ГАЗИНФОРМ СЕРВИС

Программный комплекс «Litoria Desktop 2»
Описание применения

Санкт-Петербург, 2022

Аннотация

Настоящий документ содержит сведения о применении программного комплекса «Litoria Desktop 2» версия 2.8.7-1 (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 условия, необходимые для использования комплекса, требования к аппаратным средствам автоматизированного рабочего места (АРМ).

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 зашифрованных 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, в т.ч. запроса, подписанного актуальной ЭП; установки сертификата на устройство; установки сертификата из устройства в реестр; просмотра установленных криптопровайдеров и их параметров; продления срока доверенного архивного хранения подписанных электронных документов, использования службы доверенной третьей стороны (ДТС) для проверки ЭП.

ПК «Litoria Desktop 2» поддерживает работу с USB-токенами, представленными в таблице 1.1.

Таблица 1.1 – Поддержка работы с носителями в зависимости от ОС, в которой функционирует ПК «Litoria Desktop 2»

Операционные системы	**Носитель**
Windows	Рутокен S, Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен Lite; JaCarta PKI, JaCarta ГОСТ, JaCarta LT; eToken NG-FLASH (Java), eToken PRO, eToken PRO (Java), eToken ГОСТ; ESMART Token USB 64K
Linux	ruToken S, ruToken ЭЦП, ruToken ЭЦП 2.0, ruToken Lite

ПК «Litoria Desktop 2» поддерживает обращение к функциональным ключевым носителям через интерфейс PKCS#11[1].

[1] Корректная работа с интерфейсом PKCS#11 в ПК «Litoria Desktop 2» осуществляется только для ruToken ЭЦП и ruToken ЭЦП 2.0.

2 Условия применения

2.1 Требования к среде функционирования

ПК «Litoria Desktop 2» функционирует под управлением следующих операционных систем (ОС) Microsoft Windows:

- Windows 7 (32 бит/64 бит) [2];
- Windows 8/8.1 (32 бит/64 бит);
- Windows 10 (32 бит/64 бит).
- Windows Server 2008 R2;
- Windows Server 2012/2012R2/2016/2019 (64 бит).

и ОС семейств Linux, поддерживающих системную библиотеку GNU C Library (Glibc) версии не ниже 2.22.

Гарантирована работа ПК «Litoria Desktop 2» на следующих ОС семейств Linux:

- AltLinux версии 8.2 или выше (64 бит);
- Ubuntu версии 16 или выше (64 бит);
- RedOS версии 7.1 или выше (64 бит);
- Astra Linux Special Edition версии 1.6 (64 бит);
- Astra Linux Common Edition версии 2.12.42 или выше (64 бит).

2.2 Требования к аппаратному и программному обеспечению

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

При использовании аппаратных идентификаторов необходимо наличие на рабочей станции USB-порта.

Для корректного отображения ПК «Litoria Desktop 2» рекомендуется использовать разрешение экрана монитора не менее 1280x960 пикселей.

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 драйверы для аппаратных СКЗИ – «Криптотокен» в составе изделия «eToken

[2] Срок эксплуатации ОС определяется сроками выпуска обновлений критических уязвимостей.

ГОСТ» или «РУТОКЕН ЭЦП».

3 Описание задачи

3.1 Определение задачи

Электронная подпись 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 драйверы 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 работы с ЭП.

Для подготовки АРМ к работе с ЭП ПК «Litoria Desktop 2» предоставляет пользователю возможность выполнить следующие функции:

- создание нового запроса на сертификат, в т.ч. подписанного актуальной ЭП;
- 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 списку отзыва сертификатов (COC) и по протоколу OCSP в реальном времени;
- просмотр списка криптопровайдеров;
- управление контейнерами (импорт сертификатов в контейнер, экспорт сертификатов из контейнера, в том числе с экспортированием ключей);
- управление настройками комплекса.

Для работы с ЭП комплекс обеспечивает выполнение следующих функций:

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

- создание, добавление, заверение ЭП для документов в соответствии со стандартами CAdES (согласно RFC 5126) и PAdES (согласно ETSI as TS 102 778)[3];
- создание, добавление, заверение ЭП для xml документов в соответствии со стандартами CAdES (согласно RFC 5126) и XAdES (согласно ETSI as TS 101 903);
- проверка ЭП для подписанных файлов с возможностью получения исходного документа;
- использование службы ДТС для проверки ЭП;
- 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;
- поддержка электронных документов длительного архивного хранения.

Для проверки целостности и достоверности при передаче данных заказчику комплекс обеспечивает возможность хеширования файлов по алгоритмам ГОСТ.

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 криптопровайдер, имя ключевого контейнера и ПИН-код к контейнеру, 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.

Также ПК «Litoria Desktop 2» позволяет создать запрос на сертификат на основе

[3] Операции заверения для pdf документов по стандарту PAdES недоступны.

предустановленного шаблона и возможность подписи создаваемого запроса имеющейся актуальной 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 криптопровайдер, имя ключевого контейнера и ПИН-код к контейнеру, 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 и пользовательскими 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 отозванных сертификатов с локального диска в хранилище сертификатов.

Экспорт – это копирование сертификатов и списков отозванных сертификатов из хранилища сертификатов на локальный диск.

С помощью функции *Импорт* можно установить сертификаты или списки отзыва (с расширениями *.cer, *.crl, *.crt, *.p7b) и сертификаты из файлов обмена ключевой информации (*.pfx):

1) сертификаты доверенных корневых центров сертификации и промежуточных центров сертификации в хранилища *«Доверенные корневые центры сертификации»* и *«Промежуточные центры сертификации»* соответственно;

2) списки отозванных сертификатов в хранилище сертификатов «*Списки*

отозванных сертификатов»;

3) личные сертификаты из файлов, полученных от УЦ в ответ на отправленный запрос, в хранилище сертификатов *«Личные сертификаты»*;

4) личные сертификаты из pfx-контейнеров в хранилище сертификатов *«Личные сертификаты»*, при этом создается контейнер с необходимыми ключами.

3.2.6 Просмотр списка криптопровайдеров

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

ПК «Litoria Desktop 2» поддерживает работу с криптографическими алгоритмами, приведенными в таблице 3.1.

Таблица 3.1 – Криптографические алгоритмы, поддерживаемые ПК «Litoria Desktop 2»

Алгоритм	**Длина ключа**	**ОС**
КриптоПро ГОСТ Р 34.10-2012	512, 1024	Windows/Linux
КриптоПро ГОСТ Р 34.10-2001	512	Windows/Linux
RSA	384-16384	Windows/Linux
CNG RSA	512-4096	Windows
CNG ECDSA_P256	256	Windows
CNG ECDSA_P384	384	Windows
CNG ECDSA_P521	521	Windows

3.2.7 Управление контейнерами

ПК «Litoria Desktop 2» предоставляет возможность импортировать сертификаты в контейнеры, экспортировать сертификаты из контейнеров в заданный файл (в том числе с экспортированием ключевой информации), а также удалять контейнеры 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 стандарт PAdES при создании и проверке подписи pdf-документов и другое.

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 меткой доверенного времени на значение ЭП;
- создание с доказательством действительности сертификата.

Процесс создания ЭП с доказательством действительности сертификата делится на следующие этапы:

- создание ЭП;
- получение метки доверенного времени на значение ЭП;
- сбор доказательств действительности сертификата ключа проверки подписи и присоединение этих доказательств и их хеш-кодов к подписанному документу;
- получение метки доверенного 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.

Заверение ЭП возможно лишь для подписанных ранее файлов.

3.2.12 Проверка ЭП

Проверка ЭП подразумевает подтверждение подлинности электронной подписи в

электронном документе, то есть:

- принадлежность электронной подписи в электронном документе владельцу сертификата ключа проверки подписи;
- отсутствие искажений в электронном документе, который подписан данной ЭП;
- 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 ЭП с доказательством действительности сертификата файла с отделенной подписью – проверка корректности самого файла подписи.

3.2.13 Использование службы ДТС для проверки ЭП

ПК «Litoria Desktop 2» позволяет получать подтверждение корректности ЭП электронного документа (Validation of Digitally Signed Document – VSD) от службы ДТС.

Для обращения к службе необходимо наличие сертификата ключа проверки ЭП, зарегистрированного ранее на сервере ДТС. Подписанный указанным сертификатом DVCS-запрос отправляется для проверки на сервер службы ДТС. При этом, если найден подходящий криптопровайдер, используется хеширование подписанного файла. В ответ сервер присылает информацию о действительности ЭП документа.

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

Использование службы ДТС для проверки ЭП позволяет пользователю не устанавливать списки отзывов сертификатов на локальный компьютер. Проверка 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 ДТС для проверки ЭП осуществляется пользователем с правами администратора. Более подробное описание настройки смотрите в документе «ПК «Litoria Desktop 2». Руководство администратора».

3.2.14 Поддержка электронных документов длительного архивного хранения

Необходимым условием архивного хранения электронных документов является использование ЭП с доказательством действительности сертификата. Такой формат подписи предусматривает обязательное включение в реквизиты подписанного документа доказательства момента создания подписи (метку доверенного 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 ЭП с доказательством действительности сертификата, к подписи добавляется архивная метка доверенного времени, повышая значимость подписи до стандарта CAdES-A.[4]

В ПК «Litoria Desktop 2» реализована поддержка электронных документов длительного архивного хранения включая доказательство момента подписи документа 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

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

[4] Архивное хранение pdf документа по стандарту PAdES не осуществляется.

пользователя.

3.2.18 Универсальная операция извлечения файла и проверки ЭП

Данная операция выполняется в два этапа: 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 Вычисление контрольных сумм файлов

С помощью ПК «Litoria Desktop 2» возможно вычисление хеш-суммы для любого файла по алгоритмам хеширования ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 с длиной хеш-кода 256 бит и ГОСТ Р 34.11-2012 с длиной хеш-кода 512 бит.

Расчет хеш-сумм файлов необходим для проверки целостности и достоверности при передаче данных заказчику.

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[5].
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 иметь в наличии чистый ключевой носитель.
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.

[5] В качестве ключевого носителя может использоваться любой носитель, например, реестр ОС, сменный носитель с интерфейсом USB и др.

Функция	Входные данные	Примечание
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.
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.
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.
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.	
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).	

Функция	Входные данные	Примечание
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	• В ОС Windows зависимости от заданных настроек (по умолчанию p7s). • В ОС Linux – lp7s	Подписан в DER-кодировке или в BASE64-кодировке
	Зашифрованный файл	• В ОС Windows зависимости от заданных настроек (по умолчанию p7m). • В ОС Linux – lp7m	Зашифрован в DER-кодировке или в BASE64-кодировке
	Подписанный и зашифрованный файл	• В ОС Windows зависимости от заданных настроек (по умолчанию p7s. p7m). • В ОС Linux – lp7s. lp7m	Подписан и зашифрован в DER-кодировке или в BASE64-кодировке

Новое расширение назначается файлу 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.

При операциях создания и добавления подписи в ПК «Litoria Desktop 2» для pdf документов возможно создание подписи по стандарту PAdES, по умолчанию для pdf документов создается подпись по стандарту CAdES (подробное описание настройки подписи pdf документов приведено в документах «ПК «Litoria Desktop 2». Руководство администратора» и «ПК «Litoria Desktop 2». Руководство пользователя»).

Операции заверения pdf документов по стандарту PAdES недоступны.

Перечень сокращений

АРМ	–	Автоматизированное Рабочее Место
ГОСТ	–	ГОсударственный СТандарт
ДТС	–	Доверенная Третья Сторона
ОС	–	Операционная Система
ПИН	–	Персональный Идентификационный Номер
ПК	–	Программный комплекс
СКЗИ	–	Средство Криптографической Защиты Информации
СОС	–	Список Отзыва Сертификата
УЦ	–	Удостоверяющий Центр
ЭП	–	Электронная Подпись
DVCS	–	Data Validation and Certification Server (сервер проверки достоверности данных и сертификации)
OSCP	–	Online Certificate Status Protocol (протокол для проверки статуса сертификата электронной подписи)
PDF	–	Portable Document Format (межплатформенный открытый формат электронных документов)
PKCS	–	Public Key Cryptography Standards (криптографические стандарты открытого ключа)
RSA	–	Аббревиатура от фамилий Rivest, Shamir и Adleman (криптографический алгоритм с открытым ключом)
TSP	–	Time-Stamp Protocol (протокол штампа времени)
VSD	–	Validation of Digitally Signed Document (подтверждение корректности ЭП электронного документа)

Термины и определения

CAdES – Стандарт ЭП, являющийся расширенной версией стандарта CMS.
CMS (Cryptographic Message Syntax) утвержден в RFC5652 вместо устаревшего стандарта RSAPKCS#7. Синтаксис CMS описывает способы формирования криптографических сообщений, в результате чего сообщение становится полностью самодостаточным для его открытия и выполнения всех необходимых операций.
Стандарт CAdES сохраняет существующую структуру ЭП формата CMS, добавляя только подписываемые или не подписываемые атрибуты. ЭП с доказательством действительности сертификата предоставляет возможность осуществления:
- множественной подписи (данные могут быть подписаны несколькими сторонами);
- подписания не только данных, но и некоторых атрибутов сообщения (хеша сообщения, времени подписи, значения другой подписи).

Формат CAdES определен в RFC5126 «CMS Advanced Electronic Signatures (CAdES)».

DVCS-запрос – Электронный документ, подписанный ЭП пользователя (сертификат ЭП должен быть зарегистрирован в службе DVCS), содержащий сведения, зависящие от типа запроса, который направляется для проверки на сервер проверки подлинности.

PAdES	– Стандарт ЭП, представляющий собой набор ограничений и расширений для PDF и ISO 32000-1. ЭП на основе PAdES, имеет статус передовой электронной подписи. Это означает, что: – подпись однозначно связана с подписавшим; – способность идентифицировать подписавшего; – только подписавшая сторона контролирует данные, используемые для создания подписи; – возможность идентификации, если данные, прикрепленные к подписи, были изменены после подписания. Формат PAdES определен в ETSI TS 102 778-1 V1.1.1 (2009-07) «PDF Advanced Electronic Signatures (PAdES)».
XAdES	– Стандарт ЭП, основанный на стандарте XML DSig. XML DSig является основой для цифровой подписи документов и рекомендован консорциумом W3C. Фактически XML DSig решает те же задачи, что и PKCS#7 (т.е. утверждает целостность информации и неотрекаемость обладателя ЭП), но областью применения XML DSig являются веб-приложения и веб-сервисы.
Ключ ЭП	– Уникальная последовательность символов, предназначенная для создания ЭП.
Ключ проверки ЭП	– Уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП.
Простая ЭП	– По Федеральному закону №63-ФЗ, простая ЭП получена посредством использования кодов, паролей или иных средств, и подтверждает факт формирования электронной подписи определенным лицом.
Сертификат ключа проверки ЭП	– Электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом УЦ и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.
Служба штампов времени	– Доверенный субъект инфраструктуры открытых ключей, обладающий точным и надежным источником времени и оказывающий услуги по созданию меток доверенного времени.

Список отозванных сертификатов, список отзыва (COC, CRL)	–	Электронный документ с электронной подписью уполномоченного лица удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были аннулированы (отозваны) или действие которых было приостановлено.
Удостоверяющий центр	–	Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки ЭП, а также иные функции, предусмотренные Федеральным законом №63-ФЗ от 06.04.2011 г. «Об электронной подписи».
ЭП с доказательством действительности сертификата	–	Предусматривает включение в электронную подпись информации о времени создания подписи (TSP) и о статусе сертификата электронной подписи (OCSP) в момент подписания (действителен или отозван).
Хеш-функция	–	Алгоритм, конвертирующий строку произвольной длины (сообщение) в битовую строку фиксированной длины, называемой *хеш-кодом*, проверочной суммой или цифровым отпечатком.
Метка доверенного времени	–	Достоверная информация в электронной форме о дате и времени подписания электронного документа электронной подписью, создаваемая службой штампов времени и полученная в момент подписания электронного документа электронной подписью.
Электронная подпись	–	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.