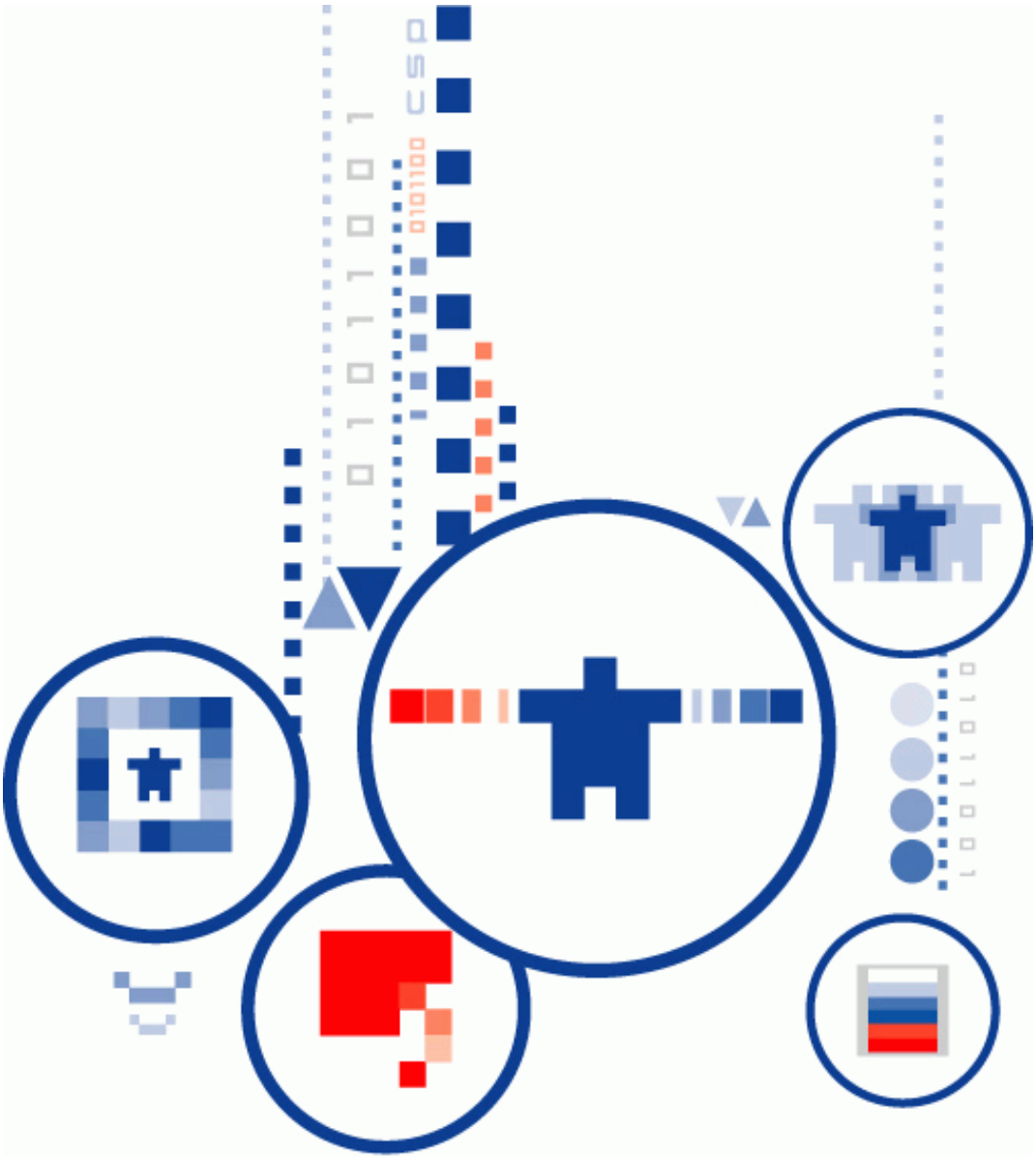

Программное обеспечение

«КриптоПро Архив»

Общее описание

СОДЕРЖАНИЕ

1. Аннотация 5
2. Общие сведения 6
2.1. Назначение КриптоПро Архив 6
2.2. Цели КриптоПро Архив 6
2.3. Задачи КриптоПро Архив 6
3. Описание КриптоПро Архив 8
3.1. Состав КриптоПро Архив 8
3.2. Описание компонентов КриптоПро Архив 9
4. Аутентификация в КриптоПро Архив 14
5. Архитектура решения КриптоПро Архив 15
6. Системные требования 15
6.1. Аппаратное обеспечение 15
6.2. Программное обеспечение 15
7. Система ролей в КриптоПро Архив 16
8. Поддерживаемые типы ЭП и форматы документов 18

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

CAdES	—	Расширенная версия стандарта электронной подписи CMS (CMS Advanced Electronic Signatures)
CRL	—	Список отзыва сертификатов (Certificate Revocation List)
CSP	—	Криптопровайдер (Cryptographic Service Provider)
OCSP	—	Протокол получения статуса сертификата в реальном времени (Online Certificate Status Protocol)
REST	—	Архитектурный стиль построения распределенного приложения (Representational State Transfer)
RFC	—	Рекомендация Internet Engineering Task Force (Request for Comments)
SDK	—	Набор программных компонентов для использования в мобильных приложениях (Software development kit)
TLS	—	Протокол защиты транспортного уровня (Transport Layer Security)
URL	—	Единый указатель ресурсов (Uniform Resource Locator)
АРМ	—	Автоматизированное рабочее место
БД	—	База данных
ИС	—	Информационная система
ОС	—	Операционная система
ПО	—	Программное обеспечение
СКЗИ	—	Средство криптографической защиты информации
СУБД	—	Система управления базой данных
ЭП	—	Электронная подпись

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Владелец сертификата открытого ключа	—	лицо, которому в установленном Федеральным законом (№63-ФЗ от 06.04.2011 г. «Об электронной подписи») порядке выдан сертификат открытого ключа.
Закрытый ключ	—	уникальная последовательность символов, предназначенная для шифрования.
Квалифицированный сертификат открытого ключа (квалифицированный сертификат)	—	сертификат открытого ключа, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.
Ключ проверки электронной подписи	—	уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.
Ключ электронной подписи	—	уникальная последовательность символов, предназначенная для создания электронной подписи
Средства электронной подписи	—	шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание закрытого и открытого ключей.
Сертификат открытого ключа	—	электронный или бумажный документ, содержащий открытый ключ, информацию о владельце ключа,

		области применения ключа, подписанный выдавшим его Удостоверяющим центром и подтверждающий принадлежность открытого ключа владельцу.
Удостоверяющий центр	—	юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов открытых ключей, а также иные функции, предусмотренные Федеральным законом №63-ФЗ от 06.04.2011 г. «Об электронной подписи».
Учетная запись	—	Набор сведений о Пользователе КриптоПро Архив, содержащий необходимое и достаточное для работы с ПО количество информации.
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.

1. Аннотация

В настоящее время почти каждая организация использует электронный документооборот — как внешний, так и внутренний. При этом определить истинное авторство документа и убедиться в том, что он не был изменен в процессе своего жизненного цикла позволяет использование электронной подписи. Хранение, в том числе и долговременное, является частью жизненного цикла многих видов электронных документов, подписанных электронной подписью. Однако, для этого необходимо решить задачу сохранения юридической значимости документа, подписанного электронной подписью в процессе хранения.

Настоящий документ содержит описание программного обеспечения (ПО) «КриптоПро Архив», которое предназначено для подготовки электронных подписей документов, к долговременному хранению и сохранению юридической значимости документов.

В данном документе приведено назначение ПО и основные решаемые им задачи, описаны входящие в него компоненты и архитектура предлагаемого решения. Описаны системные требования к продукту и возможности интеграции с другими ИС.

Документ предназначен для руководителей и администраторов как ознакомительный материал перед установкой и эксплуатацией программного обеспечения КриптоПро Архив.

2. Общие сведения

2.1. Назначение КриптоПро Архив

Программное обеспечение «КриптоПро Архив» (далее — КриптоПро Архив) предназначено для:

- подготовки электронной подписи документов, к временному (до 10 лет), долговременному (свыше 10 лет) и постоянному централизованному хранению;
- усовершенствования электронных подписей документов форматов CAdES-BES, CAdES-T, CAdES-C, CAdES-XLT1 до формата CAdES-E-A, для обеспечения юридической значимости документов при их длительном хранении за счет использования хранящихся в подписи доказательств подлинности и заверяющих их архивных меток(штампов) времени;
- контроля сроков действия доказательств юридической значимости документов при их длительном хранении и при необходимости – их автоматическое обновление;
- приема и передачи информации о контейнерах электронных документов временного, долговременного и постоянного хранения между Системой и внешними ИС;
- контроля сроков хранения контейнеров документов, установленных законодательством.

2.2. Цели КриптоПро Архив

Целями использования КриптоПро Архив являются:

- Обеспечение целостности документов;
- Обеспечение аутентичности (подлинности) документов;
- Обеспечение юридически значимого электронного документооборота за счет улучшения существующих электронных подписей документов до стандарта CAdES-E-A и автоматического обновления подтверждений доказательств подлинности электронной подписи документов.

2.3. Задачи КриптоПро Архив

Для выполнения поставленных целей КриптоПро Архив решает следующие задачи:

- обеспечивает прием документов от внешних ИС, подписанных электронной подписью, при этом учетной единицей электронных документов в Системе является контейнер электронного документа. Контейнер электронного документа содержит электронную подпись документа, значение хэш-функции документа и его метаданные;
- обеспечивает проверку исходных подписей документа;
- обеспечивает преобразование электронных подписей документов в контейнере электронных документов для долговременного хранения, путем преобразования исходной ЭП документа в формат CADES-E-A.
- обеспечивает создание и хранение базы данных о не менее чем 10 000 000 контейнеров электронных документов, поступивших на долговременное хранение с возможностью расширения базы данных;
- обеспечивает возможность интеграции с ней нескольких внешних ИС через предоставляемое ею API;

- поддерживает работу с внешними системами хранения данных (СХД) для хранения обработанных контейнеров электронных документов через Плагин подключения к внешней СХД;
- выполняет функцию создания резервной копии базы данных с информацией о обработанных контейнерах электронных документов;
- осуществляет поиск информации о контейнерах электронных документов, выдавать описательную информацию;
- определяет и показывает информацию о контейнерах электронных документов, подготовленных к долговременному хранению, включая сведения о проверке ЭП этих документов;
- отслеживает статус поступившего в Систему контейнера электронного документа;
- поддерживает горизонтальное масштабирование своих основных компонентов.

3. Описание КриптоПро Архив

3.1. Состав КриптоПро Архив

КриптоПро Архив включает в себя следующие компоненты (см. Рисунок 1):

- "Модуль управления обработкой документов с электронной подписью" (см. раздел 3.2.1):
  - ПО Модуля;
  - БД Модуля.
- "Модуль обеспечения доказательствами действительности электронной подписи" (см. раздел 3.2.2):
  - ПО Модуля;
  - КриптоПро CSP
  - КриптоПро TSP Client (Компонент из состава ПАК «Службы УЦ 2.0», используется опционально и при наличии действующего сертификата, выданного ФСБ России);
  - КриптоПро OCSP Client (Компонент из состава ПАК «Службы УЦ 2.0», используется опционально и при наличии действующего сертификата, выданного ФСБ России);
- Модуль Администрирования (см. раздел 3.2.3)
  - ПО Модуля;
  - Веб-интерфейс Администратора.
- Модуль Архив УЦ (см. раздел 3.2.4).
  - ПО Модуля;
  - Веб-интерфейс Оператора.

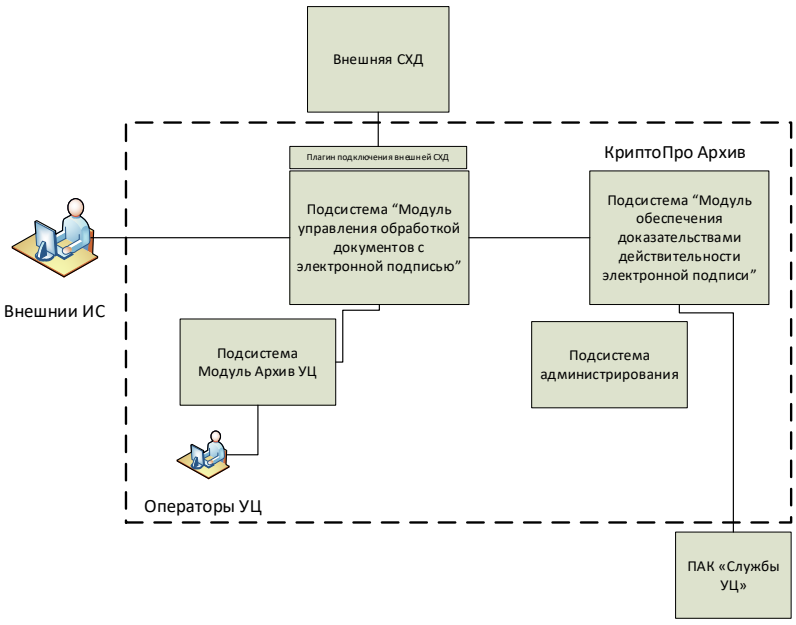

Рисунок 1 Компоненты КриптоПро Архив

Не все указанные компоненты являются обязательными. В минимальную конфигурацию КриптоПро Архив входят Модуль управления обработкой документов с электронной подписью, Модуль обеспечения доказательствами действительности электронной подписи, Веб-интерфейс Администратора. Модуль Архив УЦ является опциональным компонентом. Установщик КриптоПро Архив позволяет выбрать и

установить нужные компоненты. КриптоПро CSP, TSP Client, OCSP Client входят в комплект поставки.

3.2. Описание компонентов КриптоПро Архив

3.2.1. Модуль управления обработкой документов с электронной подписью

Модуль предназначен для приема/передачи контейнеров электронных документов между «КриптоПро Архив» версии 1.0» и внешними ИС, хранения контейнеров электронных документов, поиска информации и управления контейнерами электронных документов, а также автоматизированного взаимодействия с модулем обеспечения доказательствами подлинности электронной подписи.

Модуль:

- осуществляет прием от внешних ИС не менее 100 Гб электронных документов в сутки, при условии обеспечения, соответствующих этой нагрузке каналов связи и серверного оборудования;
- поддерживает возможность одновременной работы с нескольким ИС, передающими контейнеры электронных документов для долговременного хранения;
- имеет возможность принимать документ по ссылке из внешнего источника;
- рассчитывает значение хэш-функции исходного документа;
- отсоединяет присоединенную к документу электронную подпись;
- осуществляет взаимодействие с ИС и другими подсистемами в асинхронном режиме и с поддержкой очередей сообщений.
- при приеме контейнера электронного документа от ИС в качестве ответа возвращает уникальный идентификатор контейнера в «КриптоПро Архив» версии 1.0»;
- обеспечивает доступ внешних ИС к информации о контейнере электронного документа, доказательствах подлинности и статусе обработки переданного контейнера электронного документа в «КриптоПро Архив» версии 1.0»;
- позволяет производить поиск информации о контейнерах документов по метаданным, выдавать описательную информацию;
- отслеживает изменение статуса контейнера документа в процессе подготовки к долговременному хранению.
- фиксирует время попадания контейнера электронного документа в Систему;
- фиксирует временя и результат передачи улучшенной подписи электронного документа во внешнюю СХД.

Каждый контейнер документа, помимо электронной подписи документа содержит как минимум следующие метаданные:

- идентификатор контейнера (добавляется при внесении в «КриптоПро Архив» версии 1.0» автоматически);
- название контейнера;
- статус (добавляется при внесении в «КриптоПро Архив» версии 1.0» автоматически, см. Рисунок 2);
- тип файла в контейнере (добавляется при внесении в «КриптоПро Архив» версии 1.0» автоматически);

- внешняя ИС от которой получен;
- ссылка на внешнее хранилище документа, если в качестве исходного документа передавалась ссылка на место его хранения (добавляется при внесении в «КриптоПро Архив» версии 1.0» автоматически);
- значение хэш-функции документа (добавляется при внесении в «КриптоПро Архив» версии 1.0» автоматически);
- отдел/структурное подразделение, передавшее контейнер в «КриптоПро Архив» версии 1.0»;
- пользователь ИС, передавший контейнер документа на временное или постоянное хранение;
- пользователь (пользователь внешней ИС, ограничение пользования/доступа);
- владелец (пользователь внешней ИС, полный доступ/разрешение внесения изменений);
- Тип хранения документа (временного или постоянного хранения);
- дата Создания;
- дата Внесения на хранение (добавляется при внесении в «КриптоПро Архив» версии 1.0» автоматически);
- дата и время передачи улучшенной подписи на хранение во внешнюю СХД (добавляется при передаче во внешнюю СХД автоматически);
- идентификатор документа во внешней СХД (добавляется после передачи во внешнюю СХД);
- дата окончания Хранения;
- дата Уничтожения (заполняется, если необходимо уничтожить документ после даты окончания Хранения);
- дата планового обновления доказательств подлинности (добавляется при внесении в «КриптоПро Архив» версии 1.0» автоматически);
- дата и время последнего изменения данных в контейнере (добавляется при внесении в «КриптоПро Архив» версии 1.0» автоматически).

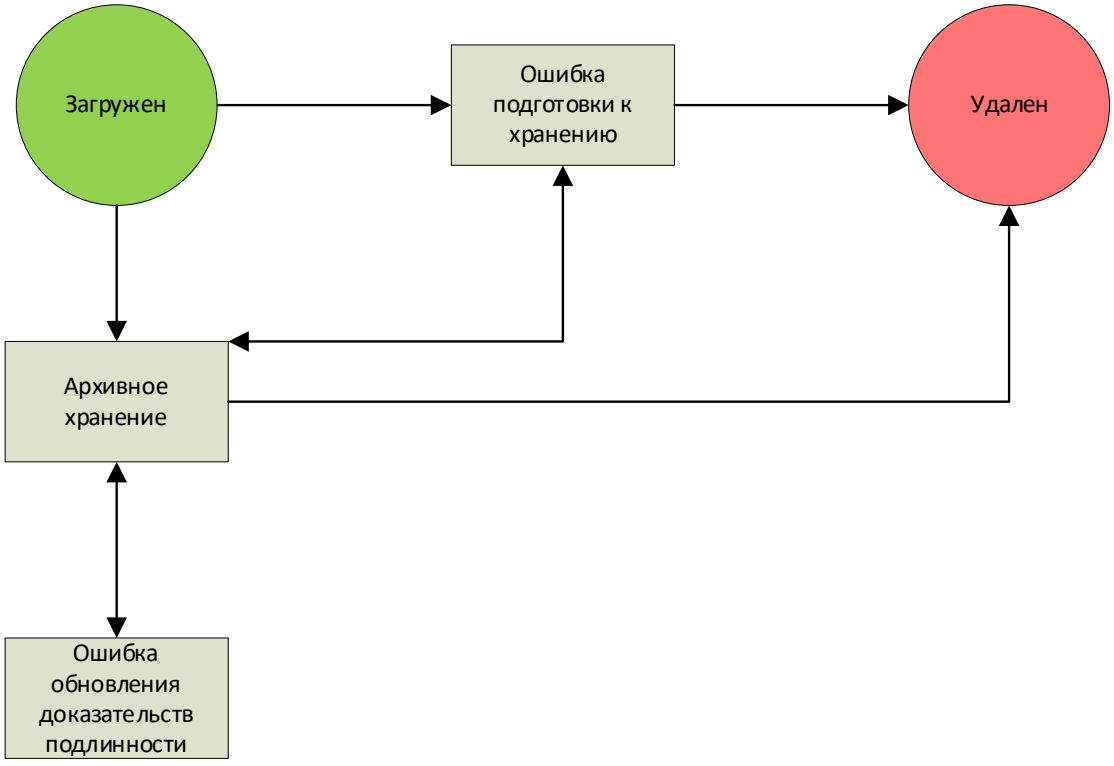

Рисунок 2 Статусная модель контейнера документа в «КриптоПро Архив» версии 1.0»

Программное обеспечение модуля в автоматическом режиме или по запросу модуля администрирования обновляет доказательства подлинности контейнеров документов, используя подсистему “Модуль обеспечения доказательствами действительности электронной подписи”.

Программное обеспечение подсистемы обеспечивает передачу улучшенной подписи документа во внешнюю СХД через создаваемые разработчиком СХД плагины подключения.

Программное обеспечение подсистемы обеспечивает регистрацию и исполнение запросов на выдачу контейнеров документов на основании поступивших запросов от ИС.

Программное обеспечение обеспечивает контроль сроков хранения контейнеров документов, установленных настройками «КриптоПро Архив» версии 1.0». В случае хранения документов в подсистеме “Модуль Архив УЦ” документы с истекшим сроком хранения либо автоматически уничтожаются (если установлена дата Уничтожения), либо сохраняются в «КриптоПро Архив» версии 1.0» с уведомлением Администратора (в случае если срок Хранения установлен, а дата Уничтожения не установлена). Метаданные, содержащиеся в контейнере уничтоженного документа, сохраняются в «КриптоПро Архив» версии 1.0», с внесением в них информации о дате уничтожения документа.

Для внешних ИС в модуле доступны следующие методы REST-сервисов:

1. загрузка контейнера документа (загрузка метаданных, а также подписанного ЭП документа или отдельно документа (ссылки на документ) и его ЭП) в «КриптоПро Архив» версии 1.0», возвращает идентификатор контейнера);
2. поиск контейнеров документов по набору метаданных документов, возвращает набор идентификаторов контейнеров;
3. получение метаданных документа по идентификатору контейнера, возвращает ЭП в формате CAdES-E-A и все метаданные документа;
4. изменение метаданных документа (кроме тех, которые устанавливаются автоматически)
5. удаление документа из «КриптоПро Архив» версии 1.0» по его идентификатору.

3.2.2. Модуль обеспечения доказательствами действительности электронной подписи

Модуль предназначен для обеспечения доказательствами подлинности и юридической значимости документов, подписанных электронной подписью, и позволяет обеспечивать:

- преобразование исходной ЭП документа в формат CAdES-E-A;
- взаимодействие с компонентами ПАК «Службы УЦ» (ПАК «КриптоПро OCSP», ПАК «КриптоПро TSP», Служба проверки сертификатов и электронной подписи «КриптоПро SVS»);
- фиксацию времени и результата преобразования исходной ЭП документа в формат CAdES-E-A, включая результаты ответов компонентов ПАК «Службы УЦ»;
- проверку исходной электронной подписи документов при подготовке к долговременному хранению с использованием Службы проверки сертификатов и электронной подписи «КриптоПро SVS». В случае

получения отрицательного результата проверки сертификатов исходной ЭП документов, поступающих на долговременное хранение, Модуль прекращает обработку документа с уведомлением пользователей «КриптоПро Архив» версии 1.0»;

- автоматическое продление срока хранения документа на основании данных из подсистемы хранения информации о документах долговременного хранения. При приближении срока окончания действия сертификата Службы штампов времени Модуль автоматически получит ещё один штамп времени на указанный документ (с использованием нового закрытого ключа и сертификата Службы штампов времени), добавит новый архивный штамп времени к ЭП документа и установит новую дату и время обновления доказательств подлинности в контейнере документа;
- соответствие всем требованиям законодательства и нормативно-правовым актам в части требований к средствам электронной подписи

Модуль состоит из нескольких компонентов, которые реализуют перечисленные функции.

ПО Модуля обеспечения доказательствами действительности электронной подписи

ПО Модуля предназначено для взаимодействия с программным интерфейсом Модуля управления обработкой документов с электронной подписью и ПАК «Службы УЦ» при проверке и усовершенствовании электронной подписи документа.

КриптоПро TSP Client

Клиент служб штампов времени «КриптоПро TSP Client» предназначен для обращения к серверу «КриптоПро TSP Server» по протоколу TSP поверх HTTP, получения от него штампов времени (меток времени), обработки и работы с запросами на штампы времени и непосредственно со штампами времени. Подробная информация о TSP-клиенте содержится в составе документации на ПАК «КриптоПро УЦ 2.0».

КриптоПро OCSP Client

Клиент служб актуальных статусов сертификатов «КриптоПро OCSP Client» предназначен для обращения к серверу «КриптоПро OCSP Server» по протоколу OCSP поверх HTTP, получения от него OCSP-ответов, обработки и работы с OCSP-запросами и OCSP-ответами. Подробнее о OCSP-клиенте можно прочитать в составе документации на ПАК «КриптоПро УЦ 2.0».

3.2.3. Модуль Администрирования

Модуль предназначен для регистрации и управления правами доступа пользователей и обеспечения возможности настройки и администрирования «КриптоПро Архив» версии 1.0». Модуль администрирования обеспечивает:

- конфигурирование настроек «КриптоПро Архив» версии 1.0»;
- регистрацию пользователей «КриптоПро Архив» версии 1.0»;
- мониторинг взаимодействия «КриптоПро Архив» версии 1.0» и внешних ИС;

- возможность приостановки и возобновления информационного взаимодействия с внешними системами;
- просмотр журналов событий «КриптоПро Архив» версии 1.0»;
- оповещение персонала «КриптоПро Архив» версии 1.0» о возникновении нештатных ситуаций;
- управление обновлением доказательств подлинности и юридической значимости контейнеров документов;
- управление резервным копированием данных, хранящихся в Системе.

Доступ к подсистеме обеспечивается через стандартные web-браузеры клиентских ОС Linux и Windows.

3.2.4. Модуль Архив УЦ

Модуль предназначен для хранения подписанных электронной подписью документов Удостоверяющего центра, а также автоматизированного взаимодействия с подсистемой хранения информации о документах долговременного хранения.

Модуль:

- обладает графическим интерфейсом для Оператора подсистемы;
- осуществляет прием документов подсистемой хранения информации о документах долговременного хранения;
- поддерживает поиск электронных документов;
- поддерживает хранение документов и информации о связанных с ними контейнеров документов;
- поддерживает процесс подготовки к уничтожению документа с истекшим сроком хранения;

Программное обеспечение Модуля обеспечивает процессы приема документа и его контейнера на хранение, регистрацию и обеспечение доказательствами подлинности и юридической значимости, как в автоматическом, получая документы и их контейнеры из подсистемы хранения информации о документах долговременного хранения, так и в ручном режиме, путем ввода регистрационных данных, прикрепления документов и подписания их подписью Оператора подсистемы через графический интерфейс Оператора Модуля.

4. Аутентификация в КриптоПро Архив

При входе в КриптоПро Архив, а также при всех вызовах из внешних информационных систем методов сервисов ПО предусмотрена аутентификация по сертификату. Данный метод требует установки защищенного TLS-соединения с двусторонней аутентификацией. Аутентификация производится с использованием пары ключей, закрытая часть которой хранится у Пользователя, а сертификат открытого ключа должен быть доверенным для КриптоПро Архив.

5. Архитектура решения КриптоПро Архив

На Рисунок 1 изображена схема взаимодействия компонентов КриптоПро Архив. Внутри пунктирной линии отображаются компоненты, непосредственно входящие в состав продукта, а также связи между ними. Сторонние продукты расположены вне границы, обозначенной пунктиром. Их присутствие на схеме необходимо для полного видения связей и зависимостей компонентов КриптоПро Архив от внешних компонентов.

Организация защищенных каналов со стороны КриптоПро Архив осуществляется с помощью СКЗИ «КриптоПро CSP». Со стороны клиента необходимо использовать сертифицированное ФСБ России СКЗИ КриптоПро CSP.

Уровень защиты при использовании КриптоПро Архив с подключением по протоколу TLS с двусторонней аутентификацией определяется уровнем защиты клиентских компонентов, используемых для TLS-соединения с сервером КриптоПро Архив.

6. Системные требования

6.1. Аппаратное обеспечение

Аппаратные требования к техническим средствам, на которых размещаются программные компоненты КриптоПро Архив, зависят от объема обрабатываемых документов в сутки и требований по производительности всего комплекса.

В данном документе приведены рекомендуемые минимальные требования к техническим средствам, которые обеспечивают установку и работу компонентов на одном сервере при нагрузке в 100Гб документов в сутки:

Таблица 1 — Требования к аппаратному обеспечению

Оборудование	Минимальные требования
Центральный процессор	64-разрядный восьми ядерный процессор с тактовой частотой 2,5 ГГц.
Оперативная память	16 ГБ ОЗУ.
Жесткий диск	Не менее 250 ГБ свободного места.
Сетевые адаптеры	Один сетевой адаптер, совместимый с операционной системой компьютера, для взаимодействия с внутренней сетью.

6.2. Программное обеспечение

КриптоПро Архив представляет собой набор веб-сервисов, как уже было сказано ранее. Поэтому ко всем его компонентам предъявляются одинаковые системные требования:

- **Операционные системы:** Astra Linux (1.6, 2.12), CentOS 7 и 8, Debian 9 и 10, openSUSE 15, Red Hat 7 и 8, Ubuntu (16.04, 18.04, 20.04, 20.10), Microsoft Windows Server 2012/2012R2/2016/2019 (x64), а также некоторые другие ОС.

- **СУБД:** PostgreSQL 8.0 и выше, MySQL 5 и выше, Oracle DB 11.2 и выше, Microsoft SQL Server 2012 и последующие, а также некоторые другие СУБД.

7. Система ролей в КриптоПро Архив

Система ролей в КриптоПро Архив позволяет разграничить права доступа лиц, работающих с КриптоПро Архив. Существуют следующие роли:

- Внешняя ИС;
- Оператор "Модуля Архив УЦ";
- Администратор;
- Системный Администратор.

Внешняя ИС — любая ИС, зарегистрированная Администратором для вызова сервисов КриптоПро Архив. Администратор может предоставить индивидуальные разрешения на вызов каждого из доступных REST сервисов.

Управление учетными записями внешних ИС в КриптоПро Архив может осуществляться только через веб-интерфейс Администратором.

Оператор "Модуля Архив УЦ" КриптоПро Архив — любой пользователь, получивший учетные данные для входа от Администратора. Ему доступен основной функционал "Модуля Архив УЦ" и личный кабинет, где он может просмотреть свой профиль.

Управление учетными записями Операторов "Модуля Архив УЦ" в КриптоПро Архив может осуществляться только через веб-интерфейс Администратором.

Администратор КриптоПро Архив — привилегированный пользователь, имеющий право на создание, редактирование и удаление учетных записей ИС и других Пользователей.

Администратор КриптоПро Архив обеспечивает выполнение следующих задач:

- Регистрация ИС и Операторов "Модуля Архив УЦ" в КриптоПро Архив;
- Управление (редактирование, удаление) учетными записями зарегистрированных ИС и Операторов "Модуля Архив УЦ" КриптоПро Архив;
- Настройка аутентификации ИС и Операторов "Модуля Архив УЦ";
- Просмотр и печать событий аудита КриптоПро Архив.
- Администрирование специального программного обеспечения;
- Настройка экземпляров компонентов КриптоПро Архив;
- Управление лицензиями КриптоПро Архив.

Системный Администратор КриптоПро Архив занимается администрированием сервера(-ов) с компонентами КриптоПро Архив. Он обеспечивает выполнение следующих задач:

- Установка общесистемного и специального программного обеспечения компонентов КриптоПро Архив;
- Создание, удаление и обновление экземпляров компонентов КриптоПро Архив;
- Администрирование общесистемного программного обеспечения;
- Архивирование и восстановление настроек общесистемного программного обеспечения;
- Установка и конфигурирование дополнительных программно-аппаратных средств, обеспечивающих контроль целостности программных средств;

- Администрирование программно-аппаратных средств, реализующих меры защиты от НСД на компонентах КриптоПро Архив.

В целях обеспечения безопасности необходимо, чтобы роли Администратора, Системного Администратора, Оператора "Модуля Архив УЦ" принадлежали разным людям из независимых структурных подразделений организации, что позволит исключить возможность сговора и компрометации данных Пользователей КриптоПро Архив.

Рекомендуется также назначать указанные роли материально ответственным лицам и лицам из руководящего состава организации.

8. Поддерживаемые типы ЭП и форматы документов

КриптоПро Архив позволяет формировать усовершенствованную подпись CAdES-A с архивным штампом (ATSv3), формат которой основан на стандарте ETSI TS 101 733 («CMS Advanced Electronic Signature, CAdES»). Формат CAdES-A v3 может быть построен на основании существующих атрибутов из форматов CAdES-BES, CAdES-T, CAdES-XLT1.

Усовершенствованная электронная подпись позволяет:

- Обеспечить доказательное подтверждение момента создания ЭП;
- Обеспечить доказательное подтверждение действительности сертификата открытого ключа на момент создания ЭП;
- Обеспечить отсутствие необходимости сетевых обращений при проверке ЭП;
- Доказательно подтвердить момент создания ЭП позволяет полученный на нее штамп времени.
- Доказательно подтвердить действительность сертификата открытого ключа на момент создания подписи позволяет информация о статусе сертификата, полученная в режиме реального времени.
- Добавляться архивные штампы времени в подпись по мере необходимости, например, в случае компрометации ранее использованных сертификатов или изменении алгоритмов.
- Обеспечивать возможность проверки подписи в течение как можно более долгого периода времени.

Данный формат подписи позволяет сформировать криптографическое сообщение, являющееся полностью самодостаточным для его открытия и выполнения всех необходимых операций. С этой целью в сообщении размещается информация об исходном документе, алгоритмах хэширования и подписи, параметрах алгоритмов, времени подписи, сертификате закрытого ключа, цепочки сертификации.

В качестве ожидаемых входящих форматов электронной подписи, КриптоПро Архив оперирует следующими форматами (а также CAdES-A, описанным выше):

- **CAdES Basic Electronic Signature (CAdES-BES).**

Представляет собой подпись формата Cryptographic Message Syntax (RFC 5652). CAdES-BES требует обязательного наличия в подписанном сообщении подписанного атрибута SigningCertificateV2. Данный атрибут идентифицирует сертификат подписывающего и позволяет дополнить подпись до формата CAdES-X Long Type 1.

Также в подписанное сообщение добавляется подписанный атрибут signingTime – отметка о времени создания подписи (время в атрибуте указывается по часам сервера).

Два следующих типа электронной подписи, доступных в КриптоПро Архив, являются усовершенствованным вариантами CAdES-BES.

- **CAdES-T (Timestamp).**

Представляет собой электронную подпись с доверенным временем Timestamp. Подходит для ситуации, в которой использованные сертификаты, будучи действительными на момент генерации подписи, были отозваны после этого. Поэтому для доказательства того, что данные были подписаны до отзыва сертификатов и что эти данные существовали на определенный момент времени, используются штампы времени, подписанные службой проверки штампов времени до истечения срока действия хотя бы одного сертификата. Это дает ценность подписи при ее проверке.

- **CAdES with Extended Long validation data Type 1 (CAdES-X Long Type 1).**

Данный формат представляет собой усовершенствованную подпись, позволяющую обеспечить участников электронного документооборота всей необходимой доказательной базой (причем собранной в самой ЭП в качестве реквизитов электронного документа), связанной с установлением момента подписи и статуса сертификата открытого ключа на момент подписи.

В зависимости от наличия исходного документа в самом сообщении, выделяют два типа CMS-подписи:

- Присоединенная подпись (attached).

Получатель такого сообщения может проверить полученную подпись даже при отсутствии исходного подписанного документа.

- Отделенная подпись (detached).

Получатель сообщения этого типа для проверки подписи должен иметь исходный документ, для которого была сформирована подпись.

СВЕДЕНИЯ О РАЗРАБОТЧИКЕ

Компания КриптоПро создана в 2000 году и в настоящее время занимает лидирующее положение по распространению средств криптографической защиты информации и электронной цифровой подписи.

Основное направление деятельности компании – разработка средств криптографической защиты информации и развитие Инфраструктуры Открытых Ключей (Public Key Infrastructure) на основе использования международных рекомендаций и российских криптографических алгоритмов.

Компания разработала полный спектр программных и аппаратных продуктов для обеспечения целостности, авторства и конфиденциальности информации с применением ЭП и шифрования для использования в различных средах (Windows, Unix, Java). Новое направление продуктов компании – программно-аппаратные средства криптографической защиты информации и использованием смарт-карт и USB ключей, позволяющих существенно повысить безопасность систем, использующих ЭП.

Компания КриптоПро является разработчиком и поставщиком средств применения ЭП в автоматизированных информационных системах. Кроме этого, компания оказывает консультационные услуги по обеспечению деятельности удостоверяющих центров и применению ЭП в автоматизированных информационных системах предприятий различных форм собственности.

Удостоверяющий центр компании КриптоПро предоставляет организациям (юридическим лицам) услуги по изготовлению и управлению открытыми и закрытыми ключами пользователей информационных систем, включая процедуру подачи и обработки запросов на сертификаты, верификацию запросов на сертификаты, формирования сертификатов, их получения, использования и отзыва. Также Удостоверяющим центром предоставляются иные сервисные функции, связанные с использованием электронных подписей, шифрованием, обеспечением электронного юридически-значимого документооборота.

Контакты:

ООО «КРИПТО-ПРО»

127018, Москва, ул. Сущевский вал, 18

Телефон: (495) 995 4820

Факс: (495) 995 4820

URL: http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru