Утвержден

RU.54819512.00021-01 31 01-ЛУ

Программный комплекс
«ОТР. Универсальный сервер криптографической защиты информации»
(ОТР.УСКЗИ)

RU.54819512.00021-01

ОПИСАНИЕ ПРИМЕНЕНИЯ

Листов: 21

Москва
2020

АННОТАЦИЯ

В данном программном документе приведено описание применения программного комплекса «ОТР. Универсальный сервер криптографической защиты информации» (далее по тексту – ПК «ОТР.УСКЗИ», Изделие).

В документе описано назначение программы, условия ее применения, описание задачи и сведения о входных и выходных данных.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

Сокращения и условные обозначения, встречающиеся в данном документе, приведены в таблице 1.

Таблица 1. Условные обозначения и сокращения

№ п/п	Термины и сокращения	Определения
1.	CSP	Cryptography Service Provider. Криптопровайдер.
2.	IP	Internet Protocol. Протокол сетевого уровня, являющийся базовым протоколом IP-сетей.
3.	SOAP-запрос	Запрос в формате SOAP для обмена с веб-сервисами, например, СМЭВ
4.	АРМ	Автоматизированное рабочее место.
5.	Метка времени	Подписанный электронной подписью документ, которым Служба штампов времени (Time-Stamping Authority – TSA) удостоверяет, что в указанный момент времени ей было предоставлено значение хэш-функции от другого документа. Само значение хэш-функции также указывается в метке (штампе).
6.	ОЗУ	Оперативное запоминающее устройство
7.	ОС	Операционная система.
8.	ПК	Программный комплекс
9.	ПО	Программное обеспечение
10.	ПС	Прикладная система
11.	СКЗИ	Средство криптографической защиты информации
12.	СКП (сертификат)	Квалифицированный сертификат ключа проверки электронной подписи
13.	СОС	Список отозванных сертификатов.
14.	СУБД	Система управления базами данных
15.	ЦП	Центральный процессор
16.	ЭП	Квалифицированная электронная подпись
17.	ЭП-CMS	Квалифицированная электронная подпись в формате, соответствующем спецификации CMS Advanced Electronic Signature (CAdES)
18.	ЭП-XMLdSig	Квалифицированная электронная подпись в формате, соответствующем спецификации XML Signature Syntax and Processing (Second Edition)
19.	ЭП-ОВ	Электронная подпись Органа власти
20.	ЭП-СМЭВ	Электронная подпись Системы межведомственного электронного взаимодействия
21.	ЭП-СП	Электронная подпись служебного пользователя

1. ОБЩИЕ СВЕДЕНИЯ

Полное наименование Изделия: программного комплекса «ОТР. Универсальный сервер криптографической защиты информации».

Сокращенное наименование Изделия: ПК «ОТР.УСКЗИ».

Обозначение Изделия: RU.54819512.00021-01.

Предприятие-разработчик и изготовитель: ООО «ОТР 2000» (127474, Москва, Дмитровское шоссе, д. 60А, ИНН 7718162032).

2. НАЗНАЧЕНИЕ ПРОГРАММЫ

2.1. Назначение и область применения

ПК «ОТР.УСКЗИ» – программный комплекс, предоставляющий сервисы формирования и проверки ЭП, а так же доведения ЭП до усовершенствованных форматов.

Изделие поддерживает несколько режимов взаимодействия с прикладными системами:

- Асинхронное через брокер сообщений Kafka.
- Синхронное взаимодействие по протоколу gRPC.
- Синхронное взаимодействие посредством встраивания компонента angular для обеспечения формирования электронной подписи на АРМ пользователя.

Изделие представляет собой набор сервисов, которые запускаются в виде самостоятельных приложений. Перечень сервисов:

- клиентский модуль ЭП;
- сервис выдачи штампов времени;
- сервис формирования электронных подписей;
- сервис проверки электронных подписей;
- сервис расчета хэш-функции;
- сервис проверки сертификатов и СОС;
- адаптер kafka сервиса формирования электронных подписей;
- адаптер kafka сервиса проверки электронных подписей.

2.2. Функциональные возможности

ПК «ОТР.УСКЗИ» реализует следующие функции:

- Вычисления значения хэш-функции от данных;
- Проверка СКП (построение цепочки, проверка цепочки, валидность, целостность, неотозванность);
- Проверка СОС (определение издателя, проверка целостности СОС на ключе издателя);
- Формирование ЭП бинарных форматов: CMS. CAdES-BES. CAdES-T. CAdES-C;
- Доведение ЭП формата CAdES-BES до форматов: CAdES-T, CAdES-C, CAdES-A;
- Проверка ЭП бинарных форматов: CMS. CAdES-BES. CAdES-T. CAdES-C, CAdES-A;
- Формирование ЭП xml форматов: XmlDSig, XAdES-BES;
- Доведение ЭП формата XAdES-BES до форматов XAdES-T, XAdES-C, XAdES-A;
- Проверка ЭП xml форматов: XmlDSig, XAdES-BES, XAdES-T, XAdES-C, XAdES-A;
- Формирование ЭП в формате WS-Security X509 Certificate Token Profile;
- Проверка ЭП в формате WS-Security X509 Certificate Token Profile;
- Формирование штампа доверенного времени в соответствии со спецификацией RFC 3161.

3. УСЛОВИЯ ПРИМЕНЕНИЯ

3.1. Минимальные системные требования

Минимальные требования к аппаратному обеспечению указаны в таблице 3.

Таблица 2. Минимальные требования к аппаратному обеспечению

Параметр	Значение
ЦП	8 ядра
ОЗУ	32 GB
Жесткий диск	150 GB

Требования к системному ПО указаны в таблице 4.

Таблица 3. Требование к программному обеспечению

Параметр	Значение
Операционная система	RHEL, релиз 7 CentOS, релиз 7
СУБД	PostgreSQL 12 и выше
JRE (Java SE Runtime Environment)	11 и выше
CSP (cryptography service provider)	СКЗИ «КриптоПро CSP» версия 4.0 исполнения 1-Base и 2-Base (для ОС 64 bit)

Для всех серверов, участвующие в обмене данными с Изделие (в том числе и для машины с установленным Изделие) должна быть настроена маршрутизация, а также открыт порты, указанные в конфигурационных файлах Изделия.

3.2. Стандарты и совместимость с другими продуктами

3.2.1. Поддерживаемые алгоритмы преобразования при формировании/проверке xml подписей

Алгоритмы каноникализации:

- http://www.w3.org/TR/2001/REC-xml-c14n-20010315
- http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
- http://www.w3.org/2001/10/xml-exc-c14n#
- http://www.w3.org/2001/10/xml-exc-c14n#WithComments
- http://www.w3.org/2006/12/xml-c14n11
- http://www.w3.org/2006/12/xml-c14n11#WithComments
- http://santuario.apache.org/c14n/physical

Алгоритмы трансформации:

- http://www.w3.org/2000/09/xmldsig#base64
- http://www.w3.org/TR/2001/REC-xml-c14n-20010315
- http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
- http://www.w3.org/2006/12/xml-c14n11
- http://www.w3.org/2006/12/xml-c14n11#WithComments
- http://www.w3.org/2001/10/xml-exc-c14n#
- http://www.w3.org/2001/10/xml-exc-c14n#WithComments
- http://www.w3.org/TR/1999/REC-xpath-19991116

- http://www.w3.org/2000/09/xmldsig#enveloped-signature
- http://www.w3.org/TR/1999/REC-xslt-19991116
- http://www.w3.org/2002/06/xmldsig-filter2
- urn://smev-gov-ru/xmldsig/transform

3.2.2. Поддерживаемые криптографические алгоритмы

Реализуемые Изделием с помощью обращения к функциям СКЗИ алгоритмы формирования электронной подписи:

- ГОСТ Р 34.10-2012;

Реализуемые Изделием с помощью обращения к функциям СКЗИ алгоритмы проверки электронной подписи:

- ГОСТ Р 34.10-2012,
- ГОСТ Р 34.10-2001;

Реализуемые Изделием с помощью обращения к функциям СКЗИ алгоритмы вычисления хэш-функции:

- ГОСТ Р 34.11-2012,
- ГОСТ Р 34.11-94[1].

3.3. Порядок работы

Порядок установки и настройки сервисов Изделия описан в Руководстве администратора RU.54819512.00021-01 34 01.

3.4. Ограничения, накладываемые на область применения Изделия

При использовании Изделия в прикладных системах необходимо по Техническому заданию, согласованному с 8 Центром ФСБ России, проводить оценку влияния прикладного программного обеспечения, использующего функции Изделия, на выполнение предъявленных к СКЗИ требований в случаях:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации защиты конфиденциальной информации, обрабатываемой СКЗИ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;
- при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты;
- при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

[1] Только в рамках выполнения функции проверки электронной подписи

4. ОПИСАНИЕ ЗАДАЧ

4.1. Определение задач

Изделие решает задачи, соответствующие функциям, приведенным в п. 2.2.

4.2. Описание решения задач

4.2.1. Описание процесса вычисление значения хэш-функции от данных

Процесс вычисления хэш-функции на данные:

1. Клиентский модуль ЭП вызывает Сервис расчета хэш-функции на данные передавая во входных параметрах:
   - Данные по которым необходимо рассчитать хэш-функцию;
   - Алгоритм расчета хэш-функции.
2. Сервис расчета хэш-функции вызывает средство ЭП:
   - Данные по которым необходимо рассчитать хэш-функцию;
   - Идентификатор алгоритма расчета хэш-функции.
3. Сервис расчета хэш-функции возвращает ответ.

4.2.2. Описание процесса проверки СКП

Процесс проверки СКП:

1. Сервисы ПК «ОТР.УСКЗИ» вызывают Сервис проверки сертификатов и СОС (далее Сервис) передавая во входных параметрах:
   - Сертификат;
   - Дата и время, на которые необходимо выполнить проверку;
   - Опционально. Цепочка ссылок на сертификаты. Используется при проверке подписей форматов CAdES-C и XAdES-C;
   - Опционально. Цепочка ссылок на списки отозванных сертификатов. Используется при проверке подписей форматов CAdES-C и XAdES-C;
   - Тип ответа:
     - SIMPLE – необходимо только результат проверки;
     - WITH_REFS – Необходима информация о сертификатах цепочки сертификатов и информация о списках отозванных сертификатов, по которым проверялся сертификат подписанта.
2. Сервис выполняет построение цепочки сертификатов:
   - Если в параметрах вызова не указаны ссылки на сертификаты цепочки:
     - Рекурсивная загрузка сертификатов цепочки по идентификатору ключа издателя из БД ПК «ОТР.УСКЗИ».
   - Если в параметрах вызова указаны ссылки на сертификаты цепочки:
     - Загрузка сертификатов цепочки на основе информации из ссылок из БД.

   Если цепочку сертификатов построить не удалось, то Сервис возвращает результата проверки:
   - Сертификат не валиден;
   - Причина не валидности сертификата.
3. Сервис выполняет проверку цепочки сертификатов:
   - Проверка валидности сертификата на дату проверки;
   - Проверка целостности сертификата путем проверки ЭП сертификата;

- Проверка на неотозванность:
  - Загрузка актуальной на дату проверки мета-информации о СОС и тела СОС из БД ПК «ОТР.УСКЗИ»:
    - Если в параметрах вызова не указаны ссылки на СОС: Загрузка СОС по идентификатору ключа издателя.
    - Если в параметрах вызова указаны ссылки на СОС: Загрузка СОС на основе информации из ссылки.
  - Проверка целостности загруженного СОС путем проверки ЭП на СОС;
  - Проверка соответствие найденного СОС:
    - Проверяемому сертификату по идентификатору ключа издателя;
    - Загруженной мета-информации.
  - Проверка на неотозванность по СОС.

Если хотя бы один сертификат из цепочки не прошел хотя бы одну проверку, то Сервис возвращает результат проверки:

- Сертификат не валиден;
- Причина не валидности сертификата.

4. Сервис выполняет формирование ответа:
   - Если в параметрах вызова указан тип ответа SIMPLE:
     - Добавление в ответ признак валидности/не валидности сертификата.
   - Если в параметрах вызова указан тип ответа WITH_REFS:
     - Добавление в ответ признак валидности/не валидности сертификата;
     - Добавление в ответ ссылок на сертификаты цепочки сертификатов;
     - Добавление в ответ ссылок на СОС по которым выполнялась проверка на неотозванность цепочки сертификатов.
5. Сервис возвращает ответ.

4.2.3. Описание процесса проверки СОС

Процесс проверки СОС:

1. Сервисы ПК «ОТР.УСКЗИ» вызывают Сервис проверки сертификатов и СОС (далее Сервис) передавая во входных параметрах:
   - Список отозванных сертификатов;
   - Тип ответа:
     - SIMPLE – необходимо только результат проверки;
     - FULL – Результат проверки и информация о СОС
2. Сервис выполняет поиск сертификата издателя СОС по идентификатору ключа издателя.

   Если сертификат не найден, формируется исключение.
3. Проверка целостности СОС путем проверки ЭП;
4. Сервис выполняет формирование ответа:
   - Если в параметрах вызова указан тип ответа SIMPLE:
     - Добавление в ответ признак валидности/не валидности СОС.
   - Если в параметрах вызова указан тип ответа FULL:
     - Добавление в ответ признак валидности/не валидности СОС;
     - Информация о СОС.
5. Сервис возвращает ответ.

4.2.4. Описание процесса формирования ЭП бинарных форматов: CMS. CAdES-BES. CAdES-T. CAdES-C

Процесс создания серверной (автоматической) ЭП форматов CMS. CAdES-BES. CAdES-T. CAdES-C.

1. ПС формирует и отправляет запрос на формирование ЭП бинарного формата в очередь сообщений kafka. Сообщение содержит следую информацию:
    - Подписываемые данные;
    - Идентификатор СКП зарегистрированного в ПК «ОТР.УСКЗИ»;
    - Требуемый формат ЭП, поддерживаемые форматы: CMS. CAdES-BES. CAdES-T. CAdES-C;
    - Тип ответа, поддерживаемые варианты: SIMPLE, FULL.
2. Адаптер формирования ЭП (далее Адаптер) получает из очереди сообщений kafka запрос на создание ЭП, выполняет его обработку:
    - Проверка сообщения на соответствие формату;
    - Переупаковка сообщение в protobuf объект.

    Если запрос не прошел проверку, то Адаптер формирует сообщение с описанием ошибки и отправляет его в ответную очередь kafka;
3. Адаптер вызывает Сервис формирования ЭП (далее Сервис);
4. Сервис в локальном хранилище производит поиск СКП, соответствующего полученному в запросе идентификатору;

    Если СКП в системном хранилище не найден, Сервис возвращает инициатору взаимодействия ответ, содержащий код и описание ошибки.
5. Осуществляет проверку найденного СКП посредством вызова Сервиса проверки сертификатов и СОС. Процесс проверки СКП описан в п. 4.2.2.;

    Если указан формат CAdES-C, то в запросе к службе проверки сертификатов и СОС указывается тип ответа – WITH_REFS.

    Если найденный СКП не прошел проверку, Сервис возвращает инициатору взаимодействия ответ, содержащий код и описание ошибки.
6. Сервис выполняет подготовку контейнера ЭП формата CMS или CAdES-BES без математической подписи. Для расчета хэш-функции Сервис вызывает Средство ЭП, передавая на вход:
    - Данные для расчета хэш-функции;
    - Идентификатор алгоритма хэширования;
7. Сервис формирует и передает в Средство ЭП запрос на создание математической ЭП, содержащий:
    - Данные, которые требуется подписать;
    - СКП.
8. Средство ЭП создает и возвращает математическую ЭП.
9. Сервис осуществляет добавление ЭП в соответствующее поле ЭП.
10. Если в параметрах вызова указан формат ЭП CAdES-T или CAdES-C, то Сервис выполняет усиление ЭП до указанного формата;

    Процесс усиления ЭП описан в п. 4.2.6.
11. Сервис возвращает результат формирования ЭП:
    - Отсоединенная подпись;

- Если тип ответа указан FULL. Информация о сформированной подписи: информация о сертификате подписанта, времени создания ЭП, формат созданной ЭП;
- Информация об ошибке, если возникла при формировании ЭП.

12. Сервис возвращает Адаптеру результат формирования ЭП указанного формата.
13. Адаптер выполняет переупаковку protobuf результата подписания в формат ответного сообщения и отправляет его в ответную очередь kafka.

4.2.5. Описание процесса проверки ЭП бинарных форматов: CMS. CAdES-BES. CAdES-T. CAdES-C

Процесс проверки ЭП форматов CMS. CAdES-BES. CAdES-T. CAdES-C.

1. ПС формирует и отправляет запрос на формирование ЭП бинарного формата в очередь сообщений kafka. Сообщение содержит следую информацию:
   - Проверяемые данные;
   - Список объектов содержащий информацию о подписях:
     - Формат подписи на соответствие которому необходимо проверить подпись. Поддерживаемые форматы: CMS. CAdES-BES, CAdES-T. CAdES-C;
     - Отсоединенная подпись;
     - Опционально. Формат подписи, до которого необходимо усилить подпись. Поддерживаемые форматы: CAdES-T. CAdES-C;
     - Идентификатор подписи.
   - Тип ответа, поддерживаемые варианты: SIMPLE, FULL.
2. Адаптер формирования ЭП (далее Адаптер) получает из очереди сообщений kafka запрос на создание ЭП, выполняет его обработку:
   - Проверка сообщения на соответствие формату;
   - Переупаковка сообщение в protobuf объект.
3. Адаптер вызывает Сервис формирования ЭП (далее Сервис);
4. Сервис выполняет проверку каждой из переданной ЭП по следующему алгоритму:
   - Проверка на соответствие указанному формату ЭП;
     Если ЭП не соответствует требуемому формату, то она помечается как не валидная с указанием причины.
   - Определение даты и времени, на которую необходимо выполнять проверку ЭП;
     - Текущая дата, для ЭП форматов CMS. CAdES-BES;
     - Дата и время создания штампа доверенного времени для форматов CAdES-T. CAdES-C;
   - Извлечение СКП из контейнера ЭП для проверки;
     Если СКП извлечь не удалось, то ЭП помещается как не валидная с указанием причины.
   - Проверка соответствие хэш-функции от проверяемых данных, хэш-функции из подписываемых атрибутов контейнера ЭП.
   - Проверка математической (чистой подписи), посредством вызова Средства ЭП;
     Если математическая подпись не прошла проверку, то ЭП помещается как не валидная с указанием причины.
   - Проверка СКП посредством вызова Сервиса проверки сертификатов и СОС.
     Параметры вызова Сервиса проверки сертификатов и СОС:
     - Для форматов CMS. CAdES-BES: Дата и время проверки – текущие дата и время, СКП;

Если после успешной проверки требуется доведение ЭП до формата CAdES-C, то в запросе к службе проверки сертификатов и СОС указывается тип ответа – WITH_REFS.

Процесс проверки СКП описан в п. 4.1.2.;

- Если СКП не валидный, то ЭП помещается как не валидная с указанием причины.

Если указан формат CAdES-T:

- Проверка валидности штампа доверенного времени:
  - Получение сертификата службы выдачи штампов времени;
  - Проверка сертификата модуля выдачи штампов врмени;
  - Проверка наличия полномочия 1.3.6.1.5.5.7.3.8 в сертификате модуля;
  - Проверка целостности ЭП штампа времени;
  - Проверка соответствия хэш-функции от математический подписи (получается из контейнера проверяемой ЭП), хэш-функции из штампа времени.
- Проверка СКП выполняется на дату и время создания штампа времени.

Если указан формат CAdES-C:

- При проверке СКП, в параметрах вызова Сервиса проверки сертификатов и СОС, передаются ссылки на цепочку сертификатов и СОС, полученные из контейнера подписи.

Если проверка ЭП успешна и в параметрах вызова указан формат до которого необходимо усилить ЭП (CAdES-T, CAdES-C), то Сервис выполняет усиление ЭП до указанного формата;

Процесс усиления ЭП описан в п. 4.2.6.

5. Сервис формирует ответ с результатами проверки;
6. Сервис возвращает ответ с результатами проверки Адаптеру;
7. Адаптер выполняет переупаковку protobuf результата проверки ЭП в формат ответного сообщения и отправляет его в ответную очередь kafka.

4.2.6. Процесс доведения ЭП формата CAdES-BES до форматов: CAdES-T, CAdES-C

Процесс доведения ЭП формата CAdES-BES до форматов CAdES-T. CAdES-C. Процесс доведения является частью процесса формирования ЭП и проверки ЭП, и не может быть выполнен независимо от них.

1. Сервис проверки ЭП/Сервиса формирования ЭП (далее Сервис) получает данные которые должен заверить штамп времени;
2. Сервис формирует и отправляет запрос на формирование штампа времени модулю выдачи штампов доверенного времени (далее Модуль);
3. Модуль получает запрос, выполняет его разбор и формирует штамп времени, для расчета хэш-функции и выработки математической подписи, Модуль вызывает Средство ЭП;
4. Модуль формирует ответ содержащий штамп времени и отправляет его Сервису;
5. Сервис получает ответ, извлекает из него штамп времени и выполняет его проверку:
   - Получение сертификата службы выдачи штампов времени;
   - Проверка сертификата модуля выдачи штампов времени посредством вызова Сервиса проверки сертификатов и СОС;

Процесс проверки СКП описан в п. 4.2.2.
- Проверка наличия полномочия 1.3.6.1.5.5.7.3.8 в сертификате модуля;
- Проверка целостности ЭП штампа времени;
- Проверка соответствия хэш-функции от математический подписи (получается из контейнера проверяемой ЭП), хэш-функции из штампа времени.

6. Сервис встраивает штамп времени в не подписываемые атрибуты контейнера ЭП (OID 1.2.840.113549.1.9.16.2.14);
7. Сервис формирует ссылки на цепочку сертификатов и СОС по которым выполнялась проверка сертификата подписанта в рамках формирования/проверки ЭП в не подписываемые атрибуты (OID 1.2.840.113549.1.9.16.2.21 и OID 1.2.840.113549.1.9.16.2.22 соответственно);
8. Возврат управления процессу формирования/проверки ЭП.

4.2.7. Описание процесса формирования ЭП Xml форматов: XmlDSig, XAdES-BES, XAdES-T, XAdES-C

Процесс создания серверной (автоматической) ЭП форматов XmlDSig, XAdES-BES, XAdES-T, XAdES-C.

1. ПС формирует и отправляет запрос на формирование ЭП xml формата в очередь сообщений kafka. Сообщение содержит следую информацию:
   - Подписываемые данные;
   - Идентификатор СКП зарегистрированного в ПК «ОТР.УСКЗИ»;
   - Требуемый формат ЭП, поддерживаемые форматы: XmlDSig. XAdES-BES. XAdES-T. XAdES-C;
   - Список указаний о подписываемых блоках данных xml документа:
     - Значение атрибута «Id» элемента xml документа, который необходимо подписать
     - Список трансформаций, которые необходимо применить к элементу xml документа перед вычислением хэш-функции;
   - Тип ответа, поддерживаемые варианты: SIMPLE, FULL.
2. Адаптер формирования ЭП (далее Адаптер) получает из очереди сообщений kafka запрос на создание ЭП, выполняет его обработку:
   - Проверка сообщения на соответствие формату;
   - Переупаковка сообщение в protobuf объект.

   Если запрос не прошел проверку, то Адаптер формирует сообщение с описанием ошибки и отправляет его в ответную очередь kafka;
3. Адаптер вызывает Сервис формирования ЭП (далее Сервис);
4. Сервис в локальном хранилище производит поиск СКП, соответствующего полученному в запросе идентификатору;

   Если СКП в системном хранилище не найден, Сервис возвращает инициатору взаимодействия ответ, содержащий код и описание ошибки.
5. Осуществляет проверку найденного СКП посредством вызова Сервиса проверки сертификатов и СОС. Процесс проверки СКП описан в п. 4.2.2.;

   Если найденный СКП не прошел проверку, Сервис возвращает инициатору взаимодействия ответ, содержащий код и описание ошибки.
6. Сервис осуществляет трансформацию XML, формирует подписываемые данные (SignedInfo), включающие набор ссылок (reference) на данные. Для формирования

каждой ссылки Сервис обращается к Средству ЭП, передавая набор данных, по которым необходимо рассчитать хэш-функцию.
Набор ссылок определяется форматом ЭП и списком указаний на подписываемые данные, переданными во входящих параметрах.

7. Сервис формирует и передает в Средство ЭП запрос на создание математической ЭП, содержащий:
    - Данные, которые требуется подписать;
    - СКП.
8. Средство ЭП создает и возвращает математическую ЭП.
9. Сервис осуществляет добавление ЭП в соответствующее поле ЭП.
10. Если проверка ЭП успешна и в параметрах вызова указан формат ЭП XAdES-T или XAdES-C, то Сервис выполняет усиление ЭП до указанного формата;

    Процесс усиления ЭП описан в п. 4.2.9.
11. Сервис возвращает результат формирования ЭП:
    - Отсоединенная подпись;
    - Если тип ответа указан FULL. Информация о сформированной подписи: информация о сертификате подписанта, времени создания ЭП, формат созданной ЭП;
    - Информация об ошибке, если возникла при формировании ЭП.
12. Сервис возвращает Адаптеру результат формирования ЭП указанного формата.
13. Адаптер выполняет переупаковку protobuf результата подписания в формат ответного сообщения и отправляет его в ответную очередь kafka.

4.2.8. Описание процесса проверки ЭП форматов XmlDSig, XAdES-BES, XAdES-T, XAdES-C

Процесс проверки ЭП форматов XmlDSig, XAdES-BES, XAdES-T, XAdES-C.

1. ПС формирует и отправляет запрос на формирование ЭП бинарного формата в очередь сообщений kafka. Сообщение содержит следую информацию:
    - Xml документ содержащий подписи;
    - Формат подписи на соответствие которому необходимо проверить подпись, перед усилением. Поддерживаемые форматы: XmlDSig, XAdES-BES. XAdES-T, XAdES-C;
    - Опционально. Формат подписи, до которого необходимо усилить подпись. Поддерживаемые форматы: XAdES-T. XAdES-C;
    - Тип ответа, поддерживаемые варианты: SIMPLE, FULL.
2. Адаптер формирования ЭП (далее Адаптер) получает из очереди сообщений kafka запрос на создание ЭП, выполняет его обработку:
    - Проверка сообщения на соответствие формату;
    - Переупаковка сообщение в protobuf объект.
3. Адаптер вызывает Сервис формирования ЭП (далее Сервис);
4. Сервис выполняет проверку каждой из переданной ЭП по следующему алгоритму:
    - Проверка на соответствие указанному формату ЭП;
      Если ЭП не соответствует требуемому формату, то она помечается как не валидная с указанием причины.
    - Определение даты и времени, на которую необходимо выполнять проверку ЭП;
        - Текущая дата, для ЭП форматов XmlDSig. XAdES-BES;
        - Дата и время создания штампа доверенного времени для форматов XAdES-T, XAdES-C;
    - Извлечение СКП из контейнера ЭП для проверки;

Если СКП извлечь не удалось, то ЭП помещается как не валидная с указанием причины.

- Проверка математической (чистой подписи), посредством вызова Средства ЭП;

  Если математическая подпись не прошла проверку, то ЭП помещается как не валидная с указанием причины.
- Проверка валидности ссылок (reference), для расчета хэш-функции выполняется обращение к Средству ЭП;

  Если хотя бы одна ссылка не валидна, то ЭП помещается как не валидная с указанием причины.
- Проверка СКП посредством вызова Сервиса проверки сертификатов и СОС. Параметры вызова Сервиса проверки сертификатов и СОС:
  - Для форматов XmlDSig. XAdES-BES: Дата и время проверки – текущие дата и время, СКП;

  Процесс проверки СКП описан в п. 4.2.2.;
- Если СКП не валидный, то ЭП помещается как не валидная с указанием причины.

Если указан формат XAdES-T:

- Проверка валидности штампа доверенного времени:
  - Получение сертификата службы выдачи штампов времени;
  - Проверка сертификата службы выдачи штампов врмени;
  - Проверка наличия полномочия 1.3.6.1.5.5.7.3.8 в сертификате службы;
  - Проверка целостности ЭП штампа времени;
  - Проверка соответствия хэш-функции от математический подписи (получается из контейнера проверяемой ЭП), хэш-функции из штампа времени.
- Проверка СКП выполняется на дату и время создания штампа времени.

Если указан формат XAdES-C:

- При проверке СКП, в параметрах вызова Сервиса проверки сертификатов и СОС, передаются ссылки на цепочку сертификатов и СОС, полученные из контейнера подписи.

5. Если в параметрах вызова указан формат до которого необходимо усилить ЭП (XAdES-T, XAdES-C), то Сервис выполняет усиление ЭП до указанного формата;

   Процесс усиления ЭП описан в п. 4.2.9.
6. Сервис формирует ответ с результатами проверки;
7. Сервис возвращает ответ с результатами проверки Адаптеру;
8. Адаптер выполняет переупаковку protobuf результата проверки ЭП в формат ответного сообщения и отправляет его в ответную очередь kafka.

4.2.9. Процесс доведения ЭП формата XAdES-BES до форматов: XAdES-T, XAdES-C

Процесс доведения ЭП формата XAdES-BES до форматов XAdES-T. XAdES-C. Процесс доведения является частью процесса формирования ЭП и проверки ЭП, и не может быть выполнен независимо от них.

1. Сервис проверки ЭП/Сервиса формирования ЭП (далее Сервис) получает данные которые должен заверить штамп времени;
2. Сервис формирует и отправляет запрос на формирование штампа времени модулю выдачи штампов доверенного времени (далее Модуль);
3. Модуль получает запрос, выполняет его разбор и формирует штамп времени, для расчета хэш-функции и выработки математической подписи, Модуль вызывает Средство ЭП;
4. Модуль формирует ответ содержащий штамп времени и отправляет его Сервису;
5. Сервис получает ответ, извлекает из него штамп времени и выполняет его проверку:
   - Получение сертификата службы выдачи штампов времени;
   - Проверка сертификата модуля выдачи штампов времени посредством вызова Сервиса проверки сертификатов и СОС;

     Процесс проверки СКП описан в п. 4.2.2.
   - Проверка наличия полномочия 1.3.6.1.5.5.7.3.8 в сертификате модуля;
   - Проверка целостности ЭП штампа времени;
   - Проверка соответствия хэш-функции от математический подписи (получается из контейнера проверяемой ЭП), хэш-функции из штампа времени.
6. Сервис получает ответ, извлекает из него штамп времени и выполняет его проверку:
7. Сервис встраивает штамп времени в не подписываемые атрибуты контейнера ЭП (SignatureTimeStamp);
8. Сервис формирует ссылки на цепочку сертификатов и СОС по которым выполнялась проверка сертификата подписанта в рамках формирования/проверки ЭП в не подписываемые атрибуты (CompleteCertificateRefs и CompleteRevocationRefs соответственно);
9. Возврат управления процессу формирования/проверки ЭП.

4.2.10. Описание процесса формирования ЭП в формате WS-Security X509 Certificate Token Profile

1. ПС формирует и отправляет запрос на формирование ЭП формата WS-Security X509 Certificate Token Profile в очередь сообщений kafka. Сообщение содержит следую информацию:
   - Soap конверт;
   - Идентификатор СКП зарегистрированного в ПК «ОТР.УСКЗИ»;
   - Actor, который необходимо указать в ЭП;
   - Список указаний о подписываемых блоках данных xml документа:
     - Значение атрибута «Id» элемента xml документа, который необходимо подписать;
     - Список трансформаций, которые необходимо применить к элементу xml документа перед вычислением хэш-функции;
   - Тип ответа, поддерживаемые варианты: SIMPLE, FULL.
2. Адаптер формирования ЭП (далее Адаптер) получает из очереди сообщений kafka запрос на создание ЭП, выполняет его обработку:
   - Проверка сообщения на соответствие формату;

- Переупаковка сообщение в protobuf объект.

3. Адаптер вызывает Сервис формирования ЭП (далее Сервис);
4. Сервис в локальном хранилище производит поиск СКП, соответствующего полученному в запросе идентификатору;
5. Осуществляет проверку найденного СКП посредством вызова Сервиса проверки сертификатов и СОС. Процесс проверки СКП описан в п. 4.2.2.;

   Если найденный СКП не прошел проверку, Сервис возвращает инициатору взаимодействия ответ, содержащий код и описание ошибки.
6. Сервис осуществляет трансформацию XML, формирует подписываемые данные (SignedInfo), включающие набор ссылок (reference) на данные. Для формирования каждой ссылки Сервис обращается к средству ЭП, передавая набор данных, по которым необходимо рассчитать хэш-функцию.
7. Сервис формирует и передает в средство ЭП запрос на создание ЭП, содержащий:

   - данные, которые требуется подписать;
   - СКП.

8. Средство ЭП создает и возвращает математическую ЭП.
9. Сервис осуществляет добавление ЭП в соответствующее поле ЭП.
10. Сервис возвращает Адаптеру SOAP-конверт, содержащий ЭП формата WS-Security X509 Certificate Token Profile.
11. Адаптер выполняет переупаковку protobuf результата подписания в формат ответного сообщения и отправляет его в ответную очередь kafka.

4.2.11. Описание процесса проверки ЭП в формате WS-Security X509 Certificate Token Profile

Процесс проверки ЭП формата WS-Security X509 Certificate Token Profile:

1. ПС формирует и отправляет запрос на проверку ЭП формата WS-Security X509 Certificate Token Profile в очередь сообщений kafka. Сообщение содержит следую информацию:
   - SOAP-конверт содержащий ЭП в формате WS-Security X509 Certificate Token Profile;
   - Actor ЭП, которую необходимо проверить;
   - Тип ответа, поддерживаемые варианты: SIMPLE, FULL.
2. Адаптер проверки ЭП (далее Адаптер) получает из очереди сообщений kafka запрос на проверку ЭП, выполняет его обработку:
   - Проверка сообщения на соответствие формату;
   - Переупаковка сообщение в protobuf объект.
3. Адаптер вызывает Сервис проверки ЭП (далее Сервис);
4. Сервис выполняет поиск ЭП которую(ые) необходимо проверить:
   - Если в параметрах вызова указан actor, то выполняется поиск ЭП с указанным actor;
   - Если в параметрах вызова actor не указан, то выполняется поиск всех ЭП формата WS-Security X509 Certificate Token Profile в SOAP-конверте.

   Если SOAP-конверт не содержит ни одной ЭП формата WS-Security X509 Certificate Token Profile или по указанному actor ЭП не найдена, Сервис возвращает ответ с ошибкой.
5. Сервис выполняет проверку ЭП по следующему алгоритму:
   - Проверка на соответствие требуемому формату ЭП;

Если ЭП не соответствует требуемому формату, то она помещается как не валидная с указанием причины.

- Извлечение СКП для проверки ЭП из XML;
  Если СКП извлечь не удалось, то ЭП помещается как не валидная с указанием причины.
- Проверка математической (чистой подписи), посредством вызова Средства ЭП;
  Если математическая подпись не прошла проверку, то ЭП помещается как не валидная с указанием причины.
- Проверка валидности ссылок (reference), для расчета хэш-функции выполняется обращение к Средству ЭП;
  Если хотя бы одна ссылка не валидна, то ЭП помещается как не валидная с указанием причины.
- Проверка СКП посредством вызова Сервиса проверки сертификатов и СОС. Процесс проверки СКП описан в п. 4.2.2.
- Если СКП не валидный, то ЭП помещается как не валидная с указанием причины.

6. Сервис формирует ответ с результатами проверки;
7. Сервис возвращает ответ с результатами проверки Адаптеру;
8. Адаптер выполняет переупаковку protobuf результата проверки ЭП в формат ответного сообщения и отправляет его в ответную очередь kafka.

4.2.12. Описание процесса формирования штампа доверенного времени

Процесс формирования штампа доверенного времени.

1. Модуль выдачи штампов времени (далее Модуль) получает запрос на выдачу штампа времени;
2. Модуль выполняет разбор и проверку запроса на выдачу штампа времени;
3. Модуль формирует структуру TSTInfo, которая включает в себя хэш полученный из запроса, дату и время создания штампа времени (текущая дата и время), серийный номер штампа времени;
4. Модуль выполняет подписание кодированной в ASN.1 структуры TSTInfo посредством обращения к Средству ЭП;
5. Модуль формирует и возвращает ответ, содержащий штамп времени.

4.2.13. Описание процесса формирования пользовательской ЭП формата CAdES-BES

Процесс создания пользовательской ЭП в форматах, CAdES-BES:

1. Создаваемые подсистемы АИС ФССП обращаются к клиентскому модулю ЭП, передавая:
   - Подписываемые данные, либо в виде ссылки на объектное хранилище, либо в виде идентификатора подписываемого объекта;
   - Требуемый формат ЭП;
   - Мета-информация о подписываемом объекте. Необходима для отображения в диалоге подписания и определении возможности визуализации средствами браузера;
   - Бизнес тип подписи. Отображается в диалоге подписи.

2. Клиентский модуль ЭП (далее Модуль) использует полученную информацию для получения подписываемых данных из хранилища бинарных данных по ссылке, либо через обращение к сервису ПС, который выполняет подготовку подписываемых данных по идентификатору документа;
3. Модуль обращается к Модуль ЭП для браузера для получения списка доступных для подписания СКП;
4. Полученные СКП Модуль отправляет в Сервис проверки сертификатов и СОС, для их проверки;
   Процесс проверки СКП описан в п. 4.2.2.
5. СКП, прошедшие проверку, отображаются пользователю, для выбора СКП, который будет использоваться для подписания;
6. После выбора пользователем СКП, Модуль выполняет подготовку контейнера ЭП формата CAdES-BES, для хеширования данных Модуль обращается Сервису расчета хэш-функции. В результате подготовки формируются:
   - Контейнер ЭП формата CAdES-BES, без математической (чистой) подписи;
   - Хеш, для подписания пользователем.
7. Модуль осуществляет визуализацию подписываемых данных. В диалоге, который отображается пользователю, по умолчанию видна общая информация о формируемой подписи. Визуализация подписываемых данных может быть выполнена по запросу пользователя, через просмотр средствами браузера (если позволяет формат файла и его размер), либо через скачивание файла на АРМ пользователя и просмотр отдельным ПО, установленным на АРМ.
8. Модуль формирует и передает модулю ЭП для веб-обозревателя (браузера) запрос на создание ЭП, содержащий:
   – Рассчитанный хэш для подписания;
   – Отпечаток СКП, выбранного пользователем;
9. Модуль ЭП для веб-обозревателя (браузера) формирует и передает средству ЭП запрос на создание ЭП, содержащий данные указанные в п. 8 процесса.
10. Средство ЭП в системном хранилище ОС производит поиск СКП, соответствующего полученному в запросе отпечатку, и соответствующего ему ключа ЭП, создает и возвращает математическую (чистую) ЭП.
11. Модуль ЭП для веб-обозревателя (браузера) возвращает математическую ЭП в Модуль.
12. Модуль встраивает полученную математическую ЭП в подготовленный контейнер формата CAdES-BES, и обращается к Сервису проверки ЭП, передавая его для проверки.
13. Сервису проверки ЭП выполняет проверку ЭП (алгоритм описан в п. 4.2.5.) и доведение ЭП до требуемого формата (алгоритм описан в п. 4.2.6.), если требуется, возвращает результат в Модуль.
14. Модуль вызывает сервис ПС, для сохранения сформированной ЭП в БД.

4.2.14. Описание процесса формирования пользовательской ЭП формата XAdES-BES

Процесс создания пользовательской ЭП форматов XAdES-BES:

1. ПС обращаются к Клиентскому модулю ЭП (далее Модуль), передавая:
   - Подписываемые данные, либо в виде ссылки на объектное хранилище, либо в виде идентификатора подписываемого объекта;
   - Требуемый формат ЭП;

- Id подписываемых элементов xml документов и набор трансформаций, которые необходимо применить к данным перед вычислением хэш-функции;
- Мета-информация о подписываемом объекте. Необходима для отображения в диалоге подписания;
- Бизнес тип подписи. Отображается в диалоге подписи.

2. Модуль использует полученную информацию для получения подписываемых данных из хранилища бинарных данных по ссылке, либо через обращение к сервису ПС, который выполняет подготовку подписываемых данных по идентификатору документа;
3. Модуль обращается к Модуль ЭП для браузера для получения списка доступных для подписания СКП;
4. Полученные СКП Клиентский модуль ЭП отправляет в Сервис проверки сертификатов и СОС, для их проверки на возможность использования при пользовательской подписи.
   Процесс проверки СКП описан в п. 4.2.2.
5. СКП, прошедшие проверку, отображаются пользователю, для выбора СКП, который будет использоваться для подписания;
6. После выбора пользователем СКП Клиентский модуль ЭП выполняет подготовку контейнера ЭП формата XAdES-BES, для расчета хэш-функции от данных Модуль вызывает Сервис расчета хэш-функции. В результате подготовки формируются:

   - Контейнер ЭП формата XAdES-BES, без математической подписи;
   - Хеш элемента SignedInfo, для подписания пользователем.

7. Модуль осуществляет визуализацию подписываемых данных. В диалоге, который отображается пользователю, по умолчанию видна только общая информация о формируемой подписи. Визуализация подписываемых данных может быть выполнена по запросу пользователя, через просмотр средствами браузера (если позволяет его размер), либо через скачивание файла на АРМ пользователя и просмотр отдельным ПО, установленным на АРМ.
8. Модуль формирует и передает Модулю ЭП для веб-обозревателя (браузера) запрос на создание ЭП, содержащий:

   – Рассчитанный хэш для подписания;
   – Отпечаток СКП, выбранного пользователем;

9. Модуль ЭП для веб-обозревателя (браузера) формирует и передает средству ЭП запрос на создание ЭП, содержащий данные указанные в п. 8 процесса.
10. Средство ЭП в системном хранилище ОС производит поиск СКП, соответствующего полученному в запросе отпечатку, и соответствующего ему ключа ЭП, создает и возвращает математическую ЭП.
11. Модуль ЭП для веб-обозревателя (браузера) возвращает математическую ЭП в клиентский модуль ЭП.
12. Модуль встраивает полученную математическую ЭП в подготовленный контейнер формата XAdES-BES, и вызывает Сервис проверки ЭП, передавая его для проверки.
13. Сервис проверки ЭП выполняет проверку ЭП (алгоритм описан в п. 4.2.8.) и доведение ЭП до требуемого формата (алгоритм описан в п. 4.2.9.), если требуется, возвращает результат проверки ЭП в Модуль.
14. Модуль вызывает сервис ПС, для сохранения сформированной ЭП в БД.

СПИСОК ИЗМЕНЕНИЙ

Версия	Дата	Внесенные изменения	Исполнитель
1.0	09.11.2020	Создание документа	Ахтямов Е.Б.