КОД безопасности

Программно-аппаратный комплекс
квалифицированной электронной подписи

Jinn-Server
Версия 1.3

Руководство программиста

RU.88338853.501430.024 33

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Введение

Руководство предназначено для программистов, работающих с изделием "Программно-аппаратный комплекс квалифицированной электронной подписи Jinn-Server. Версия 1.3" (далее — ПАК Jinn-Server, Jinn-Server, комплекс, ПАК). В руководстве содержатся сведения, необходимые для интеграции комплекса и его сопряжения с программным обеспечением клиентской информационной системы.

Дополнительные сведения по работе с ПАК Jinn-Server содержатся также в [**1**] и [**2**].

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Основные понятия, термины и определения

Термин	Определение
АРМ РКС	Автоматизированное рабочее место разбора конфликтных ситуаций
БД	База данных
ГУЦ	Головной удостоверяющий центр
ДМЗ (DMZ)	Демилитаризованная зона (Demilitarized zone) — технология обеспечения защиты информационного периметра, при которой серверы, отвечающие на запросы из внешней сети, находятся в особом сегменте сети и ограничены в доступе к основным сегментам сети с помощью межсетевого экрана с целью минимизировать ущерб при взломе одного из общедоступных сервисов, находящихся в ДМЗ
ИОК (PKI)	Инфраструктура открытых ключей (Public Key Infrastructure) — комплекс программных и/или программно-аппаратных средств и организационно-технических мероприятий по обеспечению использования криптографии с открытым ключом, управления этими ключами и сертификатами, в частности, для решения задач защищенного электронного документооборота
ИТ-система	Информационная система, которая использует функции Jinn-Server через SOAP-интерфейс
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации. СКЗИ осуществляет криптографическое преобразование информации для обеспечения ее безопасности
СМЭВ	Система межведомственного электронного взаимодействия
СОС (CRL)	Список отозванных сертификатов (Certificate revocation list)
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр. УЦ в рамках своей деятельности осуществляет создание сертификатов ключей проверки ЭП, а также ведет реестр CRL
ЭД	Электронный документ
ЭП	Электронная подпись
API	Application Programming Interface — программный интерфейс приложения
CAdES	CMS Advanced Electronic Signatures (расширенная версия формата CMS) — формат ЭП
CAS	CRL Archiving Service — сервис, предназначенный для сбора и автоматического обновления списков отозванных сертификатов и обновлений к ним (deltaCRL) с целью последующего использования хранимых CRL другими компонентами Jinn-Server
CDP	CRL Distribution Point — точки распространения (публикации) CRL УЦ
CFV	Certificate Format Validation — составная часть сервиса SVS, предназначенная для проверки сертификатов авторов подписи на соответствие требованиям к квалифицированным сертификатам
CMS	Cryptographic Message Syntax (синтаксис криптографических сообщений) — формат ЭП
CSA	Conflict Service Audit — сервис разбора конфликтов
deltaCRL	Обновление к СОС, выпускаемое УЦ в интервале между выпусками СОС
DNS	Domain Name System — система доменных имен
HTML	HyperText Markup Language — язык гипертекстовой разметки
HTTP	HyperText Transfer Protocol — протокол передачи гипертекста
IP	Internet Protocol — межсетевой протокол
IP-адрес	Уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP
MTOM	Message Transmission Optimization Mechanism — механизм оптимизации передачи сообщений
NTP	Network Time Protocol — протокол сетевого времени
OID	Object Identifier — уникальный идентификатор объекта в виде последовательности десятичных цифр
SNMP	Simple Network Management Protocol — протокол сетевого управления

Термин	Определение
SOAP	Simple Object Access Protocol (простой протокол доступа к объектам) — протокол обмена структурированными сообщениями в распределенной вычислительной среде
SS	SigningService — сервис, предназначенный для формирования ЭП
SVS	SignatureValidationService — сервис, предназначенный для проверки данных, подписанных ЭП, и усиления ЭП
TCP	Transmission Control Protocol — протокол управления передачей данных
TSL	Trusted Service List — список доверенных издателей (аккредитованных УЦ)
UDP	User Datagram Protocol — протокол пользовательских датаграмм
URL	Uniform Resource Locator — сетевой адрес ресурса
WebUI	Графический интерфейс подсистемы администрирования Jinn-Server
WS-Security (WSSec)	Web Services Security — формат ЭП блоков XML-данных
WSDL	Web Services Description Language — язык (в формате XML) описания веб-сервисов и доступа к ним
XAdES	XML Advanced Electronic Signatures (расширенная версия формата XMLDSig) — формат ЭП блоков XML-данных
XML	eXtensible Markup Language — расширяемый язык разметки
XMLDSig	XML Digital Signature — формат ЭП блоков XML-данных
XSLT	eXtensible Stylesheet Language Transformations — язык преобразования XML-документов

Глава 1
Общие сведения о ПАК Jinn-Server

Назначение, состав и структура ПАК Jinn-Server

ПАК Jinn-Server совместно с набором дополнительных программных средств предназначен для выполнения функции автоматической проверки и формирования ЭП документов с последующей сетевой выгрузкой результата криптографического преобразования во внешний сервис клиентской системы электронного документооборота, формирующей запросы на проверку и выработку ЭП к Jinn-Server.

Программное обеспечение Jinn-Server построено по модульному принципу и состоит из следующих веб-сервисов:

- сервис проверки ЭП (SVS — SignatureValidationService) — предназначен для проверки данных, подписанных ЭП, и усиления ЭП (в зависимости от параметров запроса), а также проверки сертификатов ЭП на действительность и соответствие требованиям к квалифицированным сертификатам;
- сервис формирования ЭП (SS — SigningService) — предназначен для выработки ЭП;
- сервис архивирования COC/CRL (CAS — CRLArchivingService) — предназначен для сбора и автоматического обновления списков отозванных сертификатов и обновлений к ним с целью последующего использования хранимых CRL другими компонентами ПАК. Этот сервис разделен на два модуля — внутренний сборщик CRL (CAS–1) и внешний (CAS–2);
- графический интерфейс подсистемы администрирования (WebUI, сервис ADMIN) — предназначен для мониторинга и конфигурации компонентов комплекса, а также для работы с сертификатами;
- сервис разбора конфликтов — предназначен для рассмотрения спорных ситуаций, возникающих при проверке ЭП, а также получения дополнительной информации по действительности сертификатов и ЭП на заданный момент времени. Данная информация используется в дальнейшем для урегулирования всех спорных юридических вопросов, связанных с особенностями PKI инфраструктуры.

На рисунке 1 представлена общая схема развертывания компонентов ПАК Jinn-Server (выделены светлым оттенком охры) и их взаимодействие с внешними информационными системами (выделены синим цветом).

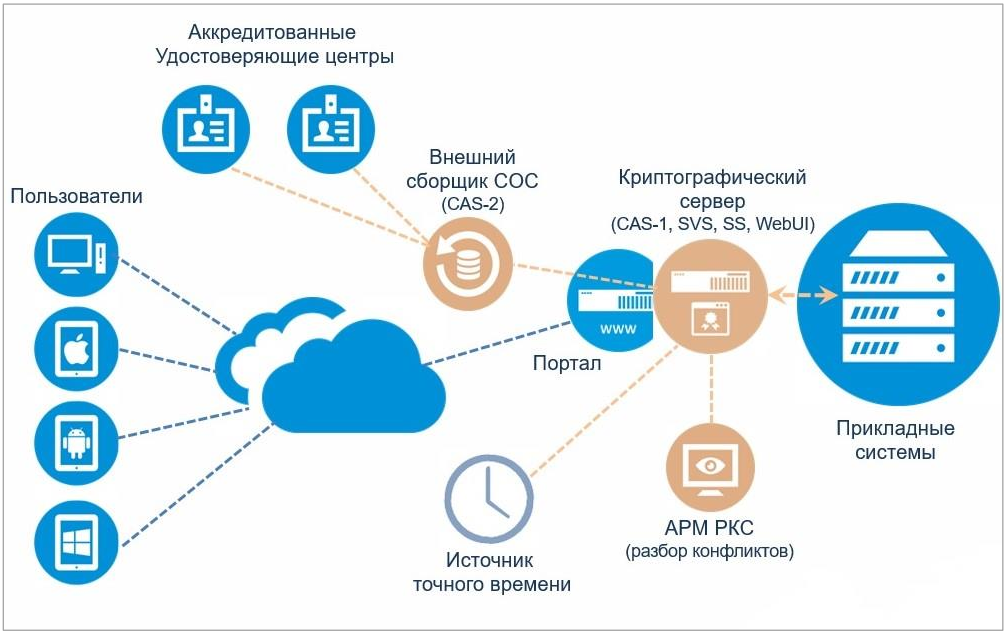

Рис. 1 Общая схема развертывания компонентов ПАК Jinn-Server

Аппаратная архитектура ПАК Jinn-Server состоит из следующих серверов и АРМ:

- криптографический сервер (сервер CAS–1) — сервер с развернутыми программными модулями CAS–1, SVS, SS, ADMIN и СКЗИ "КриптоПро CSP" 5.0;
- внешний сборщик СОС (сервер CAS–2) — сервер с развернутым программным модулем CAS–2, размещаемый в DMZ и имеющий выход в открытые телекоммуникационные сети (интернет);
- АРМ РКС — наличие отдельного АРМ для развертывания сервиса разбора конфликтов опционально.

Серверы и АРМ РКС, входящие в состав ПАК Jinn-Server, функционируют под управлением дистрибутива ОС семейства Linux — CentOS 8.1 x64.

Для хранения обрабатываемой информации на серверах CAS–1 и CAS–2 развернута БД csm под управлением СУБД PostgreSQL.

Архив собранных CRL передается между серверами CAS–2 и CAS–1 по протоколу TCP или с использованием отчуждаемого носителя (флеш-накопителя).

Для формирования штампов времени ЭП и синхронизации компонентов комплекса в ПАК Jinn-Server предусмотрена возможность работы с внешними источниками точного времени по протоколу сетевого времени NTP.

Доступ к криптографическим функциям производится с использованием MicrosoftCryptoAPI для СКЗИ "КриптоПро CSP" 5.0 для платформы ОС семейства Linux.

ПАК Jinn-Server может совместно работать с сертифицированным средством защиты информации ПАК "Соболь" версий 3.0, 3.1, 3.2 и антивирусным ПО Kaspersky Endpoint Security для Linux.

Сервисы ПАК Jinn-Server

Сервис проверки ЭП

Сервис SVS поддерживает следующие форматы ЭП — CMS, CAdES-BES, CAdES-T, CAdES-C, CAdES-A, XMLDSig, XAdES-BES, XAdES-T, XAdES-C, XAdES-A, WSSec-BES, WSSec-T, WSSec-C, WSSec-A.

Обработка заверяющей подписи (ЭП с атрибутом counterSignature) в Jinn-Server не поддерживается.

Сервис SVS выполняет криптографические преобразования по ГОСТ — ЭП в соответствии с ГОСТ Р 34.10–2012 и ГОСТ Р 34.10–2001, хэш-функция в соответствии с ГОСТ Р 34.11–2012 и ГОСТ Р 34.11–94.

Доступ к сервису SVS осуществляется поверх протокола HTTP по порту 8080 через внешний SOAP-запрос.

Сервис SVS обрабатывает входящие запросы на проверку ЭП, проверку и усиление ЭП, проверку структуры сертификата и проверку действительности сертификата.

Структура запросов к сервису SVS приведена в разделе "Описание структур входных и выходных данных веб-сервисов".

Примечание. Для передачи данных (запрос — ответ) при взаимодействии с сервисом SVS поддерживается использование MTOM.

При запросе на проверку ЭП проверяются все ЭП подписанного документа и итоговый результат содержит информацию о каждой из них.

Сервис SVS поддерживает проверку отсоединенных подписей. В этом случае исходные данные должны передаваться дополнительным параметром в запросе.

При проверке блоков XML-данных сервис SVS обеспечивает проверку всего XML или проверку отдельного элемента, входящего в XML, определяемого по ID переданного в параметрах запроса.

Сервис SVS при проверке подписи в формате WS-Security поддерживает обработку значения атрибута "actor", переданного дополнительным параметром в запросе.

Запрос на проверку и усиление ЭП поддерживает указание конкретного формата усиления, и в случае успешной проверки подписи и сертификата автора проверяемые данные дополняются необходимыми атрибутами так, чтобы привести обрабатываемые данные, в зависимости от исходного формата, в соответствие указанной спецификации — CAdES-T, CAdES-C, CAdES-A, XAdES-T, XAdES-C, XAdES-A. Для формата WS-Security усиление выполняется аналогично XAdES.

При запросе на проверку и усиление подписи блоков XML-данных проверяется и усиливается только одна ("внешняя" по отношению к остальным подписанным элементам, входящим в XML) подпись, определяемая по ID переданного в параметрах запроса, если документ или его части подписаны несколькими подписями.

В сервис SVS встроен сервис CFV, который осуществляет проверку структуры сертификатов на соответствие требованиям к квалифицированным сертификатам.

Подтверждение действительности сертификатов авторов ЭП производится сервисом SVS путем проверки отсутствия сведений об отзыве (приостановке действия) проверяемых сертификатов в CRL УЦ, загружаемых сервисом архивирования CRL. К обработке принимаются только CRL и обновления к ним, непосредственно подписанные ключом того же доверенного издателя, что и проверяемый сертификат, либо, в случае indirect CRL, ключом специально выделенного для выпуска CRL сертификата, также непосредственно подписанным соответствующим издателем. В случае использования indirect CRL сертификат, выделенный соответствующим издателем для выпуска CRL, должен устанавливаться в ПАК через подсистему администрирования, аналогично сертификату издателя.

Сервис SVS спроектирован с учетом того, что авторы проверяемых ЭП принадлежат к изначально ограниченному и административно определяемому числу УЦ (набору издателей), сертификаты которых рассматриваются сервисом проверки как доверенные.

Сервис формирования ЭП

Сервис SS формирует ЭП в следующих форматах — CMS, CAdES-BES, CAdES-T, CAdES-C, CAdES-A, XMLDSig, XAdES-BES, XAdES-T, XAdES-C, XAdES-A, WSSec-T, WSSec-C, WSSec-A.

Сервис SS выполняет криптографические преобразования по ГОСТ — ЭП в соответствии с ГОСТ Р 34.10–2012 и ГОСТ Р 34.10–2001, хэш-функция в соответствии с ГОСТ Р 34.11–2012 и ГОСТ Р 34.11–94.

Доступ к сервису SS осуществляется поверх протокола HTTP по порту 8080 через внешний SOAP-запрос.

Сервис SS обрабатывает входящие запросы на расчет хэша или формирование ЭП в соответствии с явно указанным в запросе стандартом.

Структура запросов к сервису SS приведена в разделе "Описание структур входных и выходных данных веб-сервисов".

Примечание. Для передачи данных (запрос — ответ) при взаимодействии с сервисом SS поддерживается использование MTOM. При использовании MTOM в запросе указывается, что должна быть сформирована откреплённая ЭП, ответ сервера содержит только ЭП.

Сервис SS поддерживает формирование отсоединенных подписей.

При подписании блоков XML-данных сервис SS обеспечивает подписание всего XML или подписание отдельного элемента, входящего в XML, определяемого по ID переданного в параметрах запроса.

Сервис SS при формировании подписи в формате WS-Security поддерживает обработку значения атрибута "actor", переданного дополнительным параметром в запросе.

Сервис SS поддерживает применение набора трансформов (правил нормализации XML-документов) — XPath, XSLT, SMEV3, при их объявлении в составе структуры SignedInfo при формировании подписи в формате XMLDSig и её расширенных версий (XAdES, WS-Security) для взаимодействия со СМЭВ.

При формировании подписи доступен выбор одного из ключевых контейнеров, принадлежащего только указанной в запросе подсистеме.

Сервис архивирования CRL

Сервис CAS предназначен для загрузки и автоматического обновления списков отозванных сертификатов и обновлений к ним с целью последующего использования хранимых CRL другими компонентами ПАК. Этот сервис разделен на два модуля — внутренний сборщик CRL (CAS–1) и внешний (CAS–2), что продиктовано необходимостью размещения криптографических сервисов Jinn-Server и СКЗИ в защищенном сегменте сети, не имеющем доступа к сети интернет.

Модуль CAS–2, предназначенный для загрузки CRL и обновлений к ним из точек публикации, размещается в отдельном сегменте сети, откуда доступ в интернет возможен, а коммуникация между модулями CAS–2 и CAS–1 осуществляется посредством передачи файлов на учтенных отчуждаемых носителях или по TCP-протоколу по каналу, где передача данных контролируется установленными средствами защиты от сетевых атак, сертифицированными ФСТЭК России.

На рисунке 2 представлена общая схема взаимодействия сервисов SVS, SS и модулей сервиса CAS с внешними системами и между собой.

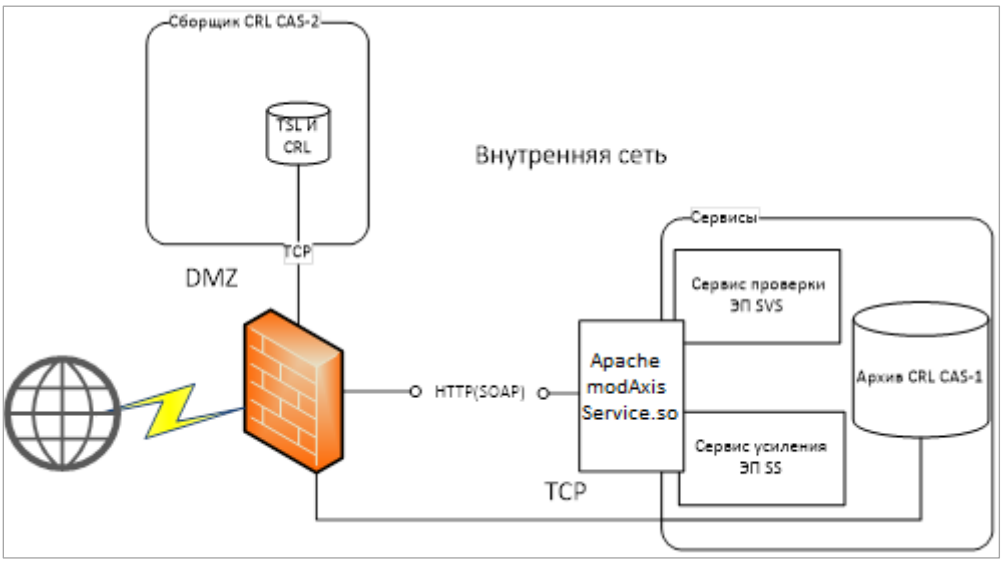

Рис. 2 Схема взаимодействия модулей сервиса CAS

Доступ к точкам публикации CRL осуществляется модулем CAS–2 по протоколу HTTP. Точки публикации CRL задаются при регистрации издателя через подсистему администрирования. Для доверенных УЦ из списка TSL точки публикации CRL определяются автоматически на основании соответствующего расширения (стандартного CDP или FreshestCRL — соответственно для регулярных CRL и их обновлений) сертификата УЦ. В случае отсутствия такого расширения у сертификата УЦ точки публикации его CRL задаются через подсистему администрирования.

Загрузка регулярных CRL из точек публикации осуществляется в автоматическом режиме через заданные в диспетчере расписаний интервалы времени. При этом для очередного регулярного CRL загрузка начинается за некоторое фиксированное время до наступления даты, указанной в поле nextUpdate имеющегося CRL.

Подсистема администрирования

Подсистема администрирования предоставляет графический интерфейс пользователю и обеспечивает мониторинг состояния сервисов ПАК Jinn-Server, а также возможность для изменения определенных конфигурационных настроек компонентов комплекса.

Подсистема администрирования предоставляет средства регистрации сертификатов и CRL УЦ — издателей ключевых контейнеров, использующихся сервисом SS при формировании ЭП и выработке штампов времени.

Подсистема администрирования предоставляет средства регистрации доверенных УЦ из списка TSL, что необходимо для функционирования сервисов проверки ЭП и разбора конфликтов.

Подсистема администрирования предоставляет средства управления сертификатами и CRL зарегистрированных УЦ:

- импорт/экспорт сертификатов УЦ и соответствующих им CRL. Средства импорта обеспечивают выгрузку данных для зарегистрированных издателей;
- возможность отметить сертификат определенного издателя как неактивный (в этом случае загрузка/обновление соответствующих CRL производиться не будет) либо полностью удалить издателя и все соответствующие ему CRL;
- возможность задания/изменения точки публикации CRL для определенного издателя;
- возможность задания упреждающего периода для загрузки очередного регулярного CRL;
- возможность принудительной загрузки/обновления CRL для одного, нескольких или всех активных издателей.

Подсистема администрирования предоставляет средства проверки формата сертификатов на соответствие требованиям к квалифицированным сертификатам.

Для входа в подсистему администрирования необходимо пройти аутентификацию (см. [**1**]).

Сервис разбора конфликтов

Сервис разбора конфликтов предоставляет графический интерфейс пользователю и предназначен для рассмотрения следующих спорных ситуаций, в случае признания ЭП недействительной:

- оспаривание действительности ЭП документа путем проверки ЭП, определения даты ЭП, проверки подписи штампа времени (при наличии) и действительности цепочки сертификатов на момент подписи или на заданный пользователем момент времени;
- оспаривание действительности сертификата ключа проверки электронной подписи с помощью выстраивания цепочки сертификатов и проверки их действительности на момент времени, указанный в штампе времени, или на заданный пользователем момент времени.

Сервис разбора конфликтов формирует отчет о результатах проверки ЭП.

Глава 2
Условия функционирования ПАК Jinn-Server

Требования к программным средствам

ОС

Серверы CAS–1, CAS–2 и АРМ РКС, входящие в состав ПАК Jinn-Server, функционируют под управлением дистрибутива ОС семейства Linux — CentOS 8.1.

Также на основании лицензии производителя дистрибутива ОС используются компиляторы, загрузчики, препроцессоры, библиотеки, пакеты, сборки и т. п., входящие в состав дистрибутива.

СУБД

Для хранения обрабатываемой информации на серверах CAS–1 и CAS–2 развернута БД csm под управлением СУБД PostgreSQL.

Установка СУБД PostgreSQL и создание структуры БД csm осуществляется в процессе установки ПО Jinn-Server.

СКЗИ

Для формирования и проверки ЭП в ПАК Jinn-Server используется сертифицированное ФСБ России СКЗИ (вплоть до класса КС2 включительно, в части защиты информации, не содержащей сведений, составляющих государственную тайну) "КриптоПро CSP" 5.0 для платформы ОС семейства Linux производства компании "КРИПТО-ПРО".

ПАК Jinn-Server (класс защиты КС2) функционирует совместно с сертифицированным ФСБ России изделием "Программно-аппаратный комплекс "Соболь" версии 3.0/3.1/3.2 (далее — ПАК "Соболь").

Порты, используемые ПАК Jinn-Server

Порты, используемые ПАК Jinn-Server, приведены в таблице 1. Должен быть настроен доступ к указанным портам при конфигурации внешних средств защиты, таких как пакетные фильтры, межсетевые экраны и т.п.

Табл. 1 Порты, используемые ПАК Jinn-Server

Компонент	Порт	Характеристика сервиса
Сервер CAS–1	TCP_80	Гипертекстовый интерфейс управления и администрирования CAS–1
	TCP_8080	Транспортный протокол HTTP, обслуживающий запросы к сервисам формирования и проверки ЭП
	TCP_11112	CRL Archiving Daemon
	UDP_161, UDP_162	Службы SNMP
	TCP_22	SSH для удаленного доступа
	UDP_53 (исходящее соединение)	Доступ к DNS-серверу
Сервер CAS–2	TCP_11113	Сборщик СОС
	UDP_161, UDP_162	Службы SNMP
	TCP_22	SSH для удаленного доступа
	UDP_53 (исходящее соединение)	Доступ к DNS-серверу

Компонент	Порт	Характеристика сервиса
АРМ РКС	TCP_8083	Гипертекстовый интерфейс управления и администрирования АРМ РКС (доступ к интерфейсу проверки ЭП документов и отчетам о результатах проверки ЭП)
	TCP_8080	Транспортный протокол HTTP, обслуживающий запросы к сервису разбора конфликтов
	UDP_161, UDP_162	Службы SNMP
	TCP_22	SSH для удаленного доступа
	UDP_53 (исходящее соединение)	Доступ к DNS-серверу

Веб-обозреватель

Для работы графического интерфейса подсистемы администрирования используются следующие веб-обозреватели:

- Google Chrome 86;
- Mozilla Firefox 81.

Требования к аппаратным средствам

Сервер CAS–1

Сервер CAS–1 должен соответствовать следующим аппаратным требованиям:

- процессор Intel® Xeon 5000 (и выше) с количеством ядер не менее 6 и тактовой частотой не менее 2,4 ГГц;
- оперативная память не менее 64 ГБ;
- свободное дисковое пространство не менее 20 ГБ;
- сетевой интерфейс Ethernet 10/100/1000 Мбит/с;
- интерфейс USB 2.0;
- интерфейс PCI-E — для установки платы ПАК "Соболь" (наличие данного интерфейса опционально и зависит от варианта исполнения ПАК Jinn-Server);
- привод DVD/CD-ROM.

Сервер CAS–2

Сервер CAS–2 должен соответствовать следующим аппаратным требованиям:

- процессор Intel® семейства x86 (или совместимый) в соответствии с требованиями ОС, установленной на сервер;
- оперативная память не менее 16 ГБ;
- свободное дисковое пространство не менее 10 ГБ;
- сетевой интерфейс Ethernet 10/100/1000 Мбит/с;
- интерфейс USB 2.0;
- интерфейс PCI-E — для установки платы ПАК "Соболь" (наличие данного интерфейса опционально и зависит от варианта исполнения ПАК Jinn-Server);
- привод DVD/CD-ROM.

АРМ РКС

АРМ РКС должно соответствовать следующим аппаратным требованиям:

- процессор Intel® семейства x86 (или совместимый) в соответствии с требованиями ОС, установленной на АРМ;
- оперативная память не менее 2 ГБ;
- свободное дисковое пространство не менее 10 ГБ;
- сетевой интерфейс Ethernet 10/100/1000 Мбит/с;

- интерфейс USB 2.0;
- интерфейс PCI-E — для установки платы ПАК "Соболь" (наличие данного интерфейса опционально и зависит от варианта исполнения ПАК Jinn-Server);
- привод DVD/CD-ROM.

Требования к персоналу

Программист должен иметь как минимум среднее техническое образование и должен быть аттестован как минимум на II квалификационную группу по электробезопасности (для работы с конторским оборудованием).

В перечень задач, выполняемых программистом, должны входить:

- контроль за работоспособностью технических средств;
- контроль за работоспособностью системных программных средств — операционной системы и иных программных компонентов в объеме, необходимом для выполнения ПАК Jinn-Server своего функционального назначения;
- контроль за выполнением ПАК Jinn-Server своих функций, помощь в выполнении своих функций операторам ПАК;
- обеспечение работоспособности сервисов и передачи информации между компонентами ПАК и во внешние модули прикладной системы;
- ведение архивных копий информационных активов ПАК (БД csm, прикладные и системные журналы и т.д.).

В рамках своих задач программист взаимодействует и с администратором системы, и с пользователями (операторами).

Глава 3
Входные и выходные данные

ПАК Jinn-Server представляет собой совокупность веб-сервисов и средств оперативного администрирования.

Веб-сервисы SVS и SS в качестве входных данных получают SOAP-запрос в виде XML-сообщения от внешней клиентской ИТ-системы, а в качестве выходных — формируют ответ в виде XML-сообщения и выгружают его в ИТ-систему.

Описание средств оперативного администрирования ПАК Jinn-Server представлено в [**2**].

API для управления ПАК Jinn-Server предоставляет возможности для формирования запросов к комплексу (входные данные) и получения ответов (выходные данные) внешними прикладными системами.

Глава 4
Описание API для управления ПАК Jinn-Server

Объекты

Объекты — основные сущности, которыми оперирует API.

Объект **host** — физическая машина.

Свойства объекта host:

- id — уникальный идентификатор, автоматически генерируемый в момент регистрации;
- name — имя объекта;
- address — IP-адрес. Задается в момент регистрации и не меняется.

Объект **subsystem** — подсистема, к которой могут быть привязаны определенные сервисные сертификаты/ключевые контейнеры. При этом один сертификат может быть привязан к любому числу подсистем.

Свойства объекта subsystem:

- id — уникальный идентификатор, автоматически генерируемый в момент регистрации. Значение "0" зарезервировано для ключей, не прикрепленных ни к одной из подсистем. Такие ключи могут использоваться только при обработке запросов, в которых не указан идентификатор подсистемы;
- name — имя объекта.

Объект **trustDomain** — домен доверия, к которому может быть привязан набор издателей. При этом один издатель может быть привязан к любому числу доменов доверия.

Свойства объекта trustDomain:

- id — уникальный идентификатор, автоматически генерируемый в момент регистрации. Значение "0" зарезервировано для издателей, перечисленных в TSL. Значение "1" зарезервировано для всех зарегистрированных издателей;
- name — имя объекта.

Объект **issuer** — издатель.

Свойство объекта issuer:

- id — уникальный идентификатор, автоматически генерируемый в момент регистрации либо загрузки TSL.

Управление настройками

API предоставляет следующие возможности по управлению настройками Jinn-Server:

- получение и установка параметров в конфигурационных файлах сервисов cas1, svs, ss;
- управление сервисами — получение и установка статуса сервисов cas1, svs, ss, admin, ws, postgres.

Запросы и ответы на получение и установку конфигурационных параметров сервисов являются списками, где каждый элемент внутри тега <configEntry> содержит следующую информацию:

- идентификатор управляемого хоста (<hostId>). Указывается значение "0";
- имя сервиса (<svc>);
- имя запрашиваемого или устанавливаемого параметра (<id>);
- значение конфигурационного параметра (<value>). Наличие элемента опционально, так как в запросе на получение параметра элемент не имеет смысла.

Примечание. При получении и установке значений конфигурационных параметров применяются следующие ограничения и правила:

- символы, имеющие специальное значение в XML, в значениях параметров не допускаются;
- получение и установка числовых значений — <value>472597</value>;
- получение строковых значений (строковые значения возвращаются в двойных кавычках) — <value>"string"</value>;
- установка строковых значений — <value>string</value>. При этом строковые значения, которые могут быть восприняты как числовые значения, необходимо передавать в апострофах и двойных кавычках, дополнительно экранировав двойные кавычки с помощью символа '\' — <value>' \"631" ' </value>.

Элемент <groupid> является deprecated-параметром и не используется.

Получение и установка конфигурационных параметров

Запрос **configGet** — получение конфигурационного параметра.

Структура запроса:

```
<csm:configGetRequest>
         <!--1 or more repetitions:-->
         <csm:configEntry>
      <!--Id хоста-->
            <csm:hostId>?</csm:hostId>
            <!--Optional:-->
      <!--Имя сервиса, конфигурационные файлы которого
настраиваются-->
            <csm:svc>?</csm:svc>
            <csm:nameAndValue>
               <!--Имя поля,- значение которого хотим
получить-->
               <csm:id>?</csm:id>
            </csm:nameAndValue>
         </csm:configEntry>
       </csm:configGetRequest>
```

Структура ответа:

```
<configGetResponse>
<configEntry>
            <hostId>?</hostId>
            <svc>?</svc>
            <nameAndValue>
               <id>?</id>
             <!--Полученное значение поля-->
            <value>?</value>
            </nameAndValue>
</configEntry>
</configGetResponse>
```

Запрос **configSet** — установка конфигурационного параметра.

Структура запроса:

```
<csm:configSetRequest>
         <!--1 or more repetitions:-->
         <csm:configEntry>
      <!--Id хоста-->
            <csm:hostId>?</csm:hostId>
            <!--Optional:-->
```

```
     <!--Имя сервиса, конфигурационные файлы которого
настраиваются-->
     <!--Допустимые сервисы: ss, svs, cas1-->
           <csm:svc>?</csm:svc>
           <csm:nameAndValue>
              <!--Имя поля, значение которого хотим задать-->
              <csm:id>?</csm:id>
          <!--Задаваемое значение поля-->
          <csm:value>?</csm:value>
            </csm:nameAndValue>
         </csm:configEntry>
      </csm:configSetRequest>
```

Структура ответа:

```
<configSetResponse>
<configEntry>
            <hostId >?</hostId>
            <svc>?</svc>
            <nameAndValue>
               <id>?</id>
             <!--Установленное значение поля-->
      <value>?</value>
            </nameAndValue>
         </configEntry>
</configSetResponse>
```

Управление сервисами

Для получения статуса сервиса в запросе **configGet** укажите имя запрашиваемого параметра (тег <id>) — service.status:

```
     <csm:nameAndValue>
               <csm:id>service.status</csm:id>
            </csm:nameAndValue>
```

Для установки статуса сервиса в запросе **configSet** укажите имя устанавливаемого параметра — service (тег <id>) и значение параметра — stop, start или restart (тег <value>):

```
     <csm:nameAndValue>
               <csm:id>service</csm:id>
          <!--Допустимые значения поля: stop,start,restart-->
          <csm:value>stop</csm:value>
        </csm:nameAndValue>
```

Управление ключами ИТ-систем

Управление ИТ-системами

В API доступны регистрация, удаление, перечисление, привязка и отключение от групп хостов ИТ-систем и вывод информации о связях ИТ-систем и групп хостов.

Управление связями производится с помощью SOAP-запросов на получение и изменение конфигурации или с помощью командной оболочки ОС. В случае управления с помощью SOAP-запросов hostId должно иметь значение идентификатора хоста CAS–1, а имя сервиса (svc) иметь значение Subsystems. Модуль, реализующий управление подсистемами посредством командной оболочки ОС, — /opt/tccs/bin/subsys_control.py.

По умолчанию предустановлены три подсистемы:

Идентификатор	Описание
0	Ключевые контейнеры, прошедшие регистрацию в Jinn-Server
1	Ключевые контейнеры, доступные для CSP
2	Ключевые контейнеры, доступные при всех операциях усиления и формирования ЭП

Предустановленные подсистемы нельзя удалить, а их идентификаторы нельзя изменить.

Регистрация подсистем

В качестве имени параметра в SOAP-запросе указывается create. Параметром для запроса на регистрацию является имя подсистемы (должно быть уникально). Ответ — уникальный идентификатор подсистемы. Для имен допустимы буквенные символы (латиница), цифры (0–9) и знаки "_" и "-".

Пример SOAP-запроса:

```
<soapenv:Body>
      <csm:configSetRequest>
      <csm:hostId>1</csm:hostId>
            <csm:svc>Subsystems</csm:svc>
            <csm:nameAndValue>
               <csm:id>create</csm:id>
               <csm:value>test_susbsystem-1</csm:value>
            </csm:nameAndValue>
         </csm:configEntry>
      </csm:configSetRequest>
   </soapenv:Body>
```

Пример команды:

```
/opt/tccs/bin/subsys_control.py --create test_susbsystem-1
```

Удаление подсистем

В качестве имени параметра в SOAP-запросе указывается delete. Параметром для запроса на удаление является уникальный идентификатор подсистемы. Ответ — сообщение о статусе операции.

Пример SOAP-запроса:

```
<soapenv:Body>
      <csm:configSetRequest>
      <csm:hostId>1</csm:hostId>
            <csm:svc>Subsystems</csm:svc>
            <csm:nameAndValue>
               <csm:id>delete</csm:id>
               <csm:value>3</csm:value>
            </csm:nameAndValue>
         </csm:configEntry>
      </csm:configSetRequest>
</soapenv:Body>
```

Пример команды:

```
/opt/tccs/bin/subsys_control.py --delete 3
```

Перечисление подсистем

В качестве имени параметра в SOAP-запросе указывается list. Перечисление подсистем не требует параметров. Ответ — список уникальных идентификаторов и имен подсистем.

Пример SOAP-запроса:

```
<soapenv:Body>
      <csm:configGetRequest>
         <csm:configEntry>
            <csm:hostId>1</csm:hostId>
            <csm:svc>Subsystems</csm:svc>
            <csm:nameAndValue>
               <csm:id>list</csm:id>
            </csm:nameAndValue>
         </csm:configEntry>
      </csm:configGetRequest>
</soapenv:Body>
```

Пример команды:

```
/opt/tccs/bin/subsys_control.py --list
```

Управление ключами

В API доступны доставка, удаление, привязка ключевых контейнеров к ИТ-системам (подсистемам), их отключение от ИТ-систем и вывод информации о контейнерах, привязанных к ИТ-системам. Управление ключами производится с помощью SOAP-запросов на получение и изменение конфигурации или с помощью командной оболочки ОС. В случае управления с помощью SOAP-запросов hostId должно иметь значение идентификатора хоста CAS–1, а имя сервиса (svc) иметь значение keyContainer. Модуль, реализующий управление ключами посредством командной оболочки ОС, — /opt/tccs/bin/key_control.py.

Существуют три предопределенные подсистемы:

Идентификатор	Описание
0	Ключевые контейнеры, прошедшие регистрацию в Jinn-Server
1	Ключевые контейнеры, доступные для CSP
2	Ключевые контейнеры, доступные при всех операциях усиления и формирования ЭП

Установка ключей

В качестве имени параметра в SOAP-запросе указывается register. Параметром при использовании SOAP-запроса является base64 от tar-архива, содержащего директорию с ключевыми контейнерами. При использовании командной строки — путь к директории, содержащей ключевые контейнеры. Если имя контейнера не уникально, но заголовок уникален, то в процессе установки имя контейнера будет изменено. Ответ — уникальные идентификаторы ключевых контейнеров и их имена.

Пример SOAP-запроса:

```
<soapenv:Body>
      <csm:configSetRequest>
       <csm:configEntry>
            <csm:hostId>1</csm:hostId>
            <csm:svc>keyContainer</csm:svc>
            <csm:nameAndValue>
                <csm:id>register</csm:id>
                <csm:value>данные в base64</csm:value>
            </csm:nameAndValue>
         </csm:configEntry>
      </csm:configSetRequest>
</soapenv:Body>
```

Пример команды:

```
/opt/tccs/bin/key_control.py --register /tmp/key_containers
```

Удаление (запрет использования) ключей

В качестве имени параметра в SOAP-запросе указывается unregister. Параметром является один или несколько уникальных идентификаторов ключевых контейнеров. Ответ — статус операции.

Пример SOAP-запроса:

```
<soapenv:Body>
      <csm:configSetRequest>
       <csm:configEntry>
            <csm:hostId>1</csm:hostId>
            <csm:svc>keyContainer</csm:svc>
            <csm:nameAndValue>
               <csm:id>unregister</csm:id>
               <csm:value>3</csm:value>
            </csm:nameAndValue>
         </csm:configEntry>
      </csm:configSetRequest>
</soapenv:Body>
```

Пример команды:

```
/opt/tccs/bin/key_control.py --unregister 3
```

Привязка ключей к подсистемам

В качестве имени параметра в SOAP-запросе указывается add_to_subsystem. Параметром является набор пар уникальных идентификаторов ключевых контейнеров и подсистем соответственно. Ответ — статус операции.

Пример SOAP-запроса:

```
<soapenv:Body>
      <csm:configSetRequest>
       <csm:configEntry>
            <csm:hostId>1</csm:hostId>
            <csm:svc>keyContainer</csm:svc>
            <csm:nameAndValue>
               <csm:id>add_to_subsystem</csm:id>
               <csm:value>4 2</csm:value>
            </csm:nameAndValue>
         </csm:configEntry>
      </csm:configSetRequest>
</soapenv:Body>
```

Пример команды:

```
/opt/tccs/bin/key_control.py --add_to_subsystem 4 2
```

Отключение ключей от подсистем

В качестве имени параметра в SOAP-запросе указывается remove_from_subsystem. Параметром является набор пар уникальных идентификаторов ключевых контейнеров и подсистем соответственно. Ответ — статус операции.

Пример SOAP-запроса:

```
<soapenv:Body>
      <csm:configSetRequest>
       <csm:configEntry>
            <csm:hostId>1</csm:hostId>
            <csm:svc>keyContainer</csm:svc>
            <csm:nameAndValue>
```

```
                <csm:id>remove_from_subsystem</csm:id>
                <csm:value>4 2</csm:value>
            </csm:nameAndValue>
         </csm:configEntry>
      </csm:configSetRequest>
</soapenv:Body>
```

Пример команды:

```
/opt/tccs/bin/key_control.py --remove_from_subsystem 4 2
```

Вывод информации о контейнерах, привязанных к подсистемам

В качестве имени параметра в SOAP-запросе указывается list. Параметром является уникальный идентификатор подсистемы. Ответ — список ключевых контейнеров, связанных с данной подсистемой.

Пример SOAP-запроса:

```
<soapenv:Body>
      <csm:configSetRequest>
       <csm:configEntry>
            <csm:hostId>1</csm:hostId>
            <csm:svc>keyContainer</csm:svc>
            <csm:nameAndValue>
                <csm:id>list</csm:id>
                <csm:value>0</csm:value>
            </csm:nameAndValue>
         </csm:configEntry>
      </csm:configSetRequest>
   </soapenv:Body>
```

Пример команды:

```
/opt/tccs/bin/key_control.py --list 0
```

Домены доверия

Управление доменами

В API доступны регистрация, удаление и получение списка доменов доверия.

Структура запроса на регистрацию домена доверия:

```
<trustDomainCreateRequest>TD-1</trustDomainCreateRequest>
```

Структура запроса на удаление домена доверия:

```
<trustDomainDeleteRequest>1</trustDomainDeleteRequest>
```

Структура запроса на получение списка доменов доверия:

```
<trustDomainListRequest/>
```

Управление издателями

В API доступны включение издателей в домен доверия, их исключение, вывод информации об идентификаторах издателей, включенных в определенный домен доверия, и вывод информации об определенном издателе.

Идентификатор домена доверия со значением "0" зарезервирован для списка издателей в TSL и может быть использован для их перечисления и регистрации.

Идентификатор домена доверия со значением "1" зарезервирован для списка всех зарегистрированных издателей и может быть использован для их перечисления и при включении в созданные домены доверия.

Структура запроса на включение издателей в домен доверия:

```
<trustDomainIssuersAddRequest>
      <srcDomainId>0</srcDomainId>
      <assignments>
   <listEntry><id>1</id>      <value>1</value></listEntry>
   <listEntry><id>2</id>      <value>1</value></listEntry>
      </assignments>
</trustDomainIssuersAddRequest>
```

Структура запроса на исключение издателей из домена доверия:

```
<trustDomainIssuersRemoveRequest>
      <listEntry> <id>2</id> <value>1</value> </listEntry>
</trustDomainIssuersRemoveRequest>
```

Структура запроса на вывод информации об идентификаторах издателей, включенных в домен доверия с указанным идентификатором:

```
<trustDomainIssuersListRequest>1</trustDomainIssuersListRequest>
```

Структура запроса на вывод информации об указанном издателе:

```
<issuerInfoRequest>
   <domainId>1</domainId>
   <issuerId>1333</issuerId>
</issuerInfoRequest>
```

Язык описания веб-сервисов и доступа к ним

Язык описания веб-сервисов и доступа к ним реализован на WSDL (Web Services Description Language).

Описание веб-сервиса (SVS, SS) в документе WSDL можно разделить на следующие логические части:

- определение типов данных (types) — определение вида отправляемых и получаемых веб-сервисом XML-сообщений;
- элементы данных (message) — сообщения, используемые веб-сервисом;
- операции (portType) — список операций, которые могут быть выполнены с сообщениями;
- связывание сервисов (binding) — способ, которым сообщение будет доставлено.

Документ WSDL может также содержать логическую часть service, которая позволяет объединить в одном отдельном документе WSDL описания нескольких веб-сервисов.

Описание веб-сервисов представлено в Приложении 1, а описание типов — в Приложении 2.

Описание структур входных и выходных данных веб-сервисов

Сервис SigningService

Сервис SS обрабатывает входящие запросы на формирование ЭП (операция Sign) и расчет хэша от произвольных данных (операция Digest).

Примечание. Алгоритм подписи или хэширования (в зависимости от запроса к сервису SS) указывается в виде OID-значения в необязательном поле algorithmId запроса.

В случае отсутствия данного необязательного поля в запросе сервис выполняет запрошенную операцию в соответствии с параметрами preferredSignatureAlgorithm (алгоритм подписи) и preferredDigestAlgorithm (алгоритм хэширования) своего конфигурационного файла (параметры конфигурационных файлов сервисов Jinn-Server приведены в [**1**]).

Значения алгоритмов (выделены рекомендованные значения):

	2001 / 94	2012-256	2012-512
Подпись ГОСТ Р 34.10–…	1.2.643.2.2.19	**1.2.643.7.1.1.1.1**	1.2.643.7.1.1.1.2
Хэш ГОСТ Р 34.11–…	1.2.643.2.2.9	**1.2.643.7.1.1.2.2**	1.2.643.7.1.1.2.3
Подпись + хэш ГОСТ Р 34.10–… + 34.11– …	1.2.643.2.2.3	**1.2.643.7.1.1.3.2**	1.2.643.7.1.1.3.3

При обработке запросов на проверку с усилением (операция Validate сервиса SVS) до уровня, требующего формирования штампа времени, значение поля algorithmId определяет алгоритм для подписания штампа времени.

Операция Digest

Структура запроса к сервису SS на выполнение операции Digest:

```
xs:complexType name="DigestRequestType">
<xs:sequence>
<xs:element minOccurs="0" name="dataBytes"
type="cst:notEmptyB64Binary" />
<xs:element minOccurs="0" name="paramOID"
type="cst:OBJECT_IDENTIFIER" />
<xs:element minOccurs="0" name="algorithmId"
type="cst:OBJECT_IDENTIFIER" />
<xs:element minOccurs="0" name="state"
type="cst:notEmptyB64Binary" />
</xs:sequence>
</xs:complexType>
```

Параметры запроса:

- **dataBytes** — поле, содержащее Base64-кодированные данные для процедуры хэширования (хэш вычисляется от исходных бинарных данных, т. е. предварительно выполняется обратное Base64-декодирование данных);
- **paramoid** — необязательное поле, содержащее идентификатор параметров алгоритма хэширования. Имеет смысл только для старого алгоритма хэширования (ГОСТ Р 34.11-94), а для других алгоритмов игнорируется. Допустимые значения (TestParamSet, CryptoProParamSet соответственно):

  ```
  { "1.2.643.2.2.30.0", "1.2.643.2.2.30.1" }
  ```

- **algorithmId** — необязательное поле, определяющее алгоритм хэширования. В случае если параметр опущен, будет использоваться алгоритм, указанный в настройках конфигурационного файла сервиса SS. Допустимые значения (ГОСТ Р 34.11–94, ГОСТ Р 34.11–2012–256, ГОСТ Р 34.11–2012–512 соответственно):

  ```
  { "1.2.643.2.2.9", "1.2.643.7.1.1.2.2", "1.2.643.7.1.1.2.3" }
  ```

- **state** — необязательное поле, содержащее состояние контекста хэширования в виде Base64-кодированных данных, необходимое для "потокового" сценария взаимодействия.

Примечание. Сценарий взаимодействия:

- "традиционный" (запрос — ответ) — применим для относительно небольших блоков данных, для которых возможна единовременная передача по сети и обработка в оперативной памяти. Запрос не должен содержать поле state;
- "потоковый" — применим для большого объема данных, для которых невозможна единовременная передача по сети и обработка в оперативной памяти. Данный сценарий представляет собой последовательность запросов и ответов, где первый запрос не содержит поле state, а для всех последующих запросов значение поля state заполняется на основании значения поля state из предыдущего ответа.

Структура ответа:

```
<xs:complexType name="DigestResponseType">
<xs:sequence>
<xs:element minOccurs="0" name="digest"
type="cst:notEmptyB64Binary" />
<xs:element minOccurs="0" name="state"
type="cst:notEmptyB64Binary" />
</xs:sequence>
</xs:complexType>
```

В случае успешного выполнения операции элемент **digest** будет содержать Base64-кодированное значение вычисленного хэша, а элемент **state** — состояние контекста хэширования, необходимое для продолжения вычислений при "потоковом" сценарии взаимодействия.

Операция Sign

Структура запроса к сервису SS на выполнение операции Sign:

```
<xs:complexType name="SigningRequestType">
<xs:sequence>
<xs:element name="data" type="cst:notEmptyB64Binary" />
<xs:element minOccurs="0" default="cades-bes"
name="signatureType" type="cst:signatureType" />
<xs:element minOccurs="0" default="false" name="detached"
type="xs:boolean" />
<xs:element minOccurs="0" name="xmlPartID" type="xs:string" />
<xs:element minOccurs="0" name="actor" type="xs:string" />
<xs:element minOccurs="0" name="algorithmId"
type="cst:OBJECT_IDENTIFIER" />
                    <xs:element minOccurs="0"
name="transforms" type="cst:notEmptyB64Binary" />
                    <xs:element minOccurs="0"
name="businessProcessId" type="xs:string" />
</xs:sequence>
</xs:complexType>
```

Параметры запроса:

- **data** — поле, содержащее Base64-кодированные данные, которые необходимо подписать;
- **signatureType** — поле, определяющее формат подписи:
  - cms — подпись в формате CMS;
  - xmldsig — подпись в формате XMLDSig;
  - cades-bes (значение по умолчанию), cades-c, cades-t, cades-a — подпись в формате CMS, усиленная в необходимом объеме (дополненная атрибутами) в соответствии с ETSI TS 101 733 (CAdES);
  - xades-bes, xades-c, xades-t, xades-a — подпись в формате XMLDSig, усиленная в необходимом объеме (дополненная атрибутами) в соответствии с ETSI TS 101 903 (XAdES);
  - wssec-bes, wssec-c, wssec-t, wssec-a — подпись в формате WS-Security, усиленная в необходимом объеме (дополненная атрибутами) в соответствии с ETSI TS 101 903 (XAdES);
- **detached** — необязательный boolean-параметр со значением по умолчанию false. В случае указания значения true будет сформирована отсоединенная подпись;
- **xmlPartID** — необязательный параметр, имеющий смысл только при подписании XML-документов. Позволяет подписать не весь документ, а только заданный элемент;

- **actor** — необязательный параметр, имеющий смысл только для подписи в формате WS-Security. Позволяет задать значение атрибута actor, который будет установлен для родительского, по отношению к создаваемой подписи, элемента wsse:Security;
- **algorithmId** — необязательное поле, определяющее алгоритм подписи. В случае если параметр опущен, будет использоваться алгоритм, указанный в настройках конфигурационного файла сервиса SS. Допустимые значения (ГОСТ Р 34.10–94, ГОСТ Р 34.10–2012–256, ГОСТ Р 34.10–2012–512 соответственно):

```
{ "1.2.643.2.2.19", "1.2.643.7.1.1.1.1", "1.2.643.7.1.1.1.2" }
```

- **transforms** — необязательное поле, предназначенное для передачи набора трансформов, которые необходимо применить при формировании подписи в формате XMLDSig и порожденных от него (XAdES, WS-Security) для взаимодействия со СМЭВ;
- **businessProcessId** — необязательное поле, предназначенное для передачи идентификатора подсистемы. При формировании подписи выбор ключевых контейнеров будет ограничен принадлежащими только указанной подсистеме. В случае если параметр опущен, будет использоваться идентификатор подсистемы по умолчанию (defaultSubsystemId), указанный в настройках конфигурационного файла сервиса SS. Для игнорирования значения параметра defaultSubsystemId в запросе передается 0 в качестве идентификатора подсистемы.

Примечание. Если в запросе указан формат подписи, отличный от CMS, то контролируется корректность формата поля data.

При формировании подписи в формате CMS и порожденных от него (CAdES) поле transforms игнорируется.

Структура ответа:

```
<xs:element name="SigningResponseType"
type="cst:notEmptyB64Binary" />
```

В случае успешного выполнения операции данный элемент будет содержать Base64-кодированное значение сформированной подписи.

Рекомендации по взаимодействию со СМЭВ

Для корректного взаимодействия со СМЭВ необходимо отформатировать исходный документ, исключив переводы строк между элементами. После чего сформировать отсоединенную подпись от заданного прикладной спецификацией фрагмента (выделено курсивом):

```
<AckRequest xmlns:ns2="urn://x-artefacts-smev-gov-
ru/services/message-exchange/types/basic/1.1" xmlns="urn://x-
artefacts-smev-gov-ru/services/message-
exchange/types/1.1"><ns2:AckTargetMessage
Id="SIGNED_BY_CALLER" accepted="true">2eee3edb-900d-4443-ba0a-
1b97f1583d36</ns2:AckTargetMessage></AckRequest>
```

Затем включить полученную отсоединенную подпись в исходный документ в соответствии с прикладной спецификацией (в данном случае в составе элемента <CallerInformationSystemSignature>, выделенного курсивом):

```
<AckRequest xmlns:ns2="urn://x-artefacts-smev-gov-
ru/services/message-exchange/types/basic/1.1" xmlns="urn://x-
artefacts-smev-gov-ru/services/message-
exchange/types/1.1"><ns2:AckTargetMessage Id="SIGNED_BY_CALLER"
accepted="true">2eee3edb-900d-4443-ba0a-
1b97f1583d36</ns2:AckTargetMessage><CallerInformationSystemSignat
ure><Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="Id-
sig-
63a3b85f39ea30d5bc5e279caa549a6821ed"><SignedInfo><Canonicalizati
onMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/><SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-
gostr3411"/><Reference URI="#SIGNED_BY_CALLER" Id="Id-dataref-
518353f081f9806284467a022da2ea950879"><Transforms><Transform
```

```
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><Transform
Algorithm="urn://smev-gov-
ru/xmldsig/transform"/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-
more#gostr3411"/><DigestValue>6R7aJGtCJ6Yp1VEWTruJgvjD/R2PPE6zsiJ
f7mNu9RQ=</DigestValue></Reference><Reference
Type="http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd#X509Data" URI="#Id-keyinfo-
77183721ccb6280b78806f70a41fffd59d85" Id="Id-keyinforef-
b27be1b26dd4ccc34ed1c973498f35a36cfc"><Transforms><Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-
more#gostr3411"/><DigestValue>+xGnQbuEh2mfRtZ5fYxb89rFTbPABkRGYDw
u5kDs3h4=</DigestValue></Reference></SignedInfo><SignatureValue>J
tnf6i4cAoa2N/MAMS0VBAQAh8wVNxcYmx99pQq3o7V3peS4kVAXoLc8C/IVDZnm
n65IqMYf8ryi2+DKEgqQ6A==</SignatureValue><KeyInfo Id="Id-keyinfo-
77183721ccb6280b78806f70a41fffd59d85"><X509Data><X509Certificate>
MIIC9DCCAqOgAwIBAgIKTv/27wACAAAUMDAIBgYqhQMCAgMwJzElMCMGA1UEAxMc
Q29udGluZW50IFN0YW5kYWxvbmUgQ0EgUm9vdDAeFw0xNzA1MjIxMDU5NTJaFw0x
OTA1MjIxMTA5NTJaMEMxCzAJBgNVBAYTAlJVMQwwCgYDVQQIEwNNU0sxDDAKBgNV
BAcTA01TSzEYMBYGA1UEAxMPU1ZDIGNlcnQgKDIwMDEpMGMwHAYGKoUDAgITMBIG
ByqFAwICJAAGByqFAwICHgEDQwAEQD4xZv/1cLkji+BoWnPPGO1G0ebFsJgctRau
kZs189vdU/fjQ4jdGyvSVruTGSwnSGaPbhZnO4FxqECObe4+/GejggGRMIIBjTAO
BgNVHQ8BAf8EBAMCBPAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFG4p
2IEE9APkT7tYZps7GcsO/XdJMB8GA1UdIwQYMBaAFEfoXqwDvDJatpxrCuT+1X4W
FVQIMFUGA1UdHwROMEwwSqBIoEaGRGh0dHA6Ly8xNzIuMTcuNy4zOC9DZXJ0RW5y
b2xsL0NvbnRpbmVudCUyMFN0YW5kYWxvbmUlMjBDQSUyMFJvb3QuY3JsMIHOBggr
BgEFBQcBAQSBwTCBvjBfBggrBgEFBQcwAoZTaHR0cDovLzIwMDNyMnNydmNhL0Nl
cnRFbnJvbGwvMjAwM3Iyc3J2Q0FfQ29udGluZW50JTIwU3RhbmRhbG9uZSUyMENB
JTIwUm9vdCgyKS5jcnQwWwYIKwYBBQUHMAKGT2ZpbGU6Ly9cXDIwMDNyMnNydkNB
XENlcnRFbnJvbGxcMjAwM3Iyc3J2Q0FfQ29udGluZW50IFN0YW5kYWxvbmUgQ0Eg
Um9vdCgyKS5jcnQwCAYGKoUDAgIDA0EA93SgGV8Tdm71QaukzPc4BwOmBChVXFfG
A0k7NdeXWpwTKwRatbZfNzcmfnhyHCsipNpELfQKcZypmO3gKJuBMQ==</X509Cer
tificate></X509Data></KeyInfo></Signature></CallerInformationSyst
emSignature></AckRequest>
```

Включаемое в запрос значение поля transforms должно формироваться как Base64-кодированное представление XML-документа, формат и содержание которого соответствуют описанию, приведенному в стандарте XMLDSig.

Переданные таким образом трансформы будут применяться **в дополнение** к тем, что положены по стандарту, т.е. будут добавлены в конец списка, формируемого в процессе подписания XML-документа.

Допускается передавать трансформы следующих типов — XPath, XSLT, SMEV3.

Сразу после пролога необходимо убедиться в наличии тега:

```
<Transforms></Tranforms>
```

Внутри данной структуры добавляется тег:

```
<Transform></Tranform>
```

Для указания алгоритма трансформа необходимо добавить атрибут Algorithm к тегу <Transform>.

Например, есть исходный XML-документ, содержащий список трансформов (в данном случае один — идентификатор трансформа SMEV3):

```
xml-transforms = "<?xml version="1.0" encoding="UTF-8"?>
<Transforms xmlns="http://www.w3.org/2000/09/xmldsig#">
  <Transform Algorithm="urn://smev-gov-ru/xmldsig/transform"/>
</Transforms>"
```

Примечание. Допускается указание только атрибута XML 1.0.

Представление этого документа в Base64:

```
b64-transforms =
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz4KPFRyYW5zZm
9ybXMgeG1sbnM9Imh0dHA6Ly93d3cudzMub3JnLzIwMDAvMDkveG1sZHNpZyMi
PgoJPFRyYW5zZm9ybSBBbGdvcml0aG09InVybjovL3NtZXYtZ292LXJ1L3htbG
RzaWcvdHJhbnNmb3JtIi8+CjwvVHJhbnNmb3Jtcz4K
```

Итоговый запрос на формирование подписи (исходные данные сокращены, в поле transforms установлено значение b64-transforms):

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"

xmlns:sgv="http://www.roskazna.ru/eb/sign/types/sgv"><soapenv:
Header/><soapenv:Body><sgv:SigningRequestType><sgv:data>PD94bW
wgdmVyc2lv……GU+DQo=</sgv:data><sgv:signatureType>wssecurity</s
gv:signatureType>
<sgv:transforms>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLT
giPz4KPFRyYW5zZm9ybXMgeG1sbnM9Imh0dHA6Ly93d3cudzMub3JnLzIwMDAv
MDkveG1sZHNpZyMiPgoJPFRyYW5zZm9ybSBBbGdvcml0aG09InVybjovL3NtZX
YtZ292LXJ1L3htbGRzaWcvdHJhbnNmb3JtIi8+CjwvVHJhbnNmb3Jtcz4K</sg
v:transforms>
</sgv:SigningRequestType></soapenv:Body></soapenv:Envelope>
```

Пример для идентификатора трансформа XSLT:

```
<Transforms xmlns="http://www.w3.org/2000/09/xmldsig#">
  <Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-
19991116">
    ..
  </Transform>
</Transforms>
```

Итоговый запрос на формирование подписи с использованием трансформа XSLT:

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:sgv="http://www.roskazna.ru/eb/sign/types/sgv">
<soapenv:Header/>
<soapenv:Body>
<sgv:SigningRequestType>
<sgv:data>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz4KPGR
vYz4KICA8Y29udGVudCBpZD0iU2VjdXJpdHlDb2RlIj4KCQk8ZmllbGQgc2lnbj0i
MSIgb3JkZXI9IjAiIGxhYmVsPSJbVGl0bGUgaWQ9JzEnIG51bWJlcj0nMScgcGFyZ
W50SWQ9JzAnIG5hbWU9J9Cf0LvQsNGC0LXQttC60LAgNjAxMCddICDQn9C70LDRgt
C10LbQvdC+0LUg0L/QvtGA0YPRh9C10L3QuNC1IOKEliIgdmFsdWU9IjYwMTAiLz4
KCQk8ZmllbGQgc2lnbj0iMSIgb3JkZXI9IjEiIGxhYmVsPSLQlNCw0YLQsCIgdmFs
dWU9IjAxLjA4LjIwMTIiLz4KCQk8ZmllbGQgc2lnbj0iMSIgb3JkZXI9IjIiIGxhY
mVsPSLQktC40LQg0L/Qu9Cw0YLQtdC20LAiIHZhbHVlPSLQrdC70LXQutGC0YDQvt
C90L3QviIvPgoJCTxmaWVsZCBzaWduPSIxIiBvcmRlcj0iMyIgbGFiZWw9ItCh0YP
QvNC80LAg0L/RgNC+0L/QuNGB0YzRjiAiIHZhbHVlPSLQktC+0YHQtdC80Ywg0LzQ
uNC70LvQuNC+0L3QvtCyINGH0LXRgtGL0YDQtdGB0YCDRgdC10LzRjNC00LXRg
dGP0YIg0LTQtdCy0Y/RgtGMINGC0YvRgdGP0Ycg0YjQtdGB0YLRjNGB0L7RgiDQst
C+0YHQtdC80YzQtNC10YHRj9GCINGA0PQsdC70LXQuSAwMCDQutC+0L/QtdC10Lo
gIi8+CgkPGZpZWxkIHNpZ249IjEiIG9yZGVyPSI0IiBsYWJlbD0iW1RpdGxlIGlk
PScyJyBudW1iZXI9JzEnIHBhcmVudElkPScxJyBuYW1lPSfQoNC10LrQstC40LfQu
NGC0YsnXSDQmNCd0J0gMzM0NDU1NzcyMzQ1ICIvPgoJCTxmaWVsZCBzaWduPSIxIi
BvcmRlcj0iNSIgbGFiZWw9ItCa0J/QnyA5OTg4Nzc0NTYgIi8+CgkPGZpZWxkIHN
pZ249IjEiIG9yZGVyPSI2IiBsYWJlbD0i0KHRg9C80LzQsCAiIHZhbHVlPSI4NDc5
NjgwIi8+CgkPGZpZWxkIHNpZ249IjEiIG9yZGVyPSI3IiBsYWJlbD0i0KHRhy4g4
oSWICIgdmFsdWU9IjM0NjM0NzgzNDcyMjM0NzgyIi8+CgkPGZpZWxkIHNpZ249Ij
EiIG9yZGVyPSI4IiBsYWJlbD0i0J7QkNCeINCQ0LvRjNGE0LDQsdCw0L3QuiDQsy7
```

```
QnNC+0YHQutCy0LAiLz4KCQk8ZmllbGQgc2lnbj0iMSIgb3JkZXI9IjkiIGxhYmVs
PSLQkdCY0JogIiB2YWx1ZT0iMDQ0NTI1NTkzICIvPgoJCTxmaWVsZCBzaWduPSIxI
iBvcmRlcj0iMTAiIGxhYmVsPSJbVGl0bGUgaWQ9JzMnIG51bWJlcj0nMScgcGFyZW
50SWQ9JzInIG5hbWU9J9Cg0LXQutCy0LjQt9C40YLRiyddINCh0YfQtdGCIOKEliA
iIHZhbHVlPSIzMDEwMTgxMDIwMDAwMDAwMDU5ICIvPgoJCTxmaWVsZCBzaWduPSIx
IiBvcmRlcj0iMTEiIGxhYmVsPSLQntCQ0J4g0J3QkdCRINCzLtCc0L7RgdC60LLQs
CIvPgoJCTxmaWVsZCBzaWduPSIxIiBvcmRlcj0iMTIiIGxhYmVsPSLQkdCY0JogIi
B2YWx1ZT0iMDQ0NTUyOTAyICIvPgoJCTxmaWVsZCBzaWduPSIxIiBvcmRlcj0iMTM
iIGxhYmVsPSLQodGH0LXRgiDihJYgIiB2YWx1ZT0iNDAyMjE4MTAyMDAwMDAwMTQy
MyAiLz4KCQk8ZmllbGQgc2lnbj0iMSIgb3JkZXI9IjE0IiBsYWJlbD0i0JjQndCdI
Dc3MTU3MTkyNDQiLz4KCQk8ZmllbGQgc2lnbj0iMSIgb3JkZXI9IjE1IiBsYWJlbD
0i0JrQn9CfIDc3MTUwMTAwMSIvPgoJCTxmaWVsZCBzaWduPSIxIiBvcmRlcj0iMTY
iIGxhYmVsPSLQodGH0LXRgiDihJYiIHZhbHVlPSI0MDcwMjgxMDAwMDAwMTU0MjEw
MCIvPgoJCTxmaWVsZCBzaWduPSIxIiBvcmRlcj0iMTciIGxhYmVsPSJbVGl0bGUga
WQ9JzQnIG51bWJlcj0nMicgcGFyZW50SWQ9JzEnIG5hbWU9J9Cf0LDRgNCw0LzQtd
GC0YDRiyDQvtC/0LvQsNGC0YsnXSDQktC40LQg0L7Qvy4iIHZhbHVlPSIwMSIvPgo
JCTxmaWVsZCBzaWduPSIxIiBvcmRlcj0iMTgiIGxhYmVsPSLQodGA0L7QuiDQvtC/
0LvQsNGC0YsiIHZhbHVlPSIgIi8+CgkJPGZpZWxkIHNpZ249IjEiIG9yZGVyPSIxO
SIgbGFiZWw9ItCd0LDQty4g0L/Quy4iIHZhbHVlPSIgIi8+CgkJPGZpZWxkIHNpZ2
49IjEiIG9yZGVyPSIyMCIgbGFiZWw9ItCe0YfQtdGALiDQvtC/0LvQsNGC0YsiIHZ
hbHVlPSI2Ii8+CgkJPGZpZWxkIHNpZ249IjEiIG9yZGVyPSIyMSIgbGFiZWw9IltU
aXRsZSBpZD0nNScgbnVtYmVyPScyJyBwYXJlbnRJZD0nNCcgbmFtZT0n0JonXdCa0
L7QtCIgdmFsdWU9IiAiLz4KCQk8ZmllbGQgc2lnbj0iMSIgb3JkZXI9IjIyIiBsYW
JlbD0iW1RpdGxlIGlkPSc2JyBudW1iZXI9JzInIHBhcmVudElkPSc0JyBuYW1lPSf
QoCdd0KDQtdC3LiDQv9C+0LvQtSIgdmFsdWU9IiAiLz4KCTwvY29udGVudD4KPC9k
b2M+</sgv:data>
         <!--Optional:-->
         <sgv:signatureType>xades-bes</sgv:signatureType>
         <!--Optional:-->
<sgv:transforms>PD94bWwgdmVyc2lvbj0nMS4wJz8+CjxUcmFuc2Zvcm1zIHhtb
G5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjIj4KCTxUcmFuc2
Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy9UUi8xOTk5L1JFQy14c2x
0LTE5OTkxMTE2Ij4KPHhzbDpzdHlsZXNoZWV0IHZlcnNpb249IjEuMCIgeG1sbnM6
eHNsPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L1hTTC9UcmFuc2Zvcm0iIHhtbG5zO
m1zeHNsPSJ1cm46c2NoZW1hcy1taWNyb3NvZnQtY29tOnhzbHQiPgo8eHNsOm91dH
B1dCBtZXRob2Q9Imh0bWwiLz4KPHhzbDp0ZW1wbGF0ZSBuYW1lPSJ0b1BsYWluIiB
tYXRjaD0iZmllbGQiPgo8eHNsOnZhbHVlLW9mIHNlbGVjdD0iQGxhYmVsIi8+PHhz
bDp0ZXh0PiA6IDwveHNsOnRleHQ+PCEtLSDRgNC10LfQtNC10LvQuNGC0LXQu9GMI
NC80LXQttC00YMgbGFiZWwg0LggdmFsdWUgLS0+PHhzbDp2YWx1ZS1vZiBzZWxlY3
Q9IkB2YWx1ZSIvPjx4c2w6dGV4dD4mI3hEOyYjeEE7PC94c2w6dGV4dD4KPCEtLSA
KIC0tPjwveHNsOnRlbXBsYXRlPjx4c2w6dGVtcGxhdGUgbmFtZT0iU3RhcnQiIG1h
dGNoPSIvIj4KPCEtLSDQutC+0YDQvdC10LLQvtC5INGC0LXQsyDQtNC70Y8g0YDQt
dC30YPQu9GM0YLQuNGA0YPRjtGJ0LXQs9C+INC00L7QutGD0LzQtdC90YLQsCAtLT
4KPHhzbDpmb3ItZWFjaCBzZWxlY3Q9ImRvYy9jb250ZW50L2ZpZWxkW0BzaWduPSc
xJ10iPgo8eHNsOnNvcnQgc2VsZWN0PSJAb3JkZXIiIG9yZGVyPSJhc2NlbmRpbmci
IGRhdGEtdHlwZT0ibnVtYmVyIi8+Cjx4c2w6Y2FsbC10ZW1wbGF0ZSBuYW1lPSJ0b
1BsYWluIi8+CjwveHNsOmZvci1lYWNoPjwveHNsOnRlbXBsYXRlPjwveHNsOnN0eW
xlc2hlZXQ+CjwhLS0gU3R5bHVzIFN0dWRpbyBtZXRhLWluZm9ybWF0aW9uIC0gKGM
pIDIwMDQtMjAwNS4gUHJvZ3Jlc3MgU29mdHdhcmUgQ29ycG9yYXRpb24uIEFsbCBy
aWdodHMgcmVzZXJ2ZWQuPG1ldGFJbmZvcm1hdGlvbj48c2NlbmFyaW9zID48c2Nlb
mFyaW8gZGVmYXVsdD0ieWVzIiBuYW1lPSJTY2VuYXJpbzEiIHVzZXJlbGF0aXZlcG
F0aHM9InllcyIgZXh0ZXJuYWxwcmV2aWV3PSJubyIgdXJsPSIuLi4uLi4uLi4uLi5
Qcm9qZWN0c1RlbXBKaW5uc3JjLnhtbCIgaHRtbGJhc2V1cmw9IiIgb3V0cHV0dXJs
PSIiIHByb2Nlc3NvcnR5cGU9ImludGVybmFsIiBwcm9maWxlbW9kZT0iMCIgcHJvZ
mlsZWRlcHRoPSIiIHByb2ZpbGVsZW5ndGg9IiIgdXJscHJvZmlsZXhtbD0iIiBjb2
1tYW5kbGluZT0iIiBhZGRpdGlvbmFscGF0aD0iIiBhZGRpdGlvbmFsY2xhc3NwYXR
oPSIiIHBvc3Rwcm9jZXNzb3J0eXBlPSJub25lIiBwb3N0cHJvY2Vzc2NvbW1hbmRs
aW5lPSIiIHBvc3Rwcm9jZXNzYWRkaXRpb25hbHBhdGg9IiIgcG9zdHByb2Nlc3NnZ
W5lcmF0ZWRleHQ9IiIvPjwvc2NlbmFyaW9zPjxNYXBwZXJNZXRhVGFnPjxNYXBwZX
JJbmZvIHNyY1NjaGVtYVBhdGhJc1JlbGF0aXZlPSJ5ZXMiIHNyY1NjaGVtYUludGV
ycHJldEFzWE1MPSJubyIgZGVzdFNjaGVtYVBhdGg9IiIgZGVzdFNjaGVtYVJvb3Q9
IiIgZGVzdFNjaGVtYVBhdGhJc1JlbGF0aXZlPSJ5ZXMiIGRlc3RTY2hlbWFJbnRlc
nByZXRBc1hNTD0ibm8iLz48TWFwcGVyQmxvY2tQb3NpdGlvbj48L01hcHBlckJsb2
```

```
NrUG9zaXRpb24+PC9NYXBwZXJNZXRhVGFnPjwvbWV0YUluZm9ybWF0aW9uPi0tPgo
JPC9UcmFuc2Zvcm0+CjwvVHJhbnNmb3JtcT4=</sgv:transforms>
      </sgv:SigningRequestType>
   </soapenv:Body>
</soapenv:Envelope>
```

Пример для идентификатора трансформа XPATH:

```
<Transforms xmlns="http://www.w3.org/2000/09/xmldsig#">
  <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-
19991116">
    <XPath xmlns:ietf="http://www.ietf.org">@*</XPath>
  </Transform>
</Transforms>
```

Сервис SignatureValidationService

Сервис SVS обрабатывает входящие запросы на проверку ЭП, проверку и усиление ЭП (операция Validate), проверку структуры сертификата (операция CertificateFormatValidate) и проверку действительности сертификата (операция CertificateValidation).

Операция Validate

Структура запроса к сервису SVS на выполнение операции Validate:

```
<xs:complexType name="ValidationRequestType">
<xs:sequence>
<xs:element name="signedData" type="cst:notEmptyB64Binary" />
<xs:element minOccurs="0" name="externalData"
type="cst:notEmptyB64Binary" />
<xs:element minOccurs="0" default="false"
name="createAdvanced" type="tccs:svsCreateAdvanced" />
<xs:element minOccurs="0" name="xmlPartID" type="xs:string" />
<xs:element minOccurs="0" name="actor" type="xs:string" />
<xs:element minOccurs="0" default="false"
name="ignoreSignatureTimeStamp" type="xs:boolean" />
<xs:element minOccurs="0" name="algorithmId"
type="cst:OBJECT_IDENTIFIER" />
</xs:sequence>
</xs:complexType>
<xs:simpleType name="svsCreateAdvanced">
<xs:restriction base="xs:string">
<xs:enumeration value="0" />
<xs:enumeration value="1" />
<xs:enumeration value="false" />
<xs:enumeration value="true" />
<xs:enumeration value="cades-t" />
<xs:enumeration value="xades-t" />
<xs:enumeration value="wssec-t" />
<xs:enumeration value="cades-c" />
<xs:enumeration value="xades-c" />
<xs:enumeration value="wssec-c" />
<xs:enumeration value="cades-a" />
<xs:enumeration value="xades-a" />
<xs:enumeration value="wssec-a" />
</xs:restriction>
```

```
</xs:simpleType>
```

Параметры запроса:

- **signedData** — поле, содержащее Base64-кодированное значение подписи, которую необходимо проверить. Позволяет единообразно передавать на проверку подписи любых поддерживаемых форматов, при этом конкретный формат определяется автоматически при декодировании;
- **externalData** — необязательный параметр, необходимый для проверки отсоединенной подписи и содержащий Base64-кодированное значение исходных данных, соответствующих отсоединенной подписи, переданной в параметре signedData;
- **createAdvanced** — необязательный строковый параметр со значением по умолчанию false. При указании значения true — в случае успешной проверки переданных данных будет сформирована усиленная подпись в формате cades-c, xades-c или wssec-c (соответственно изначальному формату данных). Параметр поддерживает указание конкретного формата усиления ЭП и содержит следующие значения для усиленных типов подписи — cades-t, cades-c, cades-a, xades-t, xades-c, xades-a, wssec-t, wssec-c, wssec-a;
- **xmlPartID** — необязательный параметр, необходимый для проверки подписи заданного элемента XML-документа;
- **actor** — необязательный параметр, необходимый для проверки подписи, содержащейся внутри элемента wsse::Security с атрибутом actor, имеющим заданное значение;
- **algorithmId** — необязательное поле, определяющее алгоритм для формирования усиленной подписи, в том числе подписания штампа времени. В случае если параметр опущен, будет использоваться алгоритм, указанный в настройках конфигурационного файла сервиса SVS. Допустимые значения (ГОСТ Р 34.10–94 + ГОСТ Р 34.11–94, ГОСТ Р 34.10–2012–256 + ГОСТ Р 34.11–2012–256, ГОСТ Р 34.10–2012–512 + ГОСТ Р 34.11–2012–512 соответственно):

  ```
  { "1.2.643.2.2.3", "1.2.643.7.1.1.3.2", "1.2.643.7.1.1.3.3" }
  ```

  В запросах на проверку ЭП без усиления значение параметра игнорируется.

В случае успешного завершения операция возвращает ответ следующего вида:

```
<xs:complexType name="ValidationRes">
<xs:sequence>
<xs:element name="gmtDateTime" type="cst:GmtDateTime" />
<xs:element name="globalStatus" type="cst:GlobalStatus" />
<xs:element minOccurs="0" name="SignatureInfos"
type="cst:SignatureInfos" />
<xs:element minOccurs="0" name="advanced"
type="cst:notEmptyB64Binary" />
</xs:sequence>
</xs:complexType>
```

Параметры ответа:

- **gmtDateTime** — время проверки по GMT;
- **globalStatus** — итоговый результат проверки (определяется по совокупности результатов проверки всех подписей, содержавшихся в переданных на проверку данных):
  - unknown — недостаточно информации для определения статуса ни одной из имеющихся подписей, что возможно в случае, если не найдены сертификаты авторов или для них недоступны полные и актуальные СОС;
  - invalid — все подписи недействительны;
  - partiallyValid — часть подписей действительна, часть — нет;
  - valid — все подписи проверены успешно;
- **SignatureInfos** — необязательный список с подробной информацией о результатах проверки каждой из имеющихся в проверяемых данных подписи.

Список может отсутствовать или быть пустым, если, например, на проверку были переданы данные в формате CMS SignedData, не содержащие ни одного элемента SignerInfo. Элементы в данном списке будут перечислены в порядке нахождения подписей в проверяемых данных. Если проверяемые данные содержали вложенные подписи, результаты проверки будут перечислены в порядке от внешнего уровня к вложенным:

```
<xs:complexType name="SignatureInfo">
<xs:sequence>
   <xs:element name="reference" type="cst:SignatureRef" />
   <xs:element name="status" type="cst:SignatureStatus" />
<xs:element name="failInfo"
   type="cst:ValidationFaultInfo" minOccurs="0" />
   <xs:element name="signerCertInfo"
         type="cst:SignerCertInfo" minOccurs="0" />
</xs:sequence>
</xs:complexType>
```

- **reference** — справочное поле;
- **status** — результат проверки:
  - unknown — недостаточно информации для определения статуса подписи, что возможно в случае, если не найден сертификат автора или для него недоступны полные и актуальные СОС;
  - invalid — подпись недействительна;
  - valid — подпись проверена успешно;
- **validationFaultInfo** — необязательное поле, раскрывающее причину отрицательного результата проверки. Содержит тип причины:

```
"unknownDigestAlgorithm"
"unknownSignatureAlgorithm"
"signerCertificateNotFound"
"signerCertificateIssuerNotFound"
"signerCertificateSignatureInvalid"
"signerCertificateCRLNotFound"
"signerCertificateExpired"
"signerCertificateRevoked"
"invalidDigestValue"
"invalidSignatureValue"
"invalidSignatureTimeStamp"
"invalidRequestDataFormat"
```

- **signerCertInfo** — необязательное поле, содержащее сертификат автора, в случае если он найден;
- **advanced** — необязательное поле, содержащее Base64-кодированное значение усиленной подписи. Присутствует в ответе только в случае, если было запрошено усиление подписи и поле globalStatus содержит значение valid.

Операция CertificateFormatValidate

Проверка структуры сертификата осуществляется в следующем порядке:

- проверка декодирования сертификата;
- проверка на наличие неизвестных путей/неверных значений (ANY_BROKEN);
- проверка на удовлетворение правилам для разных типов собственников на основе приказа ФСБ России №795 от 27 декабря 2011 г.

Структура запроса к сервису SVS на выполнение операции CertificateFormatValidate (CFV):

```
<xs:complexType name="CFVRequestType">
<xs:sequence>
<xs:element name="certificate" type="cst:notEmptyB64Binary" />
<xs:element name="subjectType" type="tccs:cfvSubjectType"
minOccurs="0" />
</xs:sequence>
</xs:complexType>
```

Параметры запроса:

- **certificate** — поле, содержащее Base64-кодированное значение сертификата, который необходимо проверить;
- **SubjectType** — параметр, определяющий тип субъекта в сертификате (неизвестен — 0 (по умолчанию), физическое лицо — 1, организация — 2).

Формат ответа — XML-отчет CFVReport, в случае ошибок состоящий из записей CFVNotice (0 — ошибки кодирования, 1 — несоответствие требованиям приказа №795):

```
<xs:complexType name="CFVReport">
            <xs:sequence>
                  <xs:element
name="CFVNotice"
type="tccs:CFVNotice"
minOccurs="0"/>
            </xs:sequence>
</xs:complexType>

      <xs:complexType name="CFVNotice">
      <xs:sequence>
      <xs:element name="level">
                  <xs:simpleType>
                        <xs:restriction base="xs:integer">
                              <xs:enumeration value="0" />
                              <xs:enumeration value="1" />
                        </xs:restriction>
                  </xs:simpleType>
            </xs:element>
            <xs:element name="offset" type="xs:integer" />
            <xs:element name="failPath" type="xs:string" />
            <xs:element name="comment" type="xs:string" />
      </xs:sequence>
      </xs:complexType>
```

В каждой записи CFVNotice содержатся следующие данные:

- **level** — уровень критичности (0 — предупреждение, 1 — критичная ошибка);
- **offset** — сдвиг в байтах от начала сертификата до ошибочного пути;
- **failPath** — ошибочный путь;
- **comment** — описание ошибки.

Операция CertificateValidation

Проверка действительности сертификата осуществляется по следующим пунктам:

- актуальность сертификата на текущую дату;
- актуальность сертификата на выбранную дату;
- проверка структуры сертификата.

Структура запроса к сервису SVS на выполнение операции CertificateValidation (CV):

```
<xs:complexType name="CVRequestType">
<xs:sequence>
<xs:element name="certificate" type="cst:notEmptyB64Binary" />
<xs:element name="params" type="tccs:CVParameters"
minOccurs="0" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="CVParameters">
<xs:sequence>
<xs:element name="validationDate" type="xs:integer"
minOccurs="0" />
<xs:element name="subjectType" type="tccs:cfvSubjectType"
minOccurs="0" />
</xs:sequence>
</xs:complexType>
```

Параметры запроса:

- **certificate** — поле, содержащее Base64-кодированное значение сертификата, который необходимо проверить;
- **validationDate** — необязательный параметр, содержащий дату в числовом формате unixtime, на которую выполняется проверка сертификата. Если дата не указана, проверка выполняется на текущую дату;
- **subjectType** — необязательный параметр, определяющий тип субъекта в сертификате (неизвестен — 0 (по умолчанию), физическое лицо — 1, организация — 2). Если параметр указан, в ответ будет добавлено поле attributes, содержащее дополнительную информацию в формате CFVReport.

Формат ответа:

```
<xs:complexType name="CVResponse">
<xs:sequence>
<xs:element name="certId" type="cst:ESSCertIdV2" />
<xs:element name="date" type="xs:integer"/>
<xs:element name="params" type="tccs:CVParameters"
minOccurs="0" />
<xs:element name="status" type="cst:SignatureStatus" />
<xs:element name="failInfo" type="cst:ValidationFaultInfo"
minOccurs="0" />
<xs:element name="attributes" type="tccs:CVAttributes"
minOccurs="0" />
</xs:sequence>
</xs:complexType>
```

Параметры ответа:

- **certId** — информация по проверяемому сертификату;
- **date** — время выполнения проверки в числовом формате unixtime;
- **params** — значение validationDate из запроса;
- **status** — результат проверки (valid — сертификат действителен, invalid — сертификат недействителен);
- **failInfo** — дополнительный параметр, который выводится в ответ для недействительного сертификата (status — invalid). Параметр содержит поле type — тип ошибки и поле comment — описание ошибки;
- **attributes** — дополнительный параметр, который выводится в ответ при наличии в запросе поля subjectType. Параметр содержит информацию в формате CFVReport.

Сервис разбора конфликтов

Сервис разбора конфликтов обрабатывает запрос на проверку ЭП документа на заданный момент времени и формирует отчет о проверке ЭП, что особенно актуально в случае признания ЭП недействительной.

Структура запроса к сервису разбора конфликтов:

```
<xs:complexType name="CSARequest">
                  <xs:sequence>
                        <xs:element name="validationRequest"

      type="tccs:ValidationRequestType">
                        </xs:element>
                        <xs:element name="validationDate"
type="cst:GeneralizedTime" maxOccurs="1"
minOccurs="0"></xs:element>
                        <xs:element name="caCerts"
type="tns:DataList" maxOccurs="1" minOccurs="0"></xs:element>
                        <xs:element name="otherCerts"
type="tns:DataList" maxOccurs="1" minOccurs="0"></xs:element>
                        <xs:element name="crls"
type="tns:DataList" maxOccurs="1" minOccurs="0"></xs:element>
                        <xs:element
name="crlAllowAfterNextUpdateSeconds" type="integer"
maxOccurs="1" minOccurs="0"></xs:element>
                        <xs:element name="signers"
type="tns:DataList" maxOccurs="1" minOccurs="0"></xs:element>
                  </xs:sequence>
            </xs:complexType>
            <xs:complexType name="DataList">
                  <xs:sequence>
                        <xs:element name="data"
type="cst:notEmptyB64Binary" maxOccurs="unbounded"
minOccurs="1"></xs:element>
                  </xs:sequence>
            </xs:complexType>
```

Параметры запроса:

- **validationRequest** — запрос на проверку;
- **validationDate** — время и дата, относительно которых проверяется ЭП.

Формат ответа:

```
            <xs:complexType name="CSAReport">
                  <xs:sequence>
                        <xs:element name="reportDateGmt"
type="cst:GeneralizedTime"></xs:element>
                        <xs:element name="actionList"
type="tns:ActionList"></xs:element>
                  </xs:sequence>
            </xs:complexType>
```

Параметры ответа:

- **reportDateGmt** — дата и время создания отчета;
- **actionList** — шаги, которые были выполнены при проверке ЭП.

Сообщения об ошибках

Все перечисленные в данном разделе документа операции в случае ошибки возвращают сообщение вида SOAPFault, содержательная часть которого имеет тип ServiceFaultInfo:

```
<xs:complexType name="ServiceFaultInfo">
<xs:sequence>
<xs:element name="type" type="cst:FaultType" />
<xs:element name="comment" type="cst:FaultComment" />
</xs:sequence>
</xs:complexType>
```

Параметр **type** содержит один из возможных типов ошибок:

- invalidRequestDataFormat — возвращается в случае ошибок в формате данных, переданных на проверку или на подписание:
  - поле signedData (операция Validate) содержит Base64 от ASN.1-кодированных данных, не являющихся CMS-SignedData либо имеющих ошибки в кодировании или расхождения со стандартами в структуре данных;
  - поле signedData (операция Validate) содержит Base64 от данных, не являющихся ни ASN.1-кодированными, ни XML-документом;
  - поле externalData (операция Validate) содержит Base64-кодированные данные, не являющиеся XML-документом;
  - поле data (операция Sign) содержит Base64-кодированные данные, не являющиеся XML-документом, и при этом указана необходимость создания подписи в формате, отличном от CMS-SignedData;
- invalidXmlPartID — указанный в запросе xmlPartID не найден в переданном XML-документе;
- invalidActor — указанный в запросе actor не найден в WS-Security;
- internalError — возвращается в случае любых ошибок, не покрываемых ни одним из других возможных значений данного поля.

Параметр **comment** содержит краткое (до 200 символов) дополнительное описание возникшей ошибки.

Примеры запросов к веб-сервисам и ответы от них

В приведенных ниже примерах запросов (request) к веб-сервисам вместо конкретных значений красным цветом выделены "переменные", которые нужно заменить конкретным значением для указанного параметра (описание параметров см. в разделе "Описание структур входных и выходных данных веб-сервисов").

В примерах ответов (response) вместо выделенных красным цветом "переменных" будут реальные сформированные веб-сервисом значения.

Digest request

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:sgv="http://www.roskazna.ru/eb/sign/types/sgv">
      <soapenv:Header/>
            <soapenv:Body>
                  <sgv:DigestRequestType>

      <sgv:dataBytes>@value_base64@</sgv:dataBytes>

      <sgv:algorithmId>@id@</sgv:algorithmId>
                  </sgv:DigestRequestType>
```

```
            </soapenv:Body>
</soapenv:Envelope>
```

Digest response

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Body>
<tccs:DigestResponseType
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">
<tccs:digest>@hash_base64@</tccs:digest>
<tccs:state>@base64@</tccs:state>
            </tccs:DigestResponseType>
   </soapenv:Body>
</soapenv:Envelope>
```

Sign request

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:sgv="http://www.roskazna.ru/eb/sign/types/sgv">
      <soapenv:Header/>
            <soapenv:Body>
                  <sgv:SigningRequestType>
                        <sgv:data>@doc_base64@</sgv:data>

      <sgv:signatureType>@type@</sgv:signatureType>

      <sgv:algorithmId>@id@</sgv:algorithmId>
                  </sgv:SigningRequestType>
            </soapenv:Body>
</soapenv:Envelope>
```

Sign response

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Body>
<tccs:SigningResponseType
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">@signed_
doc_base64@</tccs:SigningResponseType>
   </soapenv:Body>
</soapenv:Envelope>
```

Validate request

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:sgv="http://www.roskazna.ru/eb/sign/types/sgv">
<soapenv:Header/>
<soapenv:Body>
```

```
<sgv:ValidationRequestType
xmlns="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:ns2="http://www.roskazna.ru/eb/sign/types/cryptoserver">
<signedData>@signed_doc_base64@</signedData>
</sgv:ValidationRequestType>
</soapenv:Body>
</soapenv:Envelope>
```

Validate response

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
 <soapenv:Body>
<tccs:ValidationResponseType
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">
<tccs:gmtDateTime>@dd.MM.yyyy hh:mm:ss UTC@</tccs:gmtDateTime>
<tccs:globalStatus>@status@</tccs:globalStatus>
<tccs:SignatureInfos>
<cst:SignatureInfo>
<cst:reference>
<cst:issuerAndSerial>
<cst:IssuerAndSerial>
<cst:Issuer>
<cst:DistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.3</cst:AttributeType>
<cst:CommonName>
<cst:PrintableString>@value@</cst:PrintableString>
</cst:CommonName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
</cst:DistinguishedName>
</cst:Issuer>
<cst:SerialNumber>@value@</cst:SerialNumber>
</cst:IssuerAndSerial>
</cst:issuerAndSerial>
</cst:reference>
<cst:status>@status@</cst:status>
<cst:signerCertInfo>
<cst:Certificate>
<cst:TBSCertificate>
<cst:Version>@value@</cst:Version>
<cst:CertificateSerialNumber>@value@</cst:CertificateSerialNum
ber>
<cst:Signature>
<cst:AlgId>@value@</cst:AlgId>
</cst:Signature>
<cst:Issuer>
<cst:DistinguishedName>
<cst:RelativeDistinguishedName>
```

```
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.3</cst:AttributeType>
<cst:CommonName>
<cst:PrintableString>@value@</cst:PrintableString>
  </cst:CommonName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
</cst:DistinguishedName>
</cst:Issuer>
<cst:Validity>
<cst:NotBefore>
<cst:UTCTime>@dd.MM.yyyy hh:mm:ss UTC@</cst:UTCTime>
</cst:NotBefore>
<cst:NotAfter>
<cst:UTCTime>@dd.MM.yyyy hh:mm:ss UTC@</cst:UTCTime>
</cst:NotAfter>
</cst:Validity>
<cst:Subject>
<cst:DistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.6</cst:AttributeType>
<cst:CountryName>
<cst:iso-3166-code>@value@</cst:iso-3166-code>
</cst:CountryName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.8</cst:AttributeType>
<cst:StateOrProvinceName>
<cst:PrintableString>@value@</cst:PrintableString>
</cst:StateOrProvinceName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.7</cst:AttributeType>
<cst:LocalityName>
<cst:PrintableString>@value@</cst:PrintableString>
</cst:LocalityName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.10</cst:AttributeType>
<cst:OrganizationName>
<cst:PrintableString>@value@</cst:PrintableString>
</cst:OrganizationName>
</cst:AttributeTypeAndValue>
```

```
</cst:RelativeDistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.11</cst:AttributeType>
<cst:OrganizationalUnitName>
<cst:PrintableString>@value@</cst:PrintableString>
</cst:OrganizationalUnitName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.3</cst:AttributeType>
<cst:CommonName>
<cst:PrintableString>@value@</cst:PrintableString>
</cst:CommonName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>1.2.840.113549.1.9.1</cst:AttributeType>
<cst:EmailAddress>@value@</cst:EmailAddress>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
</cst:DistinguishedName>
</cst:Subject>
<cst:SubjectPublicKeyInfo>
<cst:PublicKeyAlgorithm>
<cst:AlgId>1.2.643.2.2.19</cst:AlgId>
<cst:gostR3410EC_CryptoPro>
<cst:gostR3410_2001_parameters>
<cst:OBJECT_IDENTIFIER>1.2.643.2.2.36.0</cst:OBJECT_IDENTIFIER
>
<cst:OBJECT_IDENTIFIER>1.2.643.2.2.30.1</cst:OBJECT_IDENTIFIER
>
</cst:gostR3410_2001_parameters>
</cst:gostR3410EC_CryptoPro>
</cst:PublicKeyAlgorithm>
<cst:SubjectPublicKey>@value@</cst:SubjectPublicKey>
</cst:SubjectPublicKeyInfo>
<cst:Extensions>
<cst:Extension>
<cst:ExtensionType>2.5.29.15</cst:ExtensionType>
<cst:Critical>{TRUE}</cst:Critical>
<cst:extValue>
<cst:KeyUsage>@value@</cst:KeyUsage>
</cst:extValue>
</cst:Extension>
<cst:Extension>
<cst:ExtensionType>@value@</cst:ExtensionType>
<cst:extValue>
<cst:SMIMECapabilities>
```

```
<cst:AlgorithmIdentifier>
<cst:AlgId>@value@</cst:AlgId>
</cst:AlgorithmIdentifier>
</cst:SMIMECapabilities>
</cst:extValue>
</cst:Extension>
<cst:Extension>
<cst:ExtensionType>2.5.29.14</cst:ExtensionType>
<cst:extValue>
<cst:SubjectKeyIdentifier>@value@</cst:SubjectKeyIdentifier>
</cst:extValue>
</cst:Extension>
<cst:Extension>
<cst:ExtensionType>2.5.29.37</cst:ExtensionType>
<cst:extValue>
<cst:ExtKeyUsage>
<cst:EmailProtection>@value@</cst:EmailProtection>
 </cst:ExtKeyUsage>
</cst:extValue>
</cst:Extension>
<cst:Extension>
<cst:ExtensionType>2.5.29.35</cst:ExtensionType>
<cst:extValue>
<cst:AuthorityKeyIdentifier>
<cst:KeyIdentifier>@value@</cst:KeyIdentifier>
</cst:AuthorityKeyIdentifier>
  </cst:extValue>
</cst:Extension>
<cst:Extension>
<cst:ExtensionType>2.5.29.31</cst:ExtensionType>
<cst:extValue>
<cst:CRLDistributionPoints>
<cst:DistributionPoint>
<cst:DistributionPointName>
<cst:FullName>
<cst:GeneralName>
<cst:URI>@value@</cst:URI>
</cst:GeneralName>
</cst:FullName>
</cst:DistributionPointName>
</cst:DistributionPoint>
</cst:CRLDistributionPoints>
</cst:extValue>
</cst:Extension>
<cst:Extension>
<cst:ExtensionType>1.3.6.1.5.5.7.1.1</cst:ExtensionType>
<cst:extValue>
<cst:AuthorityInfoAccess>
<cst:AccessDescription>
<cst:AccessMethod>@value@</cst:AccessMethod>
```

```
<cst:AccessLocation>
<cst:URI>@value@</cst:URI>
</cst:AccessLocation>
</cst:AccessDescription>
<cst:AccessDescription>
<cst:AccessMethod>@value@</cst:AccessMethod>
<cst:AccessLocation>
<cst:URI>@value@</cst:URI>
</cst:AccessLocation>
</cst:AccessDescription>
</cst:AuthorityInfoAccess>
</cst:extValue>
</cst:Extension>
</cst:Extensions>
</cst:TBSCertificate>
<cst:AlgorithmIdentifier>
<cst:AlgId>@value@</cst:AlgId>
</cst:AlgorithmIdentifier>
<cst:Signature>@value@</cst:Signature>
</cst:Certificate>
</cst:signerCertInfo>
<cst:validationDate>@dd.MM.yyyy hh:mm:ss
UTC@</cst:validationDate>
</cst:SignatureInfo>
</tccs:SignatureInfos>
</tccs:ValidationResponseType>
</soapenv:Body>
</soapenv:Envelope>
```

CreateAdvanced request #1

Запрос на проверку с усилением по умолчанию:

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:sgv="http://www.roskazna.ru/eb/sign/types/sgv">
<soapenv:Header/>
<soapenv:Body>
<sgv:ValidationRequestType
xmlns="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:ns2="http://www.roskazna.ru/eb/sign/types/cryptoserver">
<signedData>@signed_doc_base64@</signedData>
<createAdvanced>true</createAdvanced>
<sgv:algorithmId>1.2.643.7.1.1.3.2</sgv:algorithmId>
</sgv:ValidationRequestType>
</soapenv:Body>
</soapenv:Envelope>
```

CreateAdvanced request #2

Запрос на проверку с усилением и указанием типа подписи, до которой требуется усиление. Вместо @value@ в поле createAdvanced нужно указать конкретный тип подписи:

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:sgv="http://www.roskazna.ru/eb/sign/types/sgv">
<soapenv:Header/>
<soapenv:Body>
<sgv:ValidationRequestType
xmlns="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:ns2="http://www.roskazna.ru/eb/sign/types/cryptoserver">
<signedData>@signed_doc_base64@</signedData>
<createAdvanced>@value@</createAdvanced>
<sgv:algorithmId>1.2.643.7.1.1.3.2</sgv:algorithmId>
</sgv:ValidationRequestType>
</soapenv:Body>
</soapenv:Envelope>
```

CreateAdvanced response

Ответ будет одинаков для двух вышеперечисленных запросов с единственной разницей в значении поля advanced (сформированная усиленная подпись):

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Body>
<tccs:ValidationResponseType
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">
<tccs:gmtDateTime>@dd.MM.yyyy hh:mm:ss UTC@</tccs:gmtDateTime>
<tccs:globalStatus>@status@</tccs:globalStatus>
<tccs:SignatureInfos>
<cst:SignatureInfo>
<cst:reference>
<cst:issuerAndSerial>
<cst:IssuerAndSerial>
<cst:Issuer>
<cst:DistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.3</cst:AttributeType>
   <cst:CommonName>
<cst:PrintableString>@value@</cst:PrintableString>
     </cst:CommonName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
</cst:DistinguishedName>
  </cst:Issuer>
<cst:SerialNumber>@value@</cst:SerialNumber>
  </cst:IssuerAndSerial>
</cst:issuerAndSerial>
  </cst:reference>
<cst:status>@status@</cst:status>
<cst:signerCertInfo>
<cst:Certificate>
<cst:TBSCertificate>
```

```
<cst:Version>@value@</cst:Version>
<cst:CertificateSerialNumber>@value@</cst:CertificateSerialNum
ber>
<cst:Signature>
<cst:AlgId>@value@</cst:AlgId>
</cst:Signature>
<cst:Issuer>
  <cst:DistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.3</cst:AttributeType>
  <cst:CommonName>
<cst:PrintableString>@value@</cst:PrintableString>
 </cst:CommonName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
</cst:DistinguishedName>
</cst:Issuer>
<cst:Validity>
 <cst:NotBefore>
<cst:UTCTime>@dd.MM.yyyy hh:mm:ss UTC@</cst:UTCTime>
</cst:NotBefore>
<cst:NotAfter>
<cst:UTCTime>@dd.MM.yyyy hh:mm:ss UTC@</cst:UTCTime>
</cst:NotAfter>
</cst:Validity>
<cst:Subject>
<cst:DistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.6</cst:AttributeType>
<cst:CountryName>
<cst:iso-3166-code>@value@</cst:iso-3166-code>
</cst:CountryName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.8</cst:AttributeType>
<cst:StateOrProvinceName>
<cst:PrintableString>@value@</cst:PrintableString>
</cst:StateOrProvinceName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.7</cst:AttributeType>
<cst:LocalityName>
<cst:PrintableString>@value@</cst:PrintableString>
</cst:LocalityName>
</cst:AttributeTypeAndValue>
```

```
</cst:RelativeDistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.10</cst:AttributeType>
<cst:OrganizationName>
<cst:PrintableString>@value@</cst:PrintableString>
</cst:OrganizationName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.11</cst:AttributeType>
<cst:OrganizationalUnitName>
<cst:PrintableString>@value@</cst:PrintableString>
</cst:OrganizationalUnitName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>2.5.4.3</cst:AttributeType>
<cst:CommonName>
<cst:PrintableString>@value@</cst:PrintableString>
</cst:CommonName>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
<cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue>
<cst:AttributeType>1.2.840.113549.1.9.1</cst:AttributeType>
<cst:EmailAddress>@value@</cst:EmailAddress>
</cst:AttributeTypeAndValue>
</cst:RelativeDistinguishedName>
</cst:DistinguishedName>
</cst:Subject>
<cst:SubjectPublicKeyInfo>
<cst:PublicKeyAlgorithm>
<cst:AlgId>@value@</cst:AlgId>
<cst:gostR3410EC_CryptoPro>
<cst:gostR3410_2001_parameters>
<cst:OBJECT_IDENTIFIER>1.2.643.2.2.36.0</cst:OBJECT_IDENTIFIER
>
<cst:OBJECT_IDENTIFIER>1.2.643.2.2.30.1</cst:OBJECT_IDENTIFIER
>
</cst:gostR3410_2001_parameters>
</cst:gostR3410EC_CryptoPro>
</cst:PublicKeyAlgorithm>
<cst:SubjectPublicKey>@value@</cst:SubjectPublicKey>
</cst:SubjectPublicKeyInfo>
<cst:Extensions>
<cst:Extension>
<cst:ExtensionType>2.5.29.15</cst:ExtensionType>
<cst:Critical>{TRUE}</cst:Critical>
```

```
<cst:extValue>
<cst:KeyUsage>@value@</cst:KeyUsage>
</cst:extValue>
</cst:Extension>
<cst:Extension>
<cst:ExtensionType>1.2.840.113549.1.9.15</cst:ExtensionType>
<cst:extValue>
<cst:SMIMECapabilities>
<cst:AlgorithmIdentifier>
<cst:AlgId>@value@</cst:AlgId>
</cst:AlgorithmIdentifier>
</cst:SMIMECapabilities>
</cst:extValue>
</cst:Extension>
<cst:Extension>
<cst:ExtensionType>2.5.29.14</cst:ExtensionType>
<cst:extValue>
<cst:SubjectKeyIdentifier>@value@</cst:SubjectKeyIdentifier>
</cst:extValue>
</cst:Extension>
<cst:Extension>
<cst:ExtensionType>2.5.29.37</cst:ExtensionType>
<cst:extValue>
<cst:ExtKeyUsage>
<cst:EmailProtection>@value@</cst:EmailProtection>
</cst:ExtKeyUsage>
</cst:extValue>
</cst:Extension>
<cst:Extension>
<cst:ExtensionType>2.5.29.35</cst:ExtensionType>
<cst:extValue>
<cst:AuthorityKeyIdentifier>
<cst:KeyIdentifier>@value@</cst:KeyIdentifier>
</cst:AuthorityKeyIdentifier>
</cst:extValue>
</cst:Extension>
<cst:Extension>
<cst:ExtensionType>2.5.29.31</cst:ExtensionType>
<cst:extValue>
<cst:CRLDistributionPoints>
<cst:DistributionPoint>
<cst:DistributionPointName>
<cst:FullName>
<cst:GeneralName>
<cst:URI>@value@</cst:URI>
</cst:GeneralName>
</cst:FullName>
</cst:DistributionPointName>
</cst:DistributionPoint>
</cst:CRLDistributionPoints>
```

```
</cst:extValue>
</cst:Extension>
<cst:Extension>
<cst:ExtensionType>1.3.6.1.5.5.7.1.1</cst:ExtensionType>
<cst:extValue>
<cst:AuthorityInfoAccess>
<cst:AccessDescription>
<cst:AccessMethod>1.3.6.1.5.5.7.48.2</cst:AccessMethod>
<cst:AccessLocation>
<cst:URI>@value@</cst:URI>
</cst:AccessLocation>
</cst:AccessDescription>
<cst:AccessDescription>
<cst:AccessMethod>@value@</cst:AccessMethod>
<cst:AccessLocation>
<cst:URI>@value@</cst:URI>
</cst:AccessLocation>
</cst:AccessDescription>
</cst:AuthorityInfoAccess>
</cst:extValue>
</cst:Extension>
</cst:Extensions>
</cst:TBSCertificate>
<cst:AlgorithmIdentifier>
<cst:AlgId>@value@</cst:AlgId>
</cst:AlgorithmIdentifier>
<cst:Signature>@value@</cst:Signature>
</cst:Certificate>
</cst:signerCertInfo>
<cst:validationDate>@dd.MM.yyyy hh:mm:ss
UTC@</cst:validationDate>
</cst:SignatureInfo>
</tccs:SignatureInfos>
<tccs:advanced>@value@</tccs:advanced>
</tccs:ValidationResponseType>
</soapenv:Body>
</soapenv:Envelope>
```

CertificateFormatValidation request

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:sgv="http://www.roskazna.ru/eb/sign/types/sgv">
<soapenv:Header/>
<soapenv:Body>
<sgv:CFVRequestType>
<sgv:certificate>@certificate_base64@</sgv:certificate>
<sgv:subjectType>@type@</sgv:subjectType>
</sgv:CFVRequestType>
</soapenv:Body>
</soapenv:Envelope>
```

CertificateFormatValidation response

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Body>
<tccs:CFVReport
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">
<tccs:CFVNotice>
<tccs:level>@level@</tccs:level>
<tccs:noticeClass>@class@</tccs:noticeClass>
<tccs:offset>@value_bytes@</tccs:offset>
<tccs:failPath>@path_to_field_with_error@</tccs:failPath>
<tccs:comment>@comment@</tccs:comment>
</tccs:CFVNotice>
</tccs:CFVReport>
</soapenv:Body>
</soapenv:Envelope>
```

CertificateValidation request

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:sgv="http://www.roskazna.ru/eb/sign/types/sgv">
<soapenv:Header/>
<soapenv:Body>
<sgv:CVRequestType>
<sgv:certificate>@certificate_base64@</sgv:certificate>
sgv:CVRequestType>
</soapenv:Body>
</soapenv:Envelope>
```

CertificateValidation response

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Body>
<tccs:CVResponse
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">
<tccs:ESSCertIDv2>
<tccs:hashAlgorithm>
<tccs:AlgId>@id@</tccs:AlgId>
<tccs:gostR3411_CryptoPro>
<tccs:Inherit_GOST_R34.11_Crypto-
Pro_parameters>{NULL}</tccs:Inherit_GOST_R34.11_Crypto-
Pro_parameters>
</tccs:gostR3411_CryptoPro>
</tccs:hashAlgorithm>
<tccs:certHash>@hash@</tccs:certHash>
<tccs:issuerSerial>
<tccs:issuer>
<tccs:GeneralName>
```

```
<tccs:DirectoryName>
<tccs:DistinguishedName>
<tccs:RelativeDistinguishedName>
<tccs:AttributeTypeAndValue>
<tccs:AttributeType>1.2.643.100.1</tccs:AttributeType>
<tccs:OGRN>
<tccs:numeric>@value@</tccs:numeric>
</tccs:OGRN>
</tccs:AttributeTypeAndValue>
</tccs:RelativeDistinguishedName>
<tccs:RelativeDistinguishedName>
<tccs:AttributeTypeAndValue>
<tccs:AttributeType>1.2.643.3.131.1.1</tccs:AttributeType>
<tccs:INN>
<tccs:numeric>@value@</tccs:numeric>
</tccs:INN>
</tccs:AttributeTypeAndValue>
</tccs:RelativeDistinguishedName>
<tccs:RelativeDistinguishedName>
<tccs:AttributeTypeAndValue>
<tccs:AttributeType>2.5.4.9</tccs:AttributeType>
<tccs:StreetAddress>
<tccs:UTF8String>@value@</tccs:UTF8String>
</tccs:StreetAddress>
</tccs:AttributeTypeAndValue>
</tccs:RelativeDistinguishedName>
<tccs:RelativeDistinguishedName>
<tccs:AttributeTypeAndValue>
<tccs:AttributeType>1.2.840.113549.1.9.1</tccs:AttributeType>
<tccs:EmailAddress>@value@</tccs:EmailAddress>
</tccs:AttributeTypeAndValue>
</tccs:RelativeDistinguishedName>
<tccs:RelativeDistinguishedName>
<tccs:AttributeTypeAndValue>
<tccs:AttributeType>2.5.4.6</tccs:AttributeType>
<tccs:CountryName>
<tccs:iso-3166-code>@value@</tccs:iso-3166-code>
</tccs:CountryName>
</tccs:AttributeTypeAndValue>
</tccs:RelativeDistinguishedName>
<tccs:RelativeDistinguishedName>
<tccs:AttributeTypeAndValue>
<tccs:AttributeType>2.5.4.8</tccs:AttributeType>
<tccs:StateOrProvinceName>
<tccs:UTF8String>@value@</tccs:UTF8String>
</tccs:StateOrProvinceName>
</tccs:AttributeTypeAndValue>
</tccs:RelativeDistinguishedName>
<tccs:RelativeDistinguishedName>
<tccs:AttributeTypeAndValue>
```

```
<tccs:AttributeType>2.5.4.7</tccs:AttributeType>
<tccs:LocalityName>
<tccs:UTF8String>@value@</tccs:UTF8String>
</tccs:LocalityName>
</tccs:AttributeTypeAndValue>
</tccs:RelativeDistinguishedName>
<tccs:RelativeDistinguishedName>
<tccs:AttributeTypeAndValue>
<tccs:AttributeType>2.5.4.10</tccs:AttributeType>
<tccs:OrganizationName>
<tccs:UTF8String>@value@</tccs:UTF8String>
</tccs:OrganizationName>
</tccs:AttributeTypeAndValue>
</tccs:RelativeDistinguishedName>
<tccs:RelativeDistinguishedName>
<tccs:AttributeTypeAndValue>
<tccs:AttributeType>2.5.4.3</tccs:AttributeType>
<tccs:CommonName>
<tccs:UTF8String>@value@</tccs:UTF8String>
</tccs:CommonName>
</tccs:AttributeTypeAndValue>
</tccs:RelativeDistinguishedName>
</tccs:DistinguishedName>
</tccs:DirectoryName>
</tccs:GeneralName>
</tccs:issuer>
<tccs:serial>@value@</tccs:serial>
</tccs:issuerSerial>
</tccs:ESSCertIDv2>
<tccs:date>@unix_time_value@</tccs:date>
<tccs:status>@value@</tccs:status>
<cst:faultInfo>
<cst:type>@value_type@</cst:type>
<cst:comment>@value_comment@</cst:comment>
</cst:faultInfo>
</tccs:CVResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Глава 5
Контроль функционирования комплекса

Контроль работоспособности технических и программных средств

Средствами контроля работоспособности выступают штатные средства аппаратных платформ, общесистемного и прикладного программного обеспечения в соответствии с их эксплуатационной документацией.

Основными обязанностями программиста по контролю работоспособности технических и программных средств являются:

- мониторинг прикладных и общесистемных журналов. Прикладные журналы расположены в директориях /var/opt/tccs/log/ и /var/opt/tccs/apache.log/. Общесистемные журналы — в директории /var/log/. Также журналы могут использоваться для контроля работоспособности веб-сервисов и транспортных протоколов;
- обработка почтовых уведомлений с информацией о состоянии сервисов. Уведомления делятся на две группы — штатные и нештатные (в случае возникновения нештатных ситуаций, связанных с доступностью сервисов). Все уведомления инициируются программой tccs_watchdog;
- мониторинг общесистемных процессов, анализ которых выходит за рамки программы tccs_watchdog. Мониторинг общесистемных процессов выполняется с помощью консольной команды ps:

```
ps ax | grep crond
```

или

```
ps ax | grep syslogd
```

В случае отсутствия процессов либо актуальных прикладных или общесистемных журналов необходимо выполнить запуск сценариев:

```
/etc/init.d/crond restart
```

или

```
/etc/init.d/syslogd restart
```

Программные модули ПАК Jinn-Server содержат специальные средства активного контроля за работоспособностью сервисов, выполняющих автоматические попытки перезапустить зависшие процессы сервисов, а также предоставляют способы оповещения обслуживающего персонала по электронной почте (дополнительно см. главу "Сообщения" настоящего документа).

В случае нештатных ситуаций, при невозможности автоматическими средствами обеспечить восстановление штатного функционирования комплекса, следует детализировать причину нештатной ситуации по прикладным и/или общесистемным журналам.

Ведение архивных копий прикладных и общесистемных журналов

Для упрощения последующего аудита функционирования ПАК, а также минимизации времени восстановления ПАК в случае сбоев в обязанности программиста входит ведение архивных копий журналов и архивных копий содержимого БД csm.

Архивные копии журналов

Архивные копии журналов формируются штатными средствами системы с помощью механизма logrotate, а также путем копирования копий журналов на внешний отчуждаемый носитель.

Конфигурационные файлы с описанием правил ротации журналов ПАК Jinn-Server расположены в каталоге /opt/tccs/etc/logrotate.d/.

Примерный вид конфигурационного файла с правилами ротации приведен ниже:

```
su  root root
/var/opt/tccs/log/cgi /var/opt/tccs/log/online
/var/opt/tccs/log/misc /var/opt/tccs/log/offline
{
   # правила ротации
   rotate 10
   missingok
   notifempty
   create 666 root root
   compress
   maxsize 100M
   daily
   nodateext
   postrotate
   killall -HUP cas1d
   kill -HUP $(ps -eo ppid,pid,cmd | grep tccs.ss | awk '$1==1
{printf("%d ", $2);}')
   kill -HUP $(ps -eo ppid,pid,cmd | grep tccs.svs | awk
'$1==1 {printf("%d ", $2);}')
   killall -HUP rsyslogd
   endscript
}
```

Ключевым параметром является параметр rotate, значение которого указывает на количество ежедневных копий. По истечении указанного значения необходимо подключить к системе отчуждаемый носитель, создать директорию на файловой системе носителя с названием, указывающим на дату копирования журналов, и скопировать в нее содержимое директорий /var/opt/tccs/log/ и /var/opt/tccs/apache.log/.

Архивные копии БД csm

Создание архивных копий БД csm рекомендуется осуществлять по необходимости, но не реже двух раз в месяц.

Для копирования БД csm требуется подключить отчуждаемый носитель и выполнить следующие действия:

1. Остановите сервис crond командой:

   ```
   service crond stop
   ```

   Убедитесь, что сервисы, запускаемые планировщиком (cas1_crl_update, cas1_tsl_update), завершили свою работу.

2. Экспортируйте базу данных командой:

   ```
   pg_dump --column-inserts -a -S root --disable-triggers -U
   postgres csm > cas1_db.sql
   ```

   где

   - root — учетная запись суперпользователя на целевой машине;
   - cas1_db — имя целевого SQL-файла.

3. Запустите сервис crond командой:

   ```
   service crond start
   ```

Приведенный пример предусматривает предварительное монтирование отчуждаемого носителя в директорию /mnt/flash/.

Архив БД csm может быть также сохранен на любой локальный жесткий диск, имеющий достаточный для сохранения архива объем.

Глава 6
Сообщения

Компоненты ПАК Jinn-Server содержат в своем составе специальные модули, обеспечивающие мониторинг процессов (сервисов) и автоматический перезапуск в случае прерывания их работы. Оповещение обслуживающего персонала осуществляется по электронной почте на указанные в конфигурации адреса по факту следующих событий:

- процесс не запущен (прерван);
- произведена попытка запустить процесс автоматически;
- результат процедуры автоматического перезапуска.

Настройка мониторинга осуществляется в конфигурационном файле /opt/tccs/etc/csm.conf:

```
"watchedservice _tccs.admin_enable": [
        { "hostname": "tccs1.domain.ru" },
        { "port": 80 },
        { "socket": "" },
        { "action": "/opt/tccs/etc/init.d/tccs.admin" },
        { "description": "CSM WEB ADMIN" }
],
"watchedservice_tccs.cas1d_enable": [
        { "hostname": "tccs1.domain.ru" },
        { "port": 11112 },
        { "socket": "" },
        { "action": "/opt/tccs/etc/init.d/cas1d" },
        { "description": "CRL Archive Daemon" }
],
"watchedservice_psqld_enable": [
        { "hostname": "tccs1.domain.ru" },
        { "port": 0 },
        { "socket": "/tmp/.s.PGSQL.5432" },
        { "action": "/opt/tccs/etc/init.d/psqld" },
        { "description": "PostgreSQL" }
],
"notification_enable": "yes",
"notification_email": "admin@domain.ru"
```

Объект, описывающий процесс (сервис), который необходимо контролировать, представляет структуру с названием watchedservice, состоящую из следующих параметров:

- hostname — доменное имя сервера, к которому относится процесс;
- port — сетевой порт, который "слушает" процесс;
- socket — unix-сокет, который "слушает" процесс;
- action — путь к исполняемому shell-сценарию, который может выполнять остановку, запуск или перезапуск процесса;
- description — описание процесса.

Также можно настраивать почтовые уведомления с помощью параметров:

- notification_enable — включение (yes) или выключение (no) почтового уведомления;
- notification_email — адрес получателя почтового уведомления.

Настройка параметров соединения с почтовым сервером выполняется в конфигурационном файле /opt/tccs/etc/msmtp.conf:

```
defaults
tls on
tls_starttls on
# tls_trust_file @TRUST_FILE@
# tls_crl_file @CRL_FILE@
# tls_fingerprint @FINGERPRINT@
tls_certcheck off
# tls_key_file @KEY_FILE@
# tls_cert_file @TLS_CERT_FILE@
# tls_priorities @PRIORITIES@
# tls_host_override @HOST_OVERRIDE@

account ntml_config
auth ntml

host mail.domain.ru
port 587
from testing-robot@domain.ru
user testing_robot@domain.ru
password "*********"
domain domain.ru
ntlmdomain domain
# Set a default account
account default : ntlm_config
```

В данном файле настраиваются следующие параметры соединения с почтовым сервером:

- host — почтовый сервер, через который будут отправляться почтовые уведомления;
- port — сетевой порт почтового сервера;
- from — электронный адрес отправителя;
- user — имя учетной записи отправителя на почтовом сервере;
- password — пароль доступа к почтовому серверу;
- domain — доменное имя сервера;
- ntlmdomain — имя ntlm-домена при использовании ntlm-аутентификации.

Электронный адрес получателя почтового уведомления также указывается в исполняемом shell-скрипте /opt/tccs/bin/notifier.sh в параметре TO:

```
#!/bin/sh

source /opt/tccs/bin/common_functions.sh

TO="admin@domain.ru"
NAME=`installed_module`
PROG="/opt/tccs/oss/bin/msmtp"
BODY="/tmp/test_message.txt"
CONF="/opt/tccs/etc/msmtp.conf"
touch /tmp/notification.start
```

```
if  [ "x$1" = "x" ] ||  [ ! -f $1 ] || [ ! -n "$TO" ] || [ ! -
n "$NAME" ] || [ ! -n "$PROG" ] || [ ! -f $PROG ]; then
      touch /tmp/notification.error
      exit 1
fi

if test "x$2" != "x"; then
      TO=$2
fi

SUBJECT="$NAME Автоматическое уведомление об изменении
состояния процесса."
BODY=$1
mail_send
touch /tmp/notification.stop
exit 0
```

Примечание. Параметр TO должен совпадать с параметром notification_email в конфигурационном файле /opt/tccs/etc/csm.conf.

Приложение 1. Описание веб-сервисов

```
<?xml version="1.0" encoding="utf-8"?>
<!-- $Revision: 1.9 $ $Date: 2014/09/29 07:21:31 $-->
<definitions
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
      xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/
"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
      xmlns:tns="http://www.roskazna.ru/eb/sign/types/sgv"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
      xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
      name="TCCS"
targetNamespace="http://www.roskazna.ru/eb/sign/types/sgv"
      xmlns="http://schemas.xmlsoap.org/wsdl/">

    <types>
    <xs:schema
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"

xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv"
          xmlns:tns="http://schemas.xmlsoap.org/wsdl/"
          elementFormDefault="qualified"

targetNamespace="http://www.roskazna.ru/eb/sign/types/sgv">

          <xs:import
schemaLocation="http://62.181.53.2:18080/tccs.x509.xsd"

namespace="http://www.roskazna.ru/eb/sign/types/cryptoserver"
/>

            <xs:element name="ValidationRequestType"
type="tccs:ValidationRequestType" />
            <xs:element name="SigningRequestType"
type="tccs:SigningRequestType" />
            <xs:element name="DigestRequestType"
type="tccs:DigestRequestType" />
          <xs:element name="CFVRequestType"
type="cst:notEmptyB64Binary" />
            <xs:element name="ValidationResponseType"
type="tccs:ValidationRes" />
            <xs:element name="SigningResponseType"
type="cst:notEmptyB64Binary" />
            <xs:element name="DigestResponseType"
type="tccs:DigestResponseType" />
          <xs:element name="CFVReport" type="tccs:CFVReport"
/>
            <xs:element name="ServiceFaultInfo"
type="tccs:ServiceFaultInfo" />

      <xs:complexType name="CFVReport">
```

```
            <xs:sequence>
                  <xs:element name="CFVNotice"
type="tccs:CFVNotice" minOccurs="0"/>
            </xs:sequence>
      </xs:complexType>

      <xs:complexType name="CFVNotice">
            <xs:sequence>
                  <xs:element name="level">
                        <xs:simpleType>
                              <xs:restriction
base="xs:integer">
                                    <xs:enumeration value="0"
/>
                                    <xs:enumeration value="1"
/>
                              </xs:restriction>
                        </xs:simpleType>
                  </xs:element>
                  <xs:element name="offset" type="xs:integer"
/>
                  <xs:element name="failPath" type="xs:string"
/>
                  <xs:element name="comment" type="xs:string"
/>
            </xs:sequence>
      </xs:complexType>

            <xs:complexType name="ValidationRes">
                <xs:sequence>
                    <xs:element name="gmtDateTime"
type="cst:GmtDateTime" />
                    <xs:element name="globalStatus"
type="cst:GlobalStatus" />
                    <xs:element minOccurs="0"
name="SignatureInfos" type="cst:SignatureInfos" />
                    <xs:element minOccurs="0" name="advanced"
type="cst:notEmptyB64Binary" />
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="ValidationRequestType">
                <xs:sequence>
                    <xs:element name="signedData"
type="cst:notEmptyB64Binary" />
                    <xs:element minOccurs="0"
name="externalData" type="cst:notEmptyB64Binary" />
                    <xs:element minOccurs="0" default="false"
name="createAdvanced"  type="tccs:svsCreateAdvanced"/>
                    <xs:element minOccurs="0" name="xmlPartID"
type="xs:string" />
                    <xs:element minOccurs="0" name="actor"
type="xs:string" />
                    <xs:element minOccurs="0" default="false"
name="ignoreSignatureTimeStamp" type="xs:boolean" />
```

```
                    <xs:element minOccurs="0"
name="algorithmId" type="cst:OBJECT_IDENTIFIER" />
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="SigningRequestType">
                <xs:sequence>
                    <xs:element name="data"
type="cst:notEmptyB64Binary" />
                    <xs:element minOccurs="0" default="cades-
bes" name="signatureType" type="cst:signatureType" />
                    <xs:element minOccurs="0" default="false"
name="detached" type="xs:boolean" />
                    <xs:element minOccurs="0" name="xmlPartID"
type="xs:string" />
                    <xs:element minOccurs="0" name="actor"
type="xs:string" />
                    <xs:element minOccurs="0"
name="algorithmId" type="cst:OBJECT_IDENTIFIER" />
                    <xs:element minOccurs="0"
name="transforms" type="cst:notEmptyB64Binary" />
                    <xs:element minOccurs="0"
name="businessProcessId" type="xs:string" />
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="DigestRequestType">
                <xs:sequence>
                    <xs:element minOccurs="0" name="dataBytes"
type="cst:notEmptyB64Binary" />
                    <xs:element minOccurs="0" name="paramOID"
type="cst:OBJECT_IDENTIFIER" />
                    <xs:element minOccurs="0"
name="algorithmId" type="cst:OBJECT_IDENTIFIER" />
                    <xs:element minOccurs="0" name="state"
type="cst:notEmptyB64Binary" />
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="DigestResponseType">
                <xs:sequence>
                    <xs:element minOccurs="0" name="digest"
type="cst:notEmptyB64Binary" />
                    <xs:element minOccurs="0" name="state"
type="cst:notEmptyB64Binary" />
                </xs:sequence>
            </xs:complexType>

            <xs:complexType name="ServiceFaultInfo">
                <xs:sequence>
                    <xs:element name="type"
type="cst:FaultType" />
                    <xs:element name="comment"
type="cst:FaultComment" />
                </xs:sequence>
            </xs:complexType>
        </xs:schema>
```

```
    </types>
    <message name="ValidationRequestMessage">
        <part name="request"
element="tns:ValidationRequestType" />
    </message>
    <message name="ValidationResponseMessage">
        <part name="response"
element="tns:ValidationResponseType" />
    </message>
    <message name="SigningRequestMessage">
        <part name="request" element="tns:SigningRequestType"
/>
    </message>
    <message name="SigningResponseMessage">
        <part name="response"
element="tns:SigningResponseType" />
    </message>
    <message name="DigestRequestMessage">
        <part name="request" element="tns:DigestRequestType"
/>
    </message>
    <message name="DigestResponseMessage">
        <part name="response" element="tns:DigestResponseType"
/>
    </message>
    <message name="ValidationFaultMessage">
        <part name="failresponse"
element="tns:ServiceFaultInfo" />
    </message>
    <message name="SigningFaultMessage">
        <part name="failresponse"
element="tns:ServiceFaultInfo" />
    </message>
    <message name="DigestFaultMessage">
        <part name="failresponse"
element="tns:ServiceFaultInfo" />
    </message>
    <message name="CFVRequestMessage">
        <part name="request" element="tns:CFVRequestType" />
    </message>
    <message name="CFVResponseMessage">
        <part name="response" element="tns:CFVReport" />
    </message>
    <message name="CFVFaultMessage">
        <part name="failresponse"
element="tns:ServiceFaultInfo" />
    </message>

    <portType name="ValidationPortType">
        <operation name="Validate">
            <input message="tns:ValidationRequestMessage" />
            <output message="tns:ValidationResponseMessage" />
```

```
            <fault name="ValidationFault"
message="tns:ValidationFaultMessage" />
        </operation>
        <operation name="CertificateFormatValidate">
            <input message="tns:CFVRequestMessage" />
            <output message="tns:CFVResponseMessage" />
            <fault name="CFVFault"
message="tns:CFVFaultMessage" />
        </operation>
    </portType>
    <portType name="SigningPortType">
        <operation name="Sign">
            <input message="tns:SigningRequestMessage" />
            <output message="tns:SigningResponseMessage" />
            <fault name="SigningFault"
message="tns:SigningFaultMessage" />
        </operation>
        <operation name="Digest">
            <input message="tns:DigestRequestMessage" />
            <output message="tns:DigestResponseMessage" />
            <fault name="DigestFault"
message="tns:DigestFaultMessage" />
        </operation>
    </portType>
    <binding name="ValidationBinding"
type="tns:ValidationPortType">
        <soap:binding
transport="http://schemas.xmlsoap.org/soap/http" />
        <operation name="Validate">
           <soap:operation
soapAction="http://www.roskazna.ru/eb/sign/types/sgv/Validate" />
            <input>
                <soap:body use="literal" />
            </input>
            <output>
                <soap:body use="literal" />
            </output>
            <fault name="ValidationFault">
                <soap:fault name="ValidationFault"
use="literal" />
            </fault>
        </operation>
        <operation name="CertificateFormatValidate">
            <soap:operation
soapAction="http://www.roskazna.ru/eb/sign/types/sgv/Certifica
teFormatValidate" />
            <input>
                <soap:body use="literal" />
            </input>
            <output>
                <soap:body use="literal" />
            </output>
            <fault name="CFVFault">
```

```
                <soap:fault name="CFVFault" use="literal" />
            </fault>
        </operation>
    </binding>
    <binding name="SigningBinding" type="tns:SigningPortType">
        <soap:binding
transport="http://schemas.xmlsoap.org/soap/http" />
        <operation name="Sign">
            <soap:operation
soapAction="http://www.roskazna.ru/eb/sign/types/sgv/Sign" />
            <input>
                <soap:body use="literal" />
            </input>
            <output>
                <soap:body use="literal" />
            </output>
            <fault name="SigningFault">
                <soap:fault name="SigningFault" use="literal"
/>
            </fault>
        </operation>
        <operation name="Digest">
            <soap:operation
soapAction="http://www.roskazna.ru/eb/sign/types/sgv/Digest"
/>
            <input>
                <soap:body use="literal" />
            </input>
            <output>
                <soap:body use="literal" />
            </output>
            <fault name="DigestFault">
               <soap:fault name="DigestFault" use="literal" />
            </fault>
        </operation>
    </binding>
    <service name="SignatureValidationService">
        <port name="ValidationPort"
binding="tns:ValidationBinding">
            <soap:address
location="http://62.181.53.2:18080/tccs/SignatureValidationSer
vice" />
        </port>
    </service>
    <service name="SigningService">
        <port name="SigningPort" binding="tns:SigningBinding">
            <soap:address
location="http://62.181.53.2:18080/tccs/SigningService" />
        </port>
    </service>
</definitions>
```

Приложение 2. Описание типов

```
<?xml version="1.0" encoding="utf-8"?>
<!-- $Revision: 1.1 $ $Date: 2013/05/22 06:08:43 $-->
<xs:schema elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
targetNamespace="http://www.roskazna.ru/eb/sign/types/cryptose
rver">
    <xs:element name="Certificate" type="cst:Certificate" />
    <xs:element name="EmailAddress" type="cst:IA5String" />
    <xs:element name="LocalityName" type="cst:DirectoryString"
/>
    <xs:element name="OrganizationName"
type="cst:DirectoryString" />
    <xs:element name="OrganizationalUnitName"
type="cst:DirectoryString" />
    <xs:element name="CommonName" type="cst:DirectoryString"
/>
    <xs:element name="StateOrProvinceName"
type="cst:DirectoryString" />
    <xs:element name="unstructuredName"
type="cst:DirectoryString" />
    <xs:element name="unstructuredAddress"
type="cst:DirectoryString" />
    <xs:element name="Title" type="cst:DirectoryString" />
    <xs:element name="CountryName" type="cst:CountryName" />
    <xs:element name="RNSFSS" type="cst:numericOrPrintable" />
    <xs:element name="KPFSS" type="cst:numericOrPrintable" />
    <xs:element name="INN" type="cst:numericOrPrintable" />
    <xs:element name="SNILS" type="cst:numericOrPrintable" />
    <xs:element name="OGRN" type="cst:numericOrPrintable" />
    <xs:element name="OGRNIP" type="cst:numericOrPrintable" />
    <xs:element name="Pseudonym" type="cst:DirectoryString" />
    <xs:element name="DomainComponent" type="cst:IA5String" />
    <xs:element name="TelephoneNumber" type="cst:IA5String" />
    <xs:element name="LabeledURI" type="cst:IA5String" />
    <xs:element name="Surname" type="cst:DirectoryString" />
    <xs:element name="Description" type="cst:DirectoryString"
/>
    <xs:element name="BusinessCategory"
type="cst:DirectoryString" />
    <xs:element name="GivenName" type="cst:DirectoryString" />
    <xs:element name="PostalAddress" type="cst:PostalAddress"
/>
    <xs:element name="SerialNumber"
type="cst:numericOrPrintable" />
    <xs:element name="StreetAddress"
type="cst:DirectoryString" />
    <xs:element name="x509serialNumber" type="xs:string" />
    <xs:element name="RoleOccupant" type="cst:Name" />
    <xs:element name="generationQualifier"
type="cst:PrintableString" />
```

```
    <xs:element name="placeOfBirth" type="cst:DirectoryString"
/>
    <xs:element name="gender" type="cst:PrintableString" />
    <xs:element name="dateOfBirth" type="cst:GeneralizedTime"
/>
    <xs:element name="countryOfCitizenship"
type="cst:PrintableString" />
    <xs:element name="countryOfResidence"
type="cst:PrintableString" />
    <xs:element name="ANY-BROKEN" type="cst:ANY-UNKNOWN" />
    <xs:complexType name="PostalAddress">
        <xs:sequence>
            <xs:element maxOccurs="unbounded"
name="DirectoryString" type="cst:DirectoryString" />
        </xs:sequence>
    </xs:complexType>
    <xs:simpleType name="Version">
        <xs:restriction base="xs:integer" />
    </xs:simpleType>
    <xs:simpleType name="CertificateSerialNumber">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:element name="EMail" type="cst:EMail" />
    <xs:simpleType name="EMail">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:element name="IPAddress" type="cst:IPAddress" />
    <xs:simpleType name="IPAddress">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:simpleType name="DNSName">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:simpleType name="URI">
        <xs:restriction base="xs:anyURI" />
    </xs:simpleType>
    <xs:element name="BMPString" type="cst:BMPString" />
    <xs:simpleType name="BMPString">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:element name="UTF8String" type="cst:UTF8String" />
    <xs:simpleType name="UTF8String">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:element name="VisibleString" type="cst:VisibleString"
/>
    <xs:simpleType name="VisibleString">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:element name="PrintableString"
type="cst:PrintableString" />
    <xs:simpleType name="PrintableString">
```

```
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:element name="NumericString" type="cst:NumericString"
/>
    <xs:simpleType name="NumericString">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:element name="IA5String" type="cst:IA5String" />
    <xs:simpleType name="IA5String">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:element name="printable" type="cst:printable" />
    <xs:simpleType name="printable">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:element name="numeric" type="cst:numeric" />
    <xs:simpleType name="numeric">
        <xs:restriction base="xs:integer" />
    </xs:simpleType>
    <xs:element name="OBJECT_IDENTIFIER"
type="cst:OBJECT_IDENTIFIER" />
    <xs:simpleType name="OBJECT_IDENTIFIER">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:simpleType name="Critical">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:element name="ANY-UNKNOWN" type="cst:ANY-UNKNOWN" />
    <xs:simpleType name="ANY-UNKNOWN">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:simpleType name="KeyIdentifier">
        <xs:restriction base="xs:hexBinary" />
    </xs:simpleType>
    <xs:simpleType name="UniqueIdentifier">
        <xs:restriction base="xs:hexBinary" />
    </xs:simpleType>
    <xs:element name="BIT_STRING" type="cst:BIT_STRING" />
    <xs:simpleType name="BIT_STRING">
        <xs:restriction base="xs:hexBinary" />
    </xs:simpleType>
    <xs:element name="UTCTime" type="cst:UTCTime" />
    <xs:simpleType name="UTCTime">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:element name="GeneralizedTime"
type="cst:GeneralizedTime" />
    <xs:simpleType name="GeneralizedTime">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:complexType name="Certificate">
```

```
        <xs:sequence>
            <xs:element name="TBSCertificate"
type="cst:TBSCertificate" />
            <xs:element name="AlgorithmIdentifier"
type="cst:AlgorithmIdentifier" />
            <xs:element name="Signature" type="cst:BIT_STRING"
/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="TBSCertificate">
        <xs:sequence>
            <xs:element name="Version" type="cst:Version" />
            <xs:element name="CertificateSerialNumber"
type="cst:CertificateSerialNumber" />
            <xs:element name="Signature" type="cst:Signature"
/>
            <xs:element name="Issuer" type="cst:Name" />
            <xs:element name="Validity" type="cst:Validity" />
            <xs:element name="Subject" type="cst:Name" />
            <xs:element name="SubjectPublicKeyInfo"
type="cst:SubjectPublicKeyInfo" />
            <xs:element minOccurs="0"
name="IssuerUniqueIdentifier" type="cst:UniqueIdentifier" />
            <xs:element minOccurs="0"
name="SubjectUniqueIdentifier" type="cst:UniqueIdentifier" />
            <xs:element name="Extensions"
type="cst:Extensions" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="Signature">
        <xs:sequence>
            <xs:element name="AlgId"
type="cst:OBJECT_IDENTIFIER" />
            <xs:any minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="Name">
        <xs:sequence>
            <xs:element name="DistinguishedName"
type="cst:DistinguishedName" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="Time">
        <xs:choice>
            <xs:element name="UTCTime" type="cst:UTCTime" />
            <xs:element name="GeneralizedTime"
type="cst:GeneralizedTime" />
        </xs:choice>
    </xs:complexType>
    <xs:complexType name="Validity">
        <xs:sequence>
            <xs:element name="NotBefore" type="cst:Time" />
            <xs:element name="NotAfter" type="cst:Time" />
```

```
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="SubjectPublicKeyInfo">
        <xs:sequence>
            <xs:element name="PublicKeyAlgorithm"
type="cst:PublicKeyAlgorithm" />
            <xs:element name="SubjectPublicKey"
type="xs:hexBinary" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="PublicKeyAlgorithm">
        <xs:sequence>
            <xs:element name="AlgId"
type="cst:OBJECT_IDENTIFIER" />
            <xs:element name="gostR3410EC_CryptoPro"
type="cst:gostR3410EC_CryptoPro" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="gostR3410EC_CryptoPro">
        <xs:sequence>
            <xs:element minOccurs="2" maxOccurs="3"
name="OBJECT_IDENTIFIER" type="cst:OBJECT_IDENTIFIER" />
        </xs:sequence>
    </xs:complexType>
    <xs:simpleType name="ExtensionType">
        <xs:restriction base="cst:OBJECT_IDENTIFIER" />
    </xs:simpleType>
    <xs:complexType name="Extension">
        <xs:sequence>
            <xs:element name="ExtensionType"
type="cst:ExtensionType" />
            <xs:element minOccurs="0" name="Critical"
type="cst:Critical" />
            <xs:element name="extValue" type="cst:extValue" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="Extensions">
        <xs:sequence>
            <xs:element minOccurs="0" maxOccurs="unbounded"
name="Extension" type="cst:Extension" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AuthorityInfoAccess">
        <xs:sequence>
            <xs:element minOccurs="1" maxOccurs="unbounded"
name="AccessDescription" type="cst:AccessDescription" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="extValue" mixed="true">
        <xs:sequence>
            <xs:any />
        </xs:sequence>
```

```
    </xs:complexType>
    <xs:element name="AuthorityInfoAccess"
type="cst:AuthorityInfoAccess" />
    <xs:element name="AuthorityKeyIdentifier"
type="cst:AuthorityKeyIdentifier" />
    <xs:element name="BasicConstraints"
type="cst:BasicConstraints" />
    <xs:element name="CRLDistributionPoints"
type="cst:CRLDistributionPoints" />
    <xs:element name="ExtKeyUsage" type="cst:ExtKeyUsage" />
    <xs:element name="FreshestCRL"
type="cst:CRLDistributionPoints" />
    <xs:element name="KeyUsage" type="cst:KeyUsage" />
    <xs:element name="PrivateKeyUsagePeriod"
type="cst:PrivateKeyUsagePeriod" />
    <xs:element name="SubjectAltName" type="cst:GeneralNames"
/>
    <xs:element name="IssuerAltName" type="cst:GeneralNames"
/>
    <xs:element name="SubjectKeyIdentifier"
type="cst:SubjectKeyIdentifier" />
    <xs:element name="SMIMECapabilities"
type="cst:SMIMECapabilities" />
    <xs:element name="CertificatePolicies"
type="cst:CertificatePolicies" />
    <xs:element name="SubjectDirectoryAttributes"
type="cst:SubjectDirectoryAttributes" />
    <xs:simpleType name="SubjectKeyIdentifier">
        <xs:restriction base="xs:hexBinary" />
    </xs:simpleType>
    <xs:complexType name="AccessDescription">
        <xs:sequence>
            <xs:element name="AccessMethod"
type="cst:OBJECT_IDENTIFIER" />
            <xs:element name="AccessLocation"
type="cst:AccessLocation" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AccessLocation">
        <xs:sequence>
            <xs:element name="URI" type="cst:URI" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AuthorityKeyIdentifier">
        <xs:sequence>
            <xs:element minOccurs="0" name="KeyIdentifier"
type="cst:KeyIdentifier" />
            <xs:element minOccurs="0"
name="AuthorityCertIssuer" type="cst:GeneralNames" />
            <xs:element minOccurs="0"
name="AuthorityCertSerial" type="cst:CertificateSerialNumber"
/>
        </xs:sequence>
    </xs:complexType>
```

```
    <xs:complexType name="BasicConstraints">
        <xs:sequence>
            <xs:element minOccurs="0" name="IsCA"
type="xs:string" />
            <xs:element minOccurs="0" name="PathLenConstraint"
type="xs:integer" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="CRLDistributionPoints">
        <xs:sequence>
            <xs:element maxOccurs="unbounded"
name="DistributionPoint" type="cst:DistributionPoint" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="SET_OF_AnyValue">
        <xs:sequence>
            <xs:any maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="Attribute">
        <xs:sequence>
            <xs:element name="AttributeType"
type="cst:OBJECT_IDENTIFIER" />
            <xs:element name="Values"
type="cst:SET_OF_AnyValue" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="SubjectDirectoryAttributes">
        <xs:sequence>
            <xs:element maxOccurs="unbounded" name="Attribute"
type="cst:Attribute" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="SMIMECapabilities">
        <xs:sequence>
            <xs:element maxOccurs="unbounded"
name="AlgorithmIdentifier" type="cst:AlgorithmIdentifier" />
        </xs:sequence>
    </xs:complexType>
    <xs:simpleType name="KeyUsage">
        <xs:restriction base="xs:token">
            <xs:pattern value="[0-1]{0,}" />
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="ReasonFlags">
        <xs:restriction base="xs:token">
            <xs:pattern value="[0-1]{0,}" />
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="PrivateKeyUsagePeriod">
        <xs:sequence>
```

```
            <xs:element name="NotBefore"
type="cst:GeneralizedTime" />
            <xs:element name="NotAfter"
type="cst:GeneralizedTime" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AlgorithmIdentifier">
        <xs:sequence>
            <xs:element name="AlgId"
type="cst:OBJECT_IDENTIFIER" />
            <xs:any minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
    <xs:element name="gostR3410ECWithGostR3411_CryptoPro"
type="cst:gostR3410ECWithGostR3411_CryptoPro" />
    <xs:complexType name="gostR3410ECWithGostR3411_CryptoPro">
        <xs:sequence>
            <xs:element name="Inherit_GOST_R34.11_Crypto-
Pro_parameters" type="xs:string" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="GeneralNames">
        <xs:sequence>
            <xs:element maxOccurs="unbounded"
name="GeneralName" type="cst:GeneralName" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="DistinguishedName">
        <xs:sequence>
            <xs:element maxOccurs="unbounded"
name="RelativeDistinguishedName"
type="cst:RelativeDistinguishedName" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="RelativeDistinguishedName">
        <xs:sequence>
            <xs:element maxOccurs="unbounded"
name="AttributeTypeAndValue" type="cst:AttributeTypeAndValue"
/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AttributeTypeAndValue">
        <xs:sequence>
            <xs:element name="AttributeType"
type="cst:OBJECT_IDENTIFIER" />
            <xs:any />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="DirectoryString">
        <xs:choice>
            <xs:element name="NumericString"
type="cst:NumericString" />
```

```
            <xs:element name="IA5String" type="cst:IA5String"
/>
            <xs:element name="BMPString" type="cst:BMPString"
/>
            <xs:element name="VisibleString"
type="cst:VisibleString" />
            <xs:element name="PrintableString"
type="cst:PrintableString" />
            <xs:element name="UTF8String"
type="cst:UTF8String" />
        </xs:choice>
    </xs:complexType>
    <xs:complexType name="CountryName">
        <xs:choice>
            <xs:element name="iso-3166-code" type="cst:iso-
3166-code" />
            <xs:element name="x121-dcc-code" type="cst:x121-
dcc-code" />
        </xs:choice>
    </xs:complexType>
    <xs:simpleType name="iso-3166-code">
        <xs:restriction base="xs:string">
            <xs:minLength value="2" />
            <xs:maxLength value="3" />
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="x121-dcc-code">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="1" />
            <xs:maxInclusive value="999" />
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="numericOrPrintable">
        <xs:choice>
            <xs:element name="numeric" type="cst:numeric" />
            <xs:element name="printable" type="cst:printable"
/>
        </xs:choice>
    </xs:complexType>
    <xs:complexType name="unstructuredName">
        <xs:sequence>
            <xs:element name="DirectoryString"
type="cst:DirectoryString" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="DistributionPoint">
        <xs:sequence>
            <xs:element name="DistributionPointName"
type="cst:DistributionPointName" />
            <xs:element minOccurs="0" name="Reasons"
type="cst:ReasonFlags" />
            <xs:element minOccurs="0" name="CRLIssuer"
type="cst:GeneralNames" />
```

```
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="DistributionPointName">
        <xs:choice>
            <xs:element name="FullName"
type="cst:GeneralNames" />
            <xs:element name="NameRelativeToCrlIssuer"
type="cst:RelativeDistinguishedName" />
        </xs:choice>
    </xs:complexType>
    <xs:complexType name="FullName">
        <xs:sequence>
            <xs:element maxOccurs="unbounded"
name="GeneralName" type="cst:GeneralName" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AnotherNameValue" mixed="true">
        <xs:sequence>
            <xs:any minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AnotherName" mixed="true">
        <xs:sequence>
            <xs:element minOccurs="0" name="AnotherNameType"
type="cst:OBJECT_IDENTIFIER" />
            <xs:element minOccurs="0" name="AnotherNameValue"
type="cst:AnotherNameValue" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="GeneralName">
        <xs:choice>
            <xs:element name="EMail" type="cst:EMail" />
            <xs:element name="DNSName" type="cst:DNSName" />
            <xs:element name="DirectoryName" type="cst:Name"
/>
            <xs:element name="URI" type="cst:URI" />
            <xs:element name="IPAddress" type="cst:IPAddress"
/>
            <xs:element name="DistinguishedName"
type="cst:DistinguishedName" />
            <xs:element name="OtherName"
type="cst:AnotherName" />
        </xs:choice>
    </xs:complexType>
    <xs:element name="ServerAuth" type="cst:OBJECT_IDENTIFIER"
/>
    <xs:element name="ClientAuth" type="cst:OBJECT_IDENTIFIER"
/>
    <xs:element name="CodeSigning"
type="cst:OBJECT_IDENTIFIER" />
    <xs:element name="EmailProtection"
type="cst:OBJECT_IDENTIFIER" />
```

```
    <xs:element name="TimeStamping"
type="cst:OBJECT_IDENTIFIER" />
    <xs:element name="OCSPSigning"
type="cst:OBJECT_IDENTIFIER" />
    <xs:element name="DVCS" type="cst:OBJECT_IDENTIFIER" />
    <xs:element name="IPSec" type="cst:OBJECT_IDENTIFIER" />
    <xs:complexType name="ExtKeyUsage">
        <xs:sequence>
            <xs:any maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AccessMethod">
        <xs:choice>
            <xs:element name="OCSP"
type="cst:OBJECT_IDENTIFIER" />
            <xs:element name="CAIssuers"
type="cst:OBJECT_IDENTIFIER" />
            <xs:element name="TimeStamping"
type="cst:OBJECT_IDENTIFIER" />
            <xs:element name="DVCS"
type="cst:OBJECT_IDENTIFIER" />
            <xs:element name="CARepository"
type="cst:OBJECT_IDENTIFIER" />
        </xs:choice>
    </xs:complexType>
    <xs:complexType name="CertificatePolicies">
        <xs:sequence>
            <xs:element maxOccurs="unbounded"
name="PolicyInformation" type="cst:PolicyInformation" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="PolicyInformation">
        <xs:sequence>
            <xs:element name="PolicyIdentifier"
type="cst:OBJECT_IDENTIFIER" />
            <xs:element minOccurs="0" name="PolicyQualifiers"
type="cst:PolicyQualifiers" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="PolicyQualifiers">
        <xs:sequence>
            <xs:element maxOccurs="unbounded"
name="PolicyQualifierInfo" type="cst:PolicyQualifierInfo" />
        </xs:sequence>
    </xs:complexType>
    <xs:element name="UserNotice" type="cst:UserNotice" />
    <xs:complexType name="UserNotice">
        <xs:sequence>
            <xs:element minOccurs="0" name="NoticeReference"
type="cst:NoticeReference" />
            <xs:element minOccurs="0" name="ExplicitText"
type="cst:DirectoryString" />
        </xs:sequence>
```

```
    </xs:complexType>
    <xs:complexType name="NoticeReference">
        <xs:sequence>
            <xs:element name="Organization"
type="cst:DirectoryString" />
            <xs:element name="NoticeNumbers"
type="cst:NoticeNumbers" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="NoticeNumbers">
        <xs:sequence>
            <xs:element maxOccurs="unbounded" name="INTEGER"
type="xs:integer" />
        </xs:sequence>
    </xs:complexType>
    <xs:element name="CertificatePracticeStatementURI"
type="xs:anyURI" />
    <xs:complexType name="PolicyQualifierInfo">
        <xs:sequence>
            <xs:element name="PolicyQualifierId"
type="cst:OBJECT_IDENTIFIER" />
            <xs:any />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="NameConstraints">
        <xs:sequence>
            <xs:element minOccurs="0" name="PermittedSubtrees"
type="cst:GeneralSubtrees" />
            <xs:element minOccurs="0" name="ExcludedSubtrees"
type="cst:GeneralSubtrees" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="GeneralSubtrees">
        <xs:sequence>
            <xs:element maxOccurs="unbounded"
name="GeneralSubtree" type="cst:GeneralSubtree" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="GeneralSubtree">
        <xs:sequence>
            <xs:element name="Base" type="cst:GeneralName" />
            <xs:element minOccurs="0" name="Min"
type="xs:integer" />
            <xs:element minOccurs="0" name="Max"
type="xs:integer" />
        </xs:sequence>
    </xs:complexType>
    <xs:element name="SubjectSignTool"
type="cst:SubjectSignTool" />
    <xs:simpleType name="SubjectSignTool">
        <xs:restriction base="xs:string" />
    </xs:simpleType>
```

```
    <xs:element name="IssuerSignTool"
type="cst:IssuerSignTool" />
    <xs:complexType name="IssuerSignTool">
        <xs:sequence>
            <xs:element name="signTool" type="xs:string" />
            <xs:element name="cATool" type="xs:string" />
            <xs:element name="signToolCert" type="xs:string"
/>
            <xs:element name="caToolCert" type="xs:string" />
        </xs:sequence>
    </xs:complexType>
    <xs:simpleType name="notEmptyB64Binary">
        <xs:restriction base="xs:base64Binary">
            <xs:minLength value="4" />
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="FaultType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="internalError">
                <xs:annotation>
                    <xs:documentation>anything not covered by
other faultTypes</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="invalidRequestDataFormat">
                <xs:annotation>
                    <xs:documentation>covers only errors in
signed data, external data, data to be
signed</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="invalidXmlPartID">
                <xs:annotation>
                    <xs:documentation>corresponding xml part
ID not found in xml document in question</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="invalidActor">
                <xs:annotation>
                    <xs:documentation>wsse:Security element
with corresponding actor attribute not found in xml document
in question</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="FaultComment">
        <xs:restriction base="xs:string">
            <xs:maxLength value="200" />
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="SignatureStatus">
```

```
        <xs:restriction base="xs:string">
            <xs:enumeration value="unknown" />
            <xs:enumeration value="invalid" />
            <xs:enumeration value="valid" />
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="SignerIdentifier">
        <xs:choice>
            <xs:element name="IssuerAndSerial"
type="cst:IssuerAndSerial" />
            <xs:element name="KeyIdentifier"
type="cst:SubjectKeyIdentifier" />
        </xs:choice>
    </xs:complexType>
    <xs:complexType name="IssuerAndSerial">
        <xs:sequence>
            <xs:element name="Issuer" type="cst:Name" />
            <xs:element name="SerialNumber" type="xs:integer"
/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="SignatureRef">
        <xs:choice>
            <xs:element name="issuerAndSerial"
type="cst:SignerIdentifier" />
            <xs:element name="xmlID" type="xs:string" />
        </xs:choice>
    </xs:complexType>
    <xs:simpleType name="ValidationFaultType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="unknownDigestAlgorithm" />
            <xs:enumeration value="unknownSignatureAlgorithm"
/>
            <xs:enumeration value="signerCertificateNotFound"
/>
            <xs:enumeration
value="signerCertificateIssuerNotFound" />
            <xs:enumeration
value="signerCertificateSignatureInvalid" />
            <xs:enumeration
value="signerCertificateCRLNotFound" />
            <xs:enumeration value="signerCertificateExpired"
/>
            <xs:enumeration value="signerCertificateRevoked"
/>
            <xs:enumeration value="invalidDigestValue" />
            <xs:enumeration value="invalidSignatureValue" />
            <xs:enumeration value=”invalidSignatureTimeStamp”
/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="ValidationFaultInfo">
        <xs:sequence>
```

```
            <xs:element name="type"
type="cst:ValidationFaultType" />
            <xs:element name="comment" type="cst:FaultComment"
/>
        </xs:sequence>
    </xs:complexType>
    <xs:simpleType name="GlobalStatus">
        <xs:restriction base="xs:string">
            <xs:enumeration value="unknown" />
            <xs:enumeration value="invalid" />
            <xs:enumeration value="partiallyValid" />
            <xs:enumeration value="valid" />
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="GmtDateTime">
        <xs:restriction base="xs:string">
            <xs:pattern value="[0-9]{1,2}.[0-9]{1,2}.[0-9]{4}
[0-9]{1,2}:[0-9]{1,2}:[0-9]{1,2} UTC" />
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="SignerCertInfo">
        <xs:sequence>
            <xs:element name="Certificate"
type="cst:Certificate" />
            <xs:any minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="SignatureInfos">
        <xs:annotation>
            <xs:documentation>
                SignatureInfo::SignatureRef field is not
inteded to be a search key for corresponding CMS SignerInfo or
xmldsig signedInfo.
                SignatureInfo entries are listed in this
sequence just in same oreder as CMS SignerInfo-s or xmldsig
signedInfo-s in verified data.
                In case of incapsulated signatures, outermost
SignatureInfos listed first, innermost listed last.
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="SignatureInfo"
type="cst:SignatureInfo" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="SignatureInfo">
        <xs:sequence>
            <xs:element name="reference"
type="cst:SignatureRef" />
            <xs:element name="status"
type="cst:SignatureStatus" />
            <xs:element name="failInfo"
type="cst:ValidationFaultInfo" minOccurs="0" />
```

```
            <xs:element name="signerCertInfo"
type="cst:SignerCertInfo" minOccurs="0" />
            <xs:element name="validationDate"
type="cst:GeneralizedTime" />
            <xs:element name="firstTimeStamp"
type="cst:GeneralizedTime" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:simpleType name="httpURI">
        <xs:restriction base="xs:string">
            <xs:pattern value="http://.*" />
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="signatureType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="cms" />
            <xs:enumeration value="xmldsig" />
            <xs:enumeration value="wssecurity" />
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

Приложение 3. Примеры взаимодействия с веб-сервисами

validation_request_wssecurity.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:ValidationRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
>
    <tccs:signedData>PHNvYXBlbn .......
bnZlbG9wZT4K</tccs:signedData>
</tccs:ValidationRequestType>
```

signing_response_wssecurity.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:SigningResponseType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">PHNv
Y  ... bG9wZT4K</tccs:SigningResponseType>
```

signing_response_cms_detached.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:SigningResponseType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">MIIM
rQY .... V6HFCujrb+</tccs:SigningResponseType>
```

signing_response_cms.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:SigningResponseType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">MIAG
CSq .....V6HFCujrb+AAAAAAAA</tccs:SigningResponseType>
```

signing_request_wssecurity.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:SigningRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
>

<tccs:data>PHNvYXBlbnY6RW52ZWxvcGUgeG1sbnM6c29hcGVudj0iaHR0cDo
vL3NjaGVtYXMueG1sc29hcC5vcmcvc29hcC9lbnZlbG9wZS8iIAogICAgICAgI
HhtbG5zOnhzZD0iaHR0cDovL3d3dy53My5vcmcvMjAwMS9YTUxTY2hlbWEiIAo
gICAgICAgICAgICAgICAgeG1sbnM6eHNpPSJodHRwOi8vd3d3LnczLm9yZy8yM
DAxL1hNTFNjaGVtYS1pbnN0YW5jZSIgCiAgICAgICAgICAgICAgICAgICAgICA
gIHhtbG5zOlNPQVAtRU5DPSJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy9zb
2FwL2VuY29kaW5nLyI+CiAgPHNvYXBlbnY6SGVhZGVyLz4KPHNvYXBlbnY6Qm9
keT4KYXBwbGljYXRpb24gc3BlY2lmaWMgZGF0YS9jb250ZW50Cjwvc29hcGVud
jpCb2R5Pgo8L3NvYXBlbnY6RW52ZWxvcGU+Cg==</tccs:data>
    <tccs:signatureType>wssecurity</tccs:signatureType>
</tccs:SigningRequestType>
```

signing_request_cms_detached.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:SigningRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
>
    <tccs:data>UEsDBBQ ...
gAAAAALAAsAwQIAAOUjAAAAAA==</tccs:data>
    <tccs:signatureType>cms</tccs:signatureType>
    <tccs:detached>true<tccs:detached>
</tccs:SigningRequestType>
```

signing_request_cms.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:SigningRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
>
    <tccs:data>UEsDBBQA .... AAsAwQIAAOUjAAAAAA==</tccs:data>
    <tccs:signatureType>cms</tccs:signatureType>
</tccs:SigningRequestType>
```

validation_request_cms_detached.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:ValidationRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
>
    <tccs:signedData>MIIMrQYJKoZ ...
CnV6HFCujrb+</tccs:signedData>
    <tccs:externalData>UEsDBBQABgAI
.....AOUjAAAAAA==<tccs:externalData>
</tccs:ValidationRequestType>
```

validation_request_cms.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:ValidationRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
>
    <tccs:signedData>MIAGCSq ...
HFCujrb+AAAAAAAA</tccs:signedData>
</tccs:ValidationRequestType>
```

validation_response_partiallyValid.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:ValidationResponseType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
>
    <tccs:gmtDateTime>9.5.2013 9:9:9 UTC</tccs:gmtDateTime>
    <tccs:globalStatus>partiallyValid</tccs:globalStatus>
```

```
    <tccs:SignatureInfos>
        <cst:SignatureInfo>
            <cst:reference>
                <cst:xmlID></cst:xmlID>
            </cst:reference>
            <cst:status>unknown</cst:status>
            <cst:failInfo>
                <cst:type>signerCertificateNotFound</cst:type>
                <cst:comment>we can't say nothing on something
that we really don't know</cst:comment>
            </cst:failInfo>
        </cst:SignatureInfo>
        <cst:SignatureInfo>
            <cst:reference>

<cst:issuerAndSerial><cst:IssuerAndSerial><cst:Issuer><cst:Dis
tinguishedName><cst:RelativeDistinguishedName><cst:AttributeTy
peAndValue><cst:AttributeType>1.2.840.113549.1.9.1</cst:Attrib
uteType><cst:EmailAddress>uuc_fk@roskazna.ru</cst:EmailAddress
></cst:AttributeTypeAndValue></cst:RelativeDistinguishedName><
cst:RelativeDistinguishedName><cst:AttributeTypeAndValue><cst:
AttributeType>2.5.4.8</cst:AttributeType><cst:StateOrProvinceN
ame><cst:UTF8String>77 г.
Москва</cst:UTF8String></cst:StateOrProvinceName></cst:Attribu
teTypeAndValue></cst:RelativeDistinguishedName><cst:RelativeDi
stinguishedName><cst:AttributeTypeAndValue><cst:AttributeType>
1.2.643.3.131.1.1</cst:AttributeType><cst:INN><cst:numeric>007
710568760</cst:numeric></cst:INN></cst:AttributeTypeAndValue><
/cst:RelativeDistinguishedName><cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue><cst:AttributeType>1.2.643.100.1</c
st:AttributeType><cst:OGRN><cst:numeric>1047797019830</cst:num
eric></cst:OGRN></cst:AttributeTypeAndValue></cst:RelativeDist
inguishedName><cst:RelativeDistinguishedName><cst:AttributeTyp
eAndValue><cst:AttributeType>2.5.4.9</cst:AttributeType><cst:S
treetAddress><cst:UTF8String>улица Ильинка, дом
7</cst:UTF8String></cst:StreetAddress></cst:AttributeTypeAndVa
lue></cst:RelativeDistinguishedName><cst:RelativeDistinguished
Name><cst:AttributeTypeAndValue><cst:AttributeType>2.5.4.7</cs
t:AttributeType><cst:LocalityName><cst:UTF8String>Москва</cst:
UTF8String></cst:LocalityName></cst:AttributeTypeAndValue></cs
t:RelativeDistinguishedName><cst:RelativeDistinguishedName><cs
t:AttributeTypeAndValue><cst:AttributeType>2.5.4.6</cst:Attrib
uteType><cst:CountryName><cst:iso-3166-code>RU</cst:iso-3166-
code></cst:CountryName></cst:AttributeTypeAndValue></cst:Relat
iveDistinguishedName><cst:RelativeDistinguishedName><cst:Attri
buteTypeAndValue><cst:AttributeType>2.5.4.10</cst:AttributeTyp
e><cst:OrganizationName><cst:UTF8String>Федеральное
казначейство</cst:UTF8String></cst:OrganizationName></cst:Attr
ibuteTypeAndValue></cst:RelativeDistinguishedName><cst:Relativ
eDistinguishedName><cst:AttributeTypeAndValue><cst:AttributeTy
pe>2.5.4.3</cst:AttributeType><cst:CommonName><cst:UTF8String>
Уполномоченный удостоверяющий центр Федерального
казначейства</cst:UTF8String></cst:CommonName></cst:AttributeT
ypeAndValue></cst:RelativeDistinguishedName></cst:Distinguishe
dName></cst:Issuer><cst:SerialNumber>1030</cst:SerialNumber></
cst:IssuerAndSerial></cst:issuerAndSerial>
            </cst:reference>
            <cst:status>valid</cst:status>
            <cst:signerCertInfo>
```

```
<cst:Certificate><cst:TBSCertificate><cst:Version>2</cst:Versi
on><cst:CertificateSerialNumber>1030</cst:CertificateSerialNum
ber><cst:Signature><cst:AlgId>1.2.643.2.2.3</cst:AlgId></cst:S
ignature><cst:Issuer><cst:DistinguishedName><cst:RelativeDisti
nguishedName><cst:AttributeTypeAndValue><cst:AttributeType>1.2
.840.113549.1.9.1</cst:AttributeType><cst:EmailAddress>uuc_fk@
roskazna.ru</cst:EmailAddress></cst:AttributeTypeAndValue></cs
t:RelativeDistinguishedName><cst:RelativeDistinguishedName><cs
t:AttributeTypeAndValue><cst:AttributeType>2.5.4.8</cst:Attrib
uteType><cst:StateOrProvinceName><cst:UTF8String>77 г.
Москва</cst:UTF8String></cst:StateOrProvinceName></cst:Attribu
teTypeAndValue></cst:RelativeDistinguishedName><cst:RelativeDi
stinguishedName><cst:AttributeTypeAndValue><cst:AttributeType>
1.2.643.3.131.1.1</cst:AttributeType><cst:INN><cst:numeric>007
710568760</cst:numeric></cst:INN></cst:AttributeTypeAndValue><
/cst:RelativeDistinguishedName><cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue><cst:AttributeType>1.2.643.100.1</c
st:AttributeType><cst:OGRN><cst:numeric>1047797019830</cst:num
eric></cst:OGRN></cst:AttributeTypeAndValue></cst:RelativeDist
inguishedName><cst:RelativeDistinguishedName><cst:AttributeTyp
eAndValue><cst:AttributeType>2.5.4.9</cst:AttributeType><cst:S
treetAddress><cst:UTF8String>улица Ильинка, дом
7</cst:UTF8String></cst:StreetAddress></cst:AttributeTypeAndVa
lue></cst:RelativeDistinguishedName><cst:RelativeDistinguished
Name><cst:AttributeTypeAndValue><cst:AttributeType>2.5.4.7</cs
t:AttributeType><cst:LocalityName><cst:UTF8String>Москва</cst:
UTF8String></cst:LocalityName></cst:AttributeTypeAndValue></cs
t:RelativeDistinguishedName><cst:RelativeDistinguishedName><cs
t:AttributeTypeAndValue><cst:AttributeType>2.5.4.6</cst:Attrib
uteType><cst:CountryName><cst:iso-3166-code>RU</cst:iso-3166-
code></cst:CountryName></cst:AttributeTypeAndValue></cst:Relat
iveDistinguishedName><cst:RelativeDistinguishedName><cst:Attri
buteTypeAndValue><cst:AttributeType>2.5.4.10</cst:AttributeTyp
e><cst:OrganizationName><cst:UTF8String>Федеральное
казначейство</cst:UTF8String></cst:OrganizationName></cst:Attr
ibuteTypeAndValue></cst:RelativeDistinguishedName><cst:Relativ
eDistinguishedName><cst:AttributeTypeAndValue><cst:AttributeTy
pe>2.5.4.3</cst:AttributeType><cst:CommonName><cst:UTF8String>
Уполномоченный удостоверяющий центр Федерального
казначейства</cst:UTF8String></cst:CommonName></cst:AttributeT
ypeAndValue></cst:RelativeDistinguishedName></cst:Distinguishe
dName></cst:Issuer><cst:Validity><cst:NotBefore><cst:UTCTime>1
5.2.2013 9:44:58
UTC</cst:UTCTime></cst:NotBefore><cst:NotAfter><cst:UTCTime>15
.2.2014 9:44:58
UTC</cst:UTCTime></cst:NotAfter></cst:Validity><cst:Subject><c
st:DistinguishedName><cst:RelativeDistinguishedName><cst:Attri
buteTypeAndValue><cst:AttributeType>2.5.4.42</cst:AttributeTyp
e><cst:GivenName><cst:UTF8String>Иван
Иванович</cst:UTF8String></cst:GivenName></cst:AttributeTypeAn
dValue></cst:RelativeDistinguishedName><cst:RelativeDistinguis
hedName><cst:AttributeTypeAndValue><cst:AttributeType>2.5.4.4<
/cst:AttributeType><cst:Surname><cst:UTF8String>Иванов</cst:UT
F8String></cst:Surname></cst:AttributeTypeAndValue></cst:Relat
iveDistinguishedName><cst:RelativeDistinguishedName><cst:Attri
buteTypeAndValue><cst:AttributeType>1.2.643.3.131.1.1</cst:Att
ributeType><cst:INN><cst:numeric>123456789012</cst:numeric></c
st:INN></cst:AttributeTypeAndValue></cst:RelativeDistinguished
Name><cst:RelativeDistinguishedName><cst:AttributeTypeAndValue
><cst:AttributeType>1.2.643.100.3</cst:AttributeType><cst:SNIL
S><cst:numeric>12345678901</cst:numeric></cst:SNILS></cst:Attr
ibuteTypeAndValue></cst:RelativeDistinguishedName><cst:Relativ
eDistinguishedName><cst:AttributeTypeAndValue><cst:AttributeTy
```

```
pe>1.2.643.100.5</cst:AttributeType><cst:OGRNIP><cst:printable
>123456789012345</cst:printable></cst:OGRNIP></cst:AttributeTy
peAndValue></cst:RelativeDistinguishedName><cst:RelativeDistin
guishedName><cst:AttributeTypeAndValue><cst:AttributeType>2.5.
4.6</cst:AttributeType><cst:CountryName><cst:iso-3166-
code>RU</cst:iso-3166-
code></cst:CountryName></cst:AttributeTypeAndValue></cst:Relat
iveDistinguishedName><cst:RelativeDistinguishedName><cst:Attri
buteTypeAndValue><cst:AttributeType>2.5.4.8</cst:AttributeType
><cst:StateOrProvinceName><cst:UTF8String>69 Тверская
область</cst:UTF8String></cst:StateOrProvinceName></cst:Attrib
uteTypeAndValue></cst:RelativeDistinguishedName><cst:RelativeD
istinguishedName><cst:AttributeTypeAndValue><cst:AttributeType
>2.5.4.7</cst:AttributeType><cst:LocalityName><cst:UTF8String>
Нижний
Волочек</cst:UTF8String></cst:LocalityName></cst:AttributeType
AndValue></cst:RelativeDistinguishedName><cst:RelativeDistingu
ishedName><cst:AttributeTypeAndValue><cst:AttributeType>2.5.4.
3</cst:AttributeType><cst:CommonName><cst:UTF8String>ИП</cst:U
TF8String></cst:CommonName></cst:AttributeTypeAndValue></cst:R
elativeDistinguishedName></cst:DistinguishedName></cst:Subject
><cst:SubjectPublicKeyInfo><cst:PublicKeyAlgorithm><cst:AlgId>
1.2.643.2.2.19</cst:AlgId><cst:gostR3410EC_CryptoPro><cst:OBJE
CT_IDENTIFIER>1.2.643.2.2.36.0</cst:OBJECT_IDENTIFIER><cst:OBJ
ECT_IDENTIFIER>1.2.643.2.2.30.1</cst:OBJECT_IDENTIFIER></cst:g
ostR3410EC_CryptoPro></cst:PublicKeyAlgorithm><cst:SubjectPubl
icKey>0440CE875B0B1B448554CB2C904284BCAE581F7587D99FF4C991905D
EA8EE3DD21FC96670E90A80B01E77A8F6BE768248BCDC218A7B039555C7B18
0499011CB8C935</cst:SubjectPublicKey></cst:SubjectPublicKeyInf
o><cst:Extensions><cst:Extension><cst:ExtensionType>1.2.643.10
0.111</cst:ExtensionType><cst:Critical>{FALSE}</cst:Critical><
cst:extValue><cst:SubjectSignTool>"КриптоПро CSP" (версия
3.6)</cst:SubjectSignTool></cst:extValue></cst:Extension><cst:
Extension><cst:ExtensionType>1.2.643.100.112</cst:ExtensionTyp
e><cst:Critical>{FALSE}</cst:Critical><cst:extValue><cst:Issue
rSignTool><cst:signTool>"КриптоПро CSP" (версия
3.6)</cst:signTool><cst:cATool>Сертификат соответствия №
СФ/121-1857 от
17.06.2012</cst:cATool><cst:signToolCert>"Программно-
аппаратный комплекс "Юнисерт-ГОСТ". версия
3"</cst:signToolCert><cst:caToolCert>Сертификат соответствия №
СФ/000-0000 от
00.00.0000</cst:caToolCert></cst:IssuerSignTool></cst:extValue
></cst:Extension><cst:Extension><cst:ExtensionType>2.5.29.32</
cst:ExtensionType><cst:Critical>{FALSE}</cst:Critical><cst:ext
Value><cst:CertificatePolicies><cst:PolicyInformation><cst:Pol
icyIdentifier>1.2.643.100.113.1</cst:PolicyIdentifier></cst:Po
licyInformation><cst:PolicyInformation><cst:PolicyIdentifier>1
.2.643.100.113.2</cst:PolicyIdentifier></cst:PolicyInformation
></cst:CertificatePolicies></cst:extValue></cst:Extension><cst
:Extension><cst:ExtensionType>2.5.29.15</cst:ExtensionType><cs
t:Critical>{TRUE}</cst:Critical><cst:extValue><cst:KeyUsage>1<
/cst:KeyUsage></cst:extValue></cst:Extension><cst:Extension><c
st:ExtensionType>2.5.29.37</cst:ExtensionType><cst:Critical>{T
RUE}</cst:Critical><cst:extValue><cst:ExtKeyUsage><cst:EmailPr
otection>1.3.6.1.5.5.7.3.4</cst:EmailProtection></cst:ExtKeyUs
age></cst:extValue></cst:Extension><cst:Extension><cst:Extensi
onType>2.5.29.35</cst:ExtensionType><cst:Critical>{FALSE}</cst
:Critical><cst:extValue><cst:AuthorityKeyIdentifier><cst:KeyId
entifier>F9686180B9F033C9D5AAD3D2B4692BB34D829372</cst:KeyIden
tifier><cst:AuthorityCertIssuer><cst:GeneralName><cst:Director
yName><cst:DistinguishedName><cst:RelativeDistinguishedName><c
st:AttributeTypeAndValue><cst:AttributeType>1.2.840.113549.1.9
.1</cst:AttributeType><cst:EmailAddress>uuc_fk@roskazna.ru</cs
```

```
t:EmailAddress></cst:AttributeTypeAndValue></cst:RelativeDisti
nguishedName><cst:RelativeDistinguishedName><cst:AttributeType
AndValue><cst:AttributeType>2.5.4.8</cst:AttributeType><cst:St
ateOrProvinceName><cst:UTF8String>77 г.
Москва</cst:UTF8String></cst:StateOrProvinceName></cst:Attribu
teTypeAndValue></cst:RelativeDistinguishedName><cst:RelativeDi
stinguishedName><cst:AttributeTypeAndValue><cst:AttributeType>
1.2.643.3.131.1.1</cst:AttributeType><cst:INN><cst:numeric>007
710568760</cst:numeric></cst:INN></cst:AttributeTypeAndValue><
/cst:RelativeDistinguishedName><cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue><cst:AttributeType>1.2.643.100.1</c
st:AttributeType><cst:OGRN><cst:numeric>1047797019830</cst:num
eric></cst:OGRN></cst:AttributeTypeAndValue></cst:RelativeDist
inguishedName><cst:RelativeDistinguishedName><cst:AttributeTyp
eAndValue><cst:AttributeType>2.5.4.9</cst:AttributeType><cst:S
treetAddress><cst:UTF8String>улица Ильинка, дом
7</cst:UTF8String></cst:StreetAddress></cst:AttributeTypeAndVa
lue></cst:RelativeDistinguishedName><cst:RelativeDistinguished
Name><cst:AttributeTypeAndValue><cst:AttributeType>2.5.4.7</cs
t:AttributeType><cst:LocalityName><cst:UTF8String>Москва</cst:
UTF8String></cst:LocalityName></cst:AttributeTypeAndValue></cs
t:RelativeDistinguishedName><cst:RelativeDistinguishedName><cs
t:AttributeTypeAndValue><cst:AttributeType>2.5.4.6</cst:Attrib
uteType><cst:CountryName><cst:iso-3166-code>RU</cst:iso-3166-
code></cst:CountryName></cst:AttributeTypeAndValue></cst:Relat
iveDistinguishedName><cst:RelativeDistinguishedName><cst:Attri
buteTypeAndValue><cst:AttributeType>2.5.4.10</cst:AttributeTyp
e><cst:OrganizationName><cst:UTF8String>Федеральное
казначейство</cst:UTF8String></cst:OrganizationName></cst:Attr
ibuteTypeAndValue></cst:RelativeDistinguishedName><cst:Relativ
eDistinguishedName><cst:AttributeTypeAndValue><cst:AttributeTy
pe>2.5.4.3</cst:AttributeType><cst:CommonName><cst:UTF8String>
Уполномоченный удостоверяющий центр Федерального
казначейства</cst:UTF8String></cst:CommonName></cst:AttributeT
ypeAndValue></cst:RelativeDistinguishedName></cst:Distinguishe
dName></cst:DirectoryName></cst:GeneralName></cst:AuthorityCer
tIssuer><cst:AuthorityCertSerial>1</cst:AuthorityCertSerial></
cst:AuthorityKeyIdentifier></cst:extValue></cst:Extension><cst
:Extension><cst:ExtensionType>2.5.29.31</cst:ExtensionType><cs
t:Critical>{FALSE}</cst:Critical><cst:extValue><cst:CRLDistrib
utionPoints><cst:DistributionPoint><cst:DistributionPointName>
<cst:FullName><cst:GeneralName><cst:URI>ht
tp://crl.roskazna.ru/crl/UUC_FK_1.crl</cst:URI></cst:GeneralNa
me></cst:FullName></cst:DistributionPointName></cst:Distributi
onPoint><cst:DistributionPoint><cst:DistributionPointName><cst
:FullName><cst:GeneralName><cst:URI>http://crl.fsfk.local/crl/
UUC_FK_1.crl</cst:URI></cst:GeneralName></cst:FullName></cst:D
istributionPointName></cst:DistributionPoint></cst:CRLDistribu
tionPoints></cst:extValue></cst:Extension><cst:Extension><cst:
ExtensionType>2.5.29.14</cst:ExtensionType><cst:Critical>{FALS
E}</cst:Critical><cst:extValue><cst:SubjectKeyIdentifier>B397B
87E6A53C3DDB546C325D5B797A1CEBE824F</cst:SubjectKeyIdentifier>
</cst:extValue></cst:Extension></cst:Extensions></cst:TBSCerti
ficate><cst:AlgorithmIdentifier><cst:AlgId>1.2.643.2.2.3</cst:
AlgId></cst:AlgorithmIdentifier><cst:BIT_STRING>83DD1326127597
E46A17A9D667D346541507E21EF3937968958C323C7CD87ED435030A237FA9
099BFCA5B3CA2463A16F4F927E67FCD82EB476F60CE68F985997</cst:BIT_
STRING></cst:Certificate>
            </cst:signerCertInfo>
        </cst:SignatureInfo>
    </tccs:SignatureInfos>
</tccs:ValidationResponseType>
```

validation_response_valid.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:ValidationResponseType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
>
    <tccs:gmtDateTime>9.5.2013 9:9:9 UTC</tccs:gmtDateTime>
    <tccs:globalStatus>valid</tccs:globalStatus>
    <tccs:SignatureInfos>
        <cst:SignatureInfo>
            <cst:reference>

<cst:issuerAndSerial><cst:IssuerAndSerial><cst:Issuer><cst:Dis
tinguishedName><cst:RelativeDistinguishedName><cst:AttributeTy
peAndValue><cst:AttributeType>1.2.840.113549.1.9.1</cst:Attrib
uteType><cst:EmailAddress>uuc_fk@roskazna.ru</cst:EmailAddress
></cst:AttributeTypeAndValue></cst:RelativeDistinguishedName><
cst:RelativeDistinguishedName><cst:AttributeTypeAndValue><cst:
AttributeType>2.5.4.8</cst:AttributeType><cst:StateOrProvinceN
ame><cst:UTF8String>77 г.
Москва</cst:UTF8String></cst:StateOrProvinceName></cst:Attribu
teTypeAndValue></cst:RelativeDistinguishedName><cst:RelativeDi
stinguishedName><cst:AttributeTypeAndValue><cst:AttributeType>
1.2.643.3.131.1.1</cst:AttributeType><cst:INN><cst:numeric>007
710568760</cst:numeric></cst:INN></cst:AttributeTypeAndValue><
/cst:RelativeDistinguishedName><cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue><cst:AttributeType>1.2.643.100.1</c
st:AttributeType><cst:OGRN><cst:numeric>1047797019830</cst:num
eric></cst:OGRN></cst:AttributeTypeAndValue></cst:RelativeDist
inguishedName><cst:RelativeDistinguishedName><cst:AttributeTyp
eAndValue><cst:AttributeType>2.5.4.9</cst:AttributeType><cst:S
treetAddress><cst:UTF8String>улица Ильинка, дом
7</cst:UTF8String></cst:StreetAddress></cst:AttributeTypeAndVa
lue></cst:RelativeDistinguishedName><cst:RelativeDistinguished
Name><cst:AttributeTypeAndValue><cst:AttributeType>2.5.4.7</cs
t:AttributeType><cst:LocalityName><cst:UTF8String>Москва</cst:
UTF8String></cst:LocalityName></cst:AttributeTypeAndValue></cs
t:RelativeDistinguishedName><cst:RelativeDistinguishedName><cs
t:AttributeTypeAndValue><cst:AttributeType>2.5.4.6</cst:Attrib
uteType><cst:CountryName><cst:iso-3166-code>RU</cst:iso-3166-
code></cst:CountryName></cst:AttributeTypeAndValue></cst:Relat
iveDistinguishedName><cst:RelativeDistinguishedName><cst:Attri
buteTypeAndValue><cst:AttributeType>2.5.4.10</cst:AttributeTyp
e><cst:OrganizationName><cst:UTF8String>Федеральное
казначейство</cst:UTF8String></cst:OrganizationName></cst:Attr
ibuteTypeAndValue></cst:RelativeDistinguishedName><cst:Relativ
eDistinguishedName><cst:AttributeTypeAndValue><cst:AttributeTy
pe>2.5.4.3</cst:AttributeType><cst:CommonName><cst:UTF8String>
Уполномоченный удостоверяющий центр Федерального
казначейства</cst:UTF8String></cst:CommonName></cst:AttributeT
ypeAndValue></cst:RelativeDistinguishedName></cst:Distinguishe
dName></cst:Issuer><cst:SerialNumber>1030</cst:SerialNumber></
cst:IssuerAndSerial></cst:issuerAndSerial>
            </cst:reference>
            <cst:status>valid</cst:status>
            <cst:signerCertInfo>

<cst:Certificate><cst:TBSCertificate><cst:Version>2</cst:Versi
on><cst:CertificateSerialNumber>1030</cst:CertificateSerialNum
ber><cst:Signature><cst:AlgId>1.2.643.2.2.3</cst:AlgId></cst:S
```

```
ignature><cst:Issuer><cst:DistinguishedName><cst:RelativeDisti
nguishedName><cst:AttributeTypeAndValue><cst:AttributeType>1.2
.840.113549.1.9.1</cst:AttributeType><cst:EmailAddress>uuc_fk@
roskazna.ru</cst:EmailAddress></cst:AttributeTypeAndValue></cs
t:RelativeDistinguishedName><cst:RelativeDistinguishedName><cs
t:AttributeTypeAndValue><cst:AttributeType>2.5.4.8</cst:Attrib
uteType><cst:StateOrProvinceName><cst:UTF8String>77 г.
Москва</cst:UTF8String></cst:StateOrProvinceName></cst:Attribu
teTypeAndValue></cst:RelativeDistinguishedName><cst:RelativeDi
stinguishedName><cst:AttributeTypeAndValue><cst:AttributeType>
1.2.643.3.131.1.1</cst:AttributeType><cst:INN><cst:numeric>007
710568760</cst:numeric></cst:INN></cst:AttributeTypeAndValue><
/cst:RelativeDistinguishedName><cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue><cst:AttributeType>1.2.643.100.1</c
st:AttributeType><cst:OGRN><cst:numeric>1047797019830</cst:num
eric></cst:OGRN></cst:AttributeTypeAndValue></cst:RelativeDist
inguishedName><cst:RelativeDistinguishedName><cst:AttributeTyp
eAndValue><cst:AttributeType>2.5.4.9</cst:AttributeType><cst:S
treetAddress><cst:UTF8String>улица Ильинка, дом
7</cst:UTF8String></cst:StreetAddress></cst:AttributeTypeAndVa
lue></cst:RelativeDistinguishedName><cst:RelativeDistinguished
Name><cst:AttributeTypeAndValue><cst:AttributeType>2.5.4.7</cs
t:AttributeType><cst:LocalityName><cst:UTF8String>Москва</cst:
UTF8String></cst:LocalityName></cst:AttributeTypeAndValue></cs
t:RelativeDistinguishedName><cst:RelativeDistinguishedName><cs
t:AttributeTypeAndValue><cst:AttributeType>2.5.4.6</cst:Attrib
uteType><cst:CountryName><cst:iso-3166-code>RU</cst:iso-3166-
code></cst:CountryName></cst:AttributeTypeAndValue></cst:Relat
iveDistinguishedName><cst:RelativeDistinguishedName><cst:Attri
buteTypeAndValue><cst:AttributeType>2.5.4.10</cst:AttributeTyp
e><cst:OrganizationName><cst:UTF8String>Федеральное
казначейство</cst:UTF8String></cst:OrganizationName></cst:Attr
ibuteTypeAndValue></cst:RelativeDistinguishedName><cst:Relativ
eDistinguishedName><cst:AttributeTypeAndValue><cst:AttributeTy
pe>2.5.4.3</cst:AttributeType><cst:CommonName><cst:UTF8String>
Уполномоченный удостоверяющий центр Федерального
казначейства</cst:UTF8String></cst:CommonName></cst:AttributeT
ypeAndValue></cst:RelativeDistinguishedName></cst:Distinguishe
dName></cst:Issuer><cst:Validity><cst:NotBefore><cst:UTCTime>1
5.2.2013 9:44:58
UTC</cst:UTCTime></cst:NotBefore><cst:NotAfter><cst:UTCTime>15
.2.2014 9:44:58
UTC</cst:UTCTime></cst:NotAfter></cst:Validity><cst:Subject><c
st:DistinguishedName><cst:RelativeDistinguishedName><cst:Attri
buteTypeAndValue><cst:AttributeType>2.5.4.42</cst:AttributeTyp
e><cst:GivenName><cst:UTF8String>Иван
Иванович</cst:UTF8String></cst:GivenName></cst:AttributeTypeAn
dValue></cst:RelativeDistinguishedName><cst:RelativeDistinguis
hedName><cst:AttributeTypeAndValue><cst:AttributeType>2.5.4.4<
/cst:AttributeType><cst:Surname><cst:UTF8String>Иванов</cst:UT
F8String></cst:Surname></cst:AttributeTypeAndValue></cst:Relat
iveDistinguishedName><cst:RelativeDistinguishedName><cst:Attri
buteTypeAndValue><cst:AttributeType>1.2.643.3.131.1.1</cst:Att
ributeType><cst:INN><cst:numeric>123456789012</cst:numeric></c
st:INN></cst:AttributeTypeAndValue></cst:RelativeDistinguished
Name><cst:RelativeDistinguishedName><cst:AttributeTypeAndValue
><cst:AttributeType>1.2.643.100.3</cst:AttributeType><cst:SNIL
S><cst:numeric>12345678901</cst:numeric></cst:SNILS></cst:Attr
ibuteTypeAndValue></cst:RelativeDistinguishedName><cst:Relativ
eDistinguishedName><cst:AttributeTypeAndValue><cst:AttributeTy
pe>1.2.643.100.5</cst:AttributeType><cst:OGRNIP><cst:printable
>123456789012345</cst:printable></cst:OGRNIP></cst:AttributeTy
peAndValue></cst:RelativeDistinguishedName><cst:RelativeDistin
guishedName><cst:AttributeTypeAndValue><cst:AttributeType>2.5.
```

```
4.6</cst:AttributeType><cst:CountryName><cst:iso-3166-
code>RU</cst:iso-3166-
code></cst:CountryName></cst:AttributeTypeAndValue></cst:Relat
iveDistinguishedName><cst:RelativeDistinguishedName><cst:Attri
buteTypeAndValue><cst:AttributeType>2.5.4.8</cst:AttributeType
><cst:StateOrProvinceName><cst:UTF8String>69 Тверская
область</cst:UTF8String></cst:StateOrProvinceName></cst:Attrib
uteTypeAndValue></cst:RelativeDistinguishedName><cst:RelativeD
istinguishedName><cst:AttributeTypeAndValue><cst:AttributeType
>2.5.4.7</cst:AttributeType><cst:LocalityName><cst:UTF8String>
Нижний
Волочек</cst:UTF8String></cst:LocalityName></cst:AttributeType
AndValue></cst:RelativeDistinguishedName><cst:RelativeDistingu
ishedName><cst:AttributeTypeAndValue><cst:AttributeType>2.5.4.
3</cst:AttributeType><cst:CommonName><cst:UTF8String>ИП</cst:U
TF8String></cst:CommonName></cst:AttributeTypeAndValue></cst:R
elativeDistinguishedName></cst:DistinguishedName></cst:Subject
><cst:SubjectPublicKeyInfo><cst:PublicKeyAlgorithm><cst:AlgId>
1.2.643.2.2.19</cst:AlgId><cst:gostR3410EC_CryptoPro><cst:OBJE
CT_IDENTIFIER>1.2.643.2.2.36.0</cst:OBJECT_IDENTIFIER><cst:OBJ
ECT_IDENTIFIER>1.2.643.2.2.30.1</cst:OBJECT_IDENTIFIER></cst:g
ostR3410EC_CryptoPro></cst:PublicKeyAlgorithm><cst:SubjectPubl
icKey>0440CE875B0B1B448554CB2C904284BCAE581F7587D99FF4C991905D
EA8EE3DD21FC96670E90A80B01E77A8F6BE768248BCDC218A7B039555C7B18
0499011CB8C935</cst:SubjectPublicKey></cst:SubjectPublicKeyInf
o><cst:Extensions><cst:Extension><cst:ExtensionType>1.2.643.10
0.111</cst:ExtensionType><cst:Critical>{FALSE}</cst:Critical><
cst:extValue><cst:SubjectSignTool>"КриптоПро CSP" (версия
3.6)</cst:SubjectSignTool></cst:extValue></cst:Extension><cst:
Extension><cst:ExtensionType>1.2.643.100.112</cst:ExtensionTyp
e><cst:Critical>{FALSE}</cst:Critical><cst:extValue><cst:Issue
rSignTool><cst:signTool>"КриптоПро CSP" (версия
3.6)</cst:signTool><cst:cATool>Сертификат соответствия №
СФ/121-1857 от
17.06.2012</cst:cATool><cst:signToolCert>"Программно-
аппаратный комплекс "Юнисерт-ГОСТ". версия
3"</cst:signToolCert><cst:caToolCert>Сертификат соответствия №
СФ/000-0000 от
00.00.0000</cst:caToolCert></cst:IssuerSignTool></cst:extValue
></cst:Extension><cst:Extension><cst:ExtensionType>2.5.29.32</
cst:ExtensionType><cst:Critical>{FALSE}</cst:Critical><cst:ext
Value><cst:CertificatePolicies><cst:PolicyInformation><cst:Pol
icyIdentifier>1.2.643.100.113.1</cst:PolicyIdentifier></cst:Po
licyInformation><cst:PolicyInformation><cst:PolicyIdentifier>1
.2.643.100.113.2</cst:PolicyIdentifier></cst:PolicyInformation
></cst:CertificatePolicies></cst:extValue></cst:Extension><cst
:Extension><cst:ExtensionType>2.5.29.15</cst:ExtensionType><cs
t:Critical>{TRUE}</cst:Critical><cst:extValue><cst:KeyUsage>1<
/cst:KeyUsage></cst:extValue></cst:Extension><cst:Extension><c
st:ExtensionType>2.5.29.37</cst:ExtensionType><cst:Critical>{T
RUE}</cst:Critical><cst:extValue><cst:ExtKeyUsage><cst:EmailPr
otection>1.3.6.1.5.5.7.3.4</cst:EmailProtection></cst:ExtKeyUs
age></cst:extValue></cst:Extension><cst:Extension><cst:Extensi
onType>2.5.29.35</cst:ExtensionType><cst:Critical>{FALSE}</cst
:Critical><cst:extValue><cst:AuthorityKeyIdentifier><cst:KeyId
entifier>F9686180B9F033C9D5AAD3D2B4692BB34D829372</cst:KeyIden
tifier><cst:AuthorityCertIssuer><cst:GeneralName><cst:Director
yName><cst:DistinguishedName><cst:RelativeDistinguishedName><c
st:AttributeTypeAndValue><cst:AttributeType>1.2.840.113549.1.9
.1</cst:AttributeType><cst:EmailAddress>uuc_fk@roskazna.ru</cs
t:EmailAddress></cst:AttributeTypeAndValue></cst:RelativeDisti
nguishedName><cst:RelativeDistinguishedName><cst:AttributeType
AndValue><cst:AttributeType>2.5.4.8</cst:AttributeType><cst:St
ateOrProvinceName><cst:UTF8String>77 г.
```

```
Москва</cst:UTF8String></cst:StateOrProvinceName></cst:Attribu
teTypeAndValue></cst:RelativeDistinguishedName><cst:RelativeDi
stinguishedName><cst:AttributeTypeAndValue><cst:AttributeType>
1.2.643.3.131.1.1</cst:AttributeType><cst:INN><cst:numeric>007
710568760</cst:numeric></cst:INN></cst:AttributeTypeAndValue><
/cst:RelativeDistinguishedName><cst:RelativeDistinguishedName>
<cst:AttributeTypeAndValue><cst:AttributeType>1.2.643.100.1</c
st:AttributeType><cst:OGRN><cst:numeric>1047797019830</cst:num
eric></cst:OGRN></cst:AttributeTypeAndValue></cst:RelativeDist
inguishedName><cst:RelativeDistinguishedName><cst:AttributeTyp
eAndValue><cst:AttributeType>2.5.4.9</cst:AttributeType><cst:S
treetAddress><cst:UTF8String>улица Ильинка, дом
7</cst:UTF8String></cst:StreetAddress></cst:AttributeTypeAndVa
lue></cst:RelativeDistinguishedName><cst:RelativeDistinguished
Name><cst:AttributeTypeAndValue><cst:AttributeType>2.5.4.7</cs
t:AttributeType><cst:LocalityName><cst:UTF8String>Москва</cst:
UTF8String></cst:LocalityName></cst:AttributeTypeAndValue></cs
t:RelativeDistinguishedName><cst:RelativeDistinguishedName><cs
t:AttributeTypeAndValue><cst:AttributeType>2.5.4.6</cst:Attrib
uteType><cst:CountryName><cst:iso-3166-code>RU</cst:iso-3166-
code></cst:CountryName></cst:AttributeTypeAndValue></cst:Relat
iveDistinguishedName><cst:RelativeDistinguishedName><cst:Attri
buteTypeAndValue><cst:AttributeType>2.5.4.10</cst:AttributeTyp
e><cst:OrganizationName><cst:UTF8String>Федеральное
казначейство</cst:UTF8String></cst:OrganizationName></cst:Attr
ibuteTypeAndValue></cst:RelativeDistinguishedName><cst:Relativ
eDistinguishedName><cst:AttributeTypeAndValue><cst:AttributeTy
pe>2.5.4.3</cst:AttributeType><cst:CommonName><cst:UTF8String>
Уполномоченный удостоверяющий центр Федерального
казначейства</cst:UTF8String></cst:CommonName></cst:AttributeT
ypeAndValue></cst:RelativeDistinguishedName></cst:Distinguishe
dName></cst:DirectoryName></cst:GeneralName></cst:AuthorityCer
tIssuer><cst:AuthorityCertSerial>1</cst:AuthorityCertSerial></
cst:AuthorityKeyIdentifier></cst:extValue></cst:Extension><cst
:Extension><cst:ExtensionType>2.5.29.31</cst:ExtensionType><cs
t:Critical>{FALSE}</cst:Critical><cst:extValue><cst:CRLDistrib
utionPoints><cst:DistributionPoint><cst:DistributionPointName>
<cst:FullName><cst:GeneralName><cst:URI>ht
tp://crl.roskazna.ru/crl/UUC_FK_1.crl</cst:URI></cst:GeneralNa
me></cst:FullName></cst:DistributionPointName></cst:Distributi
onPoint><cst:DistributionPoint><cst:DistributionPointName><cst
:FullName><cst:GeneralName><cst:URI>http://crl.fsfk.local/crl/
UUC_FK_1.crl</cst:URI></cst:GeneralName></cst:FullName></cst:D
istributionPointName></cst:DistributionPoint></cst:CRLDistribu
tionPoints></cst:extValue></cst:Extension><cst:Extension><cst:
ExtensionType>2.5.29.14</cst:ExtensionType><cst:Critical>{FALS
E}</cst:Critical><cst:extValue><cst:SubjectKeyIdentifier>B397B
87E6A53C3DDB546C325D5B797A1CEBE824F</cst:SubjectKeyIdentifier>
</cst:extValue></cst:Extension></cst:Extensions></cst:TBSCerti
ficate><cst:AlgorithmIdentifier><cst:AlgId>1.2.643.2.2.3</cst:
AlgId></cst:AlgorithmIdentifier><cst:BIT_STRING>83DD1326127597
E46A17A9D667D346541507E21EF3937968958C323C7CD87ED435030A237FA9
099BFCA5B3CA2463A16F4F927E67FCD82EB476F60CE68F985997</cst:BIT_
STRING></cst:Certificate>
            </cst:signerCertInfo>
        </cst:SignatureInfo>
    </tccs:SignatureInfos>
    <tccs:advanced>PD94bWw ....Vsb3BlPgo=</tccs:advanced>
</tccs:ValidationResponseType>
```

signing_response_xmldsig_enveloped.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:SigningResponseType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">PD94
bW .... dmVsb3BlPgo=</tccs:SigningResponseType>
```

signing_response_xmldsig_detached.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:SigningResponseType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">PD94
bWw ... dHVyZT4K</tccs:SigningResponseType>
```

signing_request_xmldsig_enveloped.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:SigningRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver"
>

<tccs:data>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4
KICA8RGF0YT4KCUhlbGxvLCBXb3JsZCEKICA8L0RhdGE+Cg==</tccs:data>
    <tccs:signatureType>xmldsig</tccs:signatureType>
</tccs:SigningRequestType>
```

validation_request_wssec_actor.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:ValidationRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv"
xmlns:cst="http://www.roskazna.ru/eb/sign/types/cryptoserver">
    <tccs:signedData>PD94bW ...
VudmVsb3BlPgo=</tccs:signedData>
    <tccs:createAdvanced>true</tccs:createAdvanced>
    <tccs:actor>ACTOR</tccs:actor>
</tccs:ValidationRequestType>
```

validation_request_xmldsig_detached.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:ValidationRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">
    <tccs:signedData>PD94bWw .... VyZT4K</tccs:signedData>
<tccs:externalData>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVR
GLTgiPz4KICA8RGF0YT4KCUhlbGxvLCBXb3JsZCEKICA8L0RhdGE+Cg==</tcc
s:externalData>
</tccs:ValidationRequestType>
```

validation_request_xmldsig_enveloped.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:ValidationRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">
    <tccs:signedData>PD94bWw ... sb3BlPgo=</tccs:signedData>
</tccs:ValidationRequestType>
```

digest_response.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:DigestResponseType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">L+Q16i4i
DNhtg4F8cYG/ZY6s7dmpafUgYQkeM5MkAbs=</tccs:DigestResponseType>
```

digest_request_test_params.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:DigestRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">
    <tccs:dataBytes>IyEvYmluL3 ...
3B3ZH0KCg==</tccs:dataBytes>
    <tccs:paramOID>1.2.643.2.2.30.0</tccs:paramOID>
</tccs:DigestRequestType>
```

digest_request_specified_params.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:DigestRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv">
    <tccs:dataBytes>IyEvYmluL3NoC ...
xkX3B3ZH0KCg==</tccs:dataBytes>
    <tccs:paramOID>1.2.643.2.2.30.1</tccs:paramOID>
</tccs:DigestRequestType>
```

digest_request_default_params.xml

```
<?xml version="1.0" encoding="utf-8"?>
<tccs:DigestRequestType
xmlns:tccs="http://www.roskazna.ru/eb/sign/types/sgv" >
    <tccs:dataBytes>IyEvYmluL3NoCg ...
3ZH0KCg==</tccs:dataBytes>
</tccs:DigestRequestType>
```

Документация

1. Программно-аппаратный комплекс квалифицированной электронной подписи Jinn-Server. Версия 1.3. Руководство администратора.
2. Программно-аппаратный комплекс квалифицированной электронной подписи Jinn-Server. Версия 1.3. Руководство пользователя.