ГАЗИНФОРМ СЕРВИС

Программное обеспечение «Litoria Crypto Service 2»
Описание применения

Санкт-Петербург, 2023

Аннотация

Настоящий документ содержит описание применения программного обеспечения «Litoria Crypto Service 2» версия 2.2.1.1 (далее – ПО «Litoria Crypto Service 2» или приложение).

В документе приведено назначение приложения и перечислены предоставляемые возможности.

В разделе «Условия применения» указаны условия, необходимые для использования приложения, и требования к аппаратным и программным средствам рабочих станций, на которых будет использоваться ПО «Litoria Crypto Service 2».

В разделе «Описание задачи» описана задача, решаемая при применении приложения, и основные функции приложения.

В разделе «Входные и выходные данные» указаны входные и выходные данные ПО «Litoria Crypto Service 2».

В конце документа приведен список использованных сокращений.

Содержание

1 Назначение ПО «Litoria Crypto Service 2»

Основным назначением ПО «Litoria Crypto Service 2» является предоставление пользователю доступа к базовым функциям криптографической платформы «Litoria Crypto Platform» через REST интерфейс.

ПО «Litoria Crypto Service 2» предоставляет пользователю в системе документооборота возможность интеграции криптографических функций в сторонние приложения посредством REST интерфейса.

Базовые функции криптографической платформы «Litoria Crypto Platform» включают в себя операции создания электронной подписи (ЭП) и шифрования, извлечения и проверки ЭП (в том числе локальная проверка ЭП с машиночитаемой доверенностью (МЧД), функции просмотра хранилища сертификатов; создания запроса на выпуск сертификата; установки сертификата из устройства в хранилище; просмотра установленных криптопровайдеров и их параметров; пролонгации подписи; использования службы доверенной третьей стороны (ДТС) для проверки ЭП (в том числе проверка ЭП с МЧД с использованием службы ДТС), просмотр информации о МЧД.

2 Условия применения

2.1 Требования к техническим средствам

Минимальные требования к рабочей станции, на которую устанавливается ПО «Litoria Crypto Service 2», обусловлены применением используемых ОС.

2.2 Требования к программному обеспечению

ПО «Litoria Crypto Service 2» функционирует под управлением следующих ОС:

– Windows 7 (32 бит/64 бит)[1];
– Windows 8/8.1 (32 бит/64 бит);
– Windows 10 (32 бит/64 бит).
– Windows Server 2008 R2;
– Windows Server 2012/2012R2/2016R2/2019R2/2022 (64 бит);

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

Гарантирована работа ПО «Litoria Crypto Service 2» на следующих ОС семейств Linux:

– AltLinux версии 8.2 или выше (64 бит);
– Ubuntu версии 16 или выше (64 бит);
– RedOS версии 7.2, 7.3 (64 бит);
– Astra Linux Special Edition версии 1.6, 1.7 (64 бит).

Дополнительно должно быть установлено следующее программное обеспечение:

– Средство криптографической защиты информации, реализованное в соответствии с технологией Microsoft CSP (при работе с отечественной криптографией необходимо использовать соответствующие СКЗИ)[2].

– СКЗИ «КриптоПро CSP» с поддержкой графического представления или ViPNet CSP.[3]

– СУБД Postgre SQL.

Рекомендуется установка Advanced REST Client или любого другого REST клиента.

Для web-активации сервиса лицензирования необходим Chrome совместимый браузер.

[1] Срок эксплуатации ОС определяется сроками выпуска обновлений критических уязвимостей.
[2] При функционировании ПО на ОС семейства Windows.
[3] При функционировании ПО на ОС семейства Linux.

3 Описание задачи

3.1 Определение задачи

Электронный документооборот – механизм по работе с документами в электронном виде, т.е. движение документов в организации с момента их создания (или получения) до завершения исполнения (или отправления), а также способ организации работы с документами, при котором основная масса документов организации (предприятия) используется в электронном виде и хранится централизованно.

При использовании функций ПО «Litoria Crypto Service 2» осуществляется защита системы электронного документооборота (СЭД) от угрозы нарушения целостности (повреждение, уничтожение и/или искажение информации) и конфиденциальности (несанкционированного доступа).

3.2 Основные функции приложения

При использовании ПО «Litoria Crypto Service 2» пользователю доступен весь комплект необходимых функций для работы с ЭП:

- создание запроса на сертификат, в т.ч. самоподписанного;
- просмотр сертификатов в контейнерах;
- установка сертификата в хранилище сертификатов;
- управление сертификатами:
- просмотр списка криптопровайдеров;
- создание ЭП и шифрование для файлов произвольного типа;
- добавление ЭП для подписанных файлов;
- извлечение и проверка ЭП для подписанных файлов с возможностью получения исходного документа;
- пролонгация подписи, в случае истечения срока действия;
- использование службы ДТС для проверки ЭП.

3.2.1 Управление ключевой информацией и сертификатами

С помощью приложения можно выполнять следующие функции с сертификатами:

- получение сертификата(-ов) из хранилища;
- установка сертификата в заданное хранилище;
- удаление сертификата из хранилища;
- получение информации о сертификате;
- создание запроса на сертификат или самоподписанного сертификата.

3.2.2 Управление списком криптопровайдеров

С помощью приложения можно выполнить просмотр установленных на компьютере криптопровайдеров и получить информацию о них.

3.2.3 Подпись и шифрование файла

Приложение предоставляет возможность одновременного создания ЭП и шифрования файла.

Для создания ЭП должен быть осуществлен выбор сертификата ключа проверки подписи и параметров создания ЭП (отделенная ЭП или совмещенная, с вложенным штампом времени, усовершенствованная ЭП).

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.

3.2.4 Пролонгация подписи

В ПО «Litoria Crypto Service 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.

При истечении срока действия ключа проверки подписи службы штампа времени, для продления срока доверенного архивного хранения электронных документов, предоставляется возможность добавления к подписи архивного штампа времени.

3.2.5 Проверка подписи

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.

В том числе возможна проверка ЭП с машиночитаемой доверенностью.

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

3.2.6 Извлечение данных

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.

3.2.7 Присоединение подписи

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.

3.2.8 Использование службы ДТС для проверки ЭП

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

При наличии машиночитаемой доверенности (МЧД) также осуществляется проверка соответствия полномочий, определенных МЧД, в соответствии с требованиями Федерального закона № 63-ФЗ и соответствующих подзаконных актов.

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.

3.2.9 Получение информации о МЧД

МЧД – доверенность, созданная в электронной форме и подписанная электронной подписью лица, уполномоченного на действия от имени участника информационного обмена без доверенности. В МЧД указываются именно те полномочия, которые руководитель доверяет конкретному представителю.

ПО «Litoria Crypto Service 2» позволяет получить информацию о машиночитаемой доверенности при ее наличии в ЭП.

4 Входные и выходные данные

4.1 Входные данные

ПО «Litoria Crypto Service 2» выполняет функции шифрования/извлечения и создания/проверки ЭП файлов следующего типа:

- файл любого типа *.* (для генерации ЭП);
- подписанные ЭП файлы (совмещенная/отделенная ЭП);
- файл сертификата.

4.2 Выходные данные

На выходе ПО «Litoria Crypto Service 2» может формировать следующую информацию:

- байтовый массив данных (обработанный оригинал файла с ЭП);
- байтовый массив данных (файлы отделенных ЭП);
- сертификаты (из ЭП);
- сообщение об ошибке (если она имеет место).

Перечень сокращений

CSP	–	Cryptographic Service Provider (провайдер криптографических услуг, криптопровайдер)
DVCS	–	Data Validation and Certification Server (сервер сертификации и проверки достоверности данных)
VSD	–	Validation of digitally Signed Document (проверка цифрового подписанного документа)
ДТС	–	Доверенная Третья Сторона
ОС	–	Операционная Система
ПО	–	Программное Обеспечение
СКЗИ	–	Средство Криптографической Защиты Информации
СЭД	–	Система Электронного Документооборота
ЭП	–	Электронная Подпись