигается универсальность в интерфейсе и удобство для пользователя.

3.2.18 Универсальная операция извлечения файла и проверки ЭП

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

После выполнения операции пользователю становится доступна следующая информация:

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

3.2.19 Интеграция криптоплатформы в системы документооборота

Криптографическая платформа «Litoria Crypto Platform» является ядром усовершенствованной электронной подписи (УЭП) и предназначена для интеграции в различные системы документооборота, порталы и на серверы приложений с использованием российских и иностранных криптографических алгоритмов с возможностью трансграничного взаимодействия.

При использовании криптографической платформы «Litoria Crypto Platform» разработчику доступны следующие возможности:

- создание, добавление, заверение и проверка электронной подписи (ЭП) различного типа (простая, усовершенствованная, отделенная);
- создание и добавление ЭП документа без предоставления данных (подпись хеша документа);
- шифрование, расшифровывание, гарантированное удаление файлов;
- работа с ключевой информацией и сертификатами (создание сертификата; установка сертификата в заданное хранилище; получение сертификата из хранилища; получение информации о сертификате; проверка статуса сертификата по спискам отзыва сертификатов (СОС) и по Online Certificate Status Protocol (OCSP);
- управление списками отзыва сертификатов: создание, импорт, экспорт, удаление, детальный просмотр;
- применение для работы с ЭП различных криптопровайдеров, как программных (Base CSP, КриптоПро CSP, ViPNet CSP, ВАЛИДАТА CSP, Avest CSP и др.), так и аппаратных (JaCarta, eToken ГОСТ, РУТОКЕН ЭЦП);
- реализация функций службы актуальных статусов сертификатов согласно RFC2560 «Online Certificate Status Protocol (OCSP)»;

- реализация функций службы штампов времени согласно RFC3161 «Time-Stamp Protocol (TSP)»;
- формирование и проверка ЭП электронных сообщений в соответствии со спецификацией RFC3029 «Data Validation and Certification Server Protocol (DVCS)»;
- интеграция сервисов пролонгации;
- интеграция в системы электронного документооборота, включая SharePoint, Citrix, веб-сервер MS IIS (Internet Information Servies);
- предоставление интерфейсов (Com, Java, C#, SilverLight, ASP.net) для встраивания в различные среды и системы.

4 Входные и выходные данные

4.1 Входные данные

Входные данные для ПК «Litoria Desktop 2» отличаются друг от друга в зависимости от выполняемой операции. В таблице 4.1 приведены входные данные для основных функций комплекса.

Таблица 4.1. Входные данные

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

[1] В качестве ключевого носителя может использоваться любой носитель, например, реестр ОС, 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).	
Создание ЭП	1. Файл произвольного типа. 2. Сертификат подписчика (указанный вручную). 3. Параметры подписи (указанные вручную).	Для выполнения данной функции необходимо наличие ключевого носителя, содержащего контейнер ключа ЭП, на основе которого будет сформирован и подписан запрос.
Добавление ЭП Заверение ЭП	1. Подписанный файл. 2. Сертификат подписчика (указанный вручную). 3. Параметры подписи (указанные вручную).	Для выполнения данной функции необходимо наличие ключевого носителя, содержащего контейнер ключа ЭП, на основе которого будет сформирован и подписан запрос.
Проверка ЭП	1. Подписанный файл. 2. Параметры проверки подписи (указанные вручную).	
Шифрование	1. Файл произвольного типа. 2. Сертификаты получателей (указанные вручную). 3. Настройки шифрования (указанные вручную).	
Извлечение	1. Зашифрованный файл.	

Функция	Входные данные	Примечание
Создание ЭП и шифрование файла.	1. Файл произвольного типа. 2. Сертификат подписчика (указанный вручную). 3. Сертификаты получателей (указанные вручную). 4. Параметры подписи (указанные вручную). 5. Настройки шифрования (указанные вручную).	
Извлечение 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 2» формируются файлы с расширениями, указанными в настройках. Расширения, которые указаны по умолчанию, приведены в таблице 4.2.

Таблица 4.2. Типы и описания файлов

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

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 извлечения и снятия ЭП.