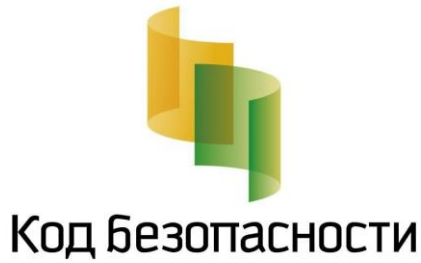
Код безопасности

Программно-аппаратный комплекс
квалифицированной электронной подписи

"Jinn-Server" версия 1.0

Руководство программиста

RU.88338853.501430.009 01 33



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

Оглавление

Введение

Данное руководство предназначено для программистов, использующих изделие "Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Server" версии 1.0" (далее – ПАК "Jinn-Server", комплекс, ПАК). В нем содержатся сведения, необходимые для установки и настройки программного обеспечения (ПО) ПАК "Jinn-Server" на компьютерах, функционирующих под управлением следующих дистрибутивов Linux:

Табл. 1. Дистрибутивы Linux, поддерживаемые ПАК "Jinn-Server"

Название дистрибутива	Версия ядра
Альт Линукс СПТ 6.0.0 x86/x64	2.6.32-el-smp-alt10.0.M55C.1
CentOS 7.0 x64	1406

Условные обозначения

В руководстве для выделения некоторых элементов текста (примечаний и ссылок) используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте примечаний или на полях.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.
- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Некоторые примечания могут не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень курсов и условия обучения представлены на сайте компании http://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
ИОК/PKI	Инфраструктура открытых ключей – 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
CAS	CRL Archiving Service – сервис, предназначенный для хранения и автоматического обновления списков отозванных сертификатов и обновлений к ним с целью последующего использования хранимых CRL другими компонентами ПАК
CFV	Cetificate Format Validation – составная часть сервиса SVS, предназначенная для проверки сертификатов открытых ключей на квалифицированность
CRL/COC	Список отозванных сертификатов (основной, регулярный)
deltaCRL	Обновление к COC, выпускаемое УЦ в интервале между выпусками COC
DMZ	Демилитаризованная зона, ДМЗ – 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 (файрвола) с целью минимизировать ущерб при взломе одного из общедоступных сервисов, находящихся в ДМЗ
SS	SigningService – сервис, предназначенный для формирования ЭП под некоторыми данными
SVS	SignatureValidationService – сервис, предназначенный для проверки данных, подписанных ЭП
ГУЦ	Головной удостоверяющий центр
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
УЦ	Удостоверяющий центр
ЭД	Электронный документ
ЭП	Электронная подпись

Глава 1
Общие сведения о ПАК "Jinn-Server"

Настоящее руководство предназначено для использования обслуживающим персоналом ПАК "Jinn-Server" на этапах установки и технического обслуживания ПАК.

При установке и техническом обслуживании дополнительно следует использовать следующие эксплуатационные документы:

Эксплуатационная документация[1]
Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Server" версия 1.0. Руководство администратора
Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Server" версия 1.0. Руководство программиста
Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Server" версия 1.0. Руководство пользователя

ПАК"Jinn-Server", а также набор дополнительных программных средств предназначены для выполнения функции автоматической проверки и выработки электронной подписи (ЭП) на электронных документах (ЭД) с сетевой выгрузкой результата во внешний сервис.

Общая схема развертывания компонентов ПАК "Jinn-Server" и их взаимодействие с внешними информационными системами представлены на рисунке 1.

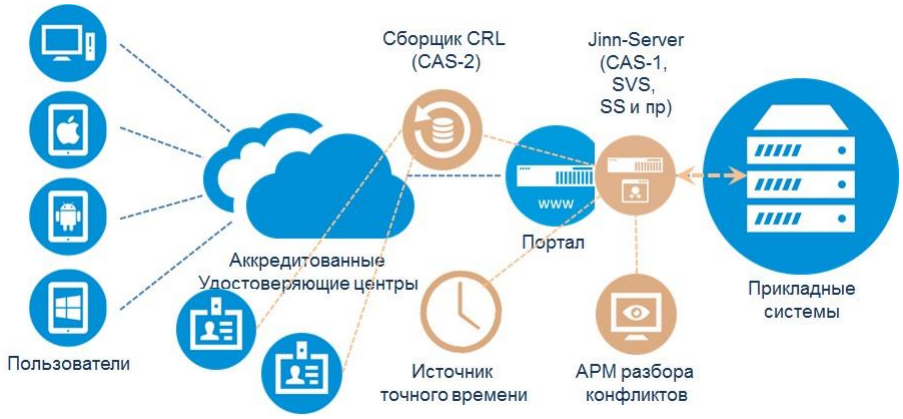


Рис. 1. Общая схема развертывания компонентов ПАК "Jinn-Server"

При использовании кластеризации число необходимых внешних сборщиков CRL (CAS-2), размещаемого в DMZ, будет диктоваться в первую очередь соображениями обеспечения надежности ПК и никак не связано с числом узлов ПК, расположенных в защищенном сегменте сети.

ПАК "Jinn-Server" построен по модульному принципу и содержит в своем составе следующие компоненты (подсистемы):

- Сервис проверки ЭП (SVS – SignatureValidationService) – предназначен для проверки данных, подписанных ЭП, и проверки сертификатов ЭП на квалифицированность и действительность.
- Сервис выработки ЭП (SS – SigningService) – предназначен для формирования ЭП под некоторыми данными.
- Сервис архивирования CRL (CAS – CRLArchivingService) – предназначен для хранения 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).
- Подсистема администрирования – предназначена для мониторинга и управления компонентами ПАК.

[1] Эксплуатационная документация поставляется в электронном виде в формате PDF (Adobe Acrobat Reader) и/или ODF, если не указано иного.

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

Требования к обслуживающему персоналу (программист)

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:

- задача контроля за работоспособностью технических средств;
- задача контроля за работоспособностью системных программных средств – операционной системы и иных программных компонентов в объеме, необходимом для выполнения ПАК "Jinn-Server" своего функционального назначения;
- задача контроля за выполнением ПАК "Jinn-Server" своих функций, помощь в выполнении своих функций операторам ПК;
- задача обеспечения работоспособности сервисов и транспортировки информации между компонентами ПК и во внешние модули прикладной системы;
- задача ведения архивных копий информационных активов ПК (хранилища СУБД, прикладные и системные журналы и т.д.).

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

Входные и выходные данные

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

Язык описания веб-сервисов и доступа к ним

Язык описания веб-сервисов и доступа к ним реализован на WSDL (Web Services Description Language). Каждый документ WSDL можно разбить на следующие логические части:

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

  Описание сервисов представлено в Приложении №1, а описание типов – в Приложении №2.

Описание структур входных и выходных данных веб-сервисов

Общие сведения

Все перечисленные в данном документе 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>
```

ServiceFaultInfo::type – содержит один из возможных типов ошибок:

- "internalError" – возвращается в случае любых ошибок, не покрываемых ни одним из других возможных значений данного поля;
- "invalidRequestDataFormat" – возвращается в случае ошибок в формате данных, переданных на проверку либо на подписание. К таким ситуациям относятся:
  - ValidationRequestType::signedData содержит Base64 от ASN.1-кодированных данных, не являющихся CMS-SignedData либо имеющих ошибки в кодировании или расхождения со стандартами в структуре данных;
  - ValidationRequestType::signedData содержит Base64 от данных, не являющихся ни ASN.1-кодированными, ни well-formed XML-документом;
  - ValidationRequestType::externalData содержит Base64 от данных, не являющихся well-formed XML-документом;
  - SigningRequestType::data содержит Base64 от данных, не являющихся well-formed XML-документом, и при этом указана необходимость создания подписи в формате, отличном от CMS-SignedData;
  - "invalidXmlPartID" – xmlPartID, указанный в запросе, не найден в переданном xml-документе.

ServiceFaultInfo::comment – содержит краткое (до 200 символов) дополнительное описание возникшей ошибки.

SigningService

Digest

Данная операция в качестве входных данных принимает структуру, соответствующую следующему описанию:

```
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>
```

DigestRequestType::dataBytes – содержит Base64-кодированные данные, подлежащие хэшированию. Хэш вычисляется от исходных бинарных данных, т. е. предварительно выполняется Base64-декодирование.

DigestRequestType::paramOID – необязательный параметр, строковое представление параметров для процедуры хэширования.

Используется необязательное поле <algorithmId>, имеющее тип <cst:OBJECT_IDENTIFIER> и соответствующий формат.

Значение этого поля определяет необходимый пользователю алгоритм подписи либо хэширования (в зависимости от сервиса, к которому он обращается). Варианты значений алгоритмов (используются и в других типах запросов):

	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
Хэш+подпись 34.11+34.10–	1.2.643.2.2.3	1.2.643.7.1.1.3.2	1.2.643.7.1.1.3.3

В случае отсутствия данного необязательного поля в запросе – сервер выполняет запрошенную операцию в соответствии с параметрами конфигурационных файлов perferredSignatureAlgorithm и preferredDigestAlgorithm.

В случае наличия поля algorithmId в запросе – его значение предварительно проверяется на соответствие параметрам конфигурационных файлов supportedsignatureAlgorithms и supportedDigestAlgorithms - в зависимости от сервиса, к которому обращен запрос.

При этом подразумевается, что указанные параметры конфигурационных файлов должны адекватно отражать наличие поддержки соответствующих алгоритмов в СКЗИ и возможность их использования. То есть ГОСТ Р 34.10–2001 не должен присутствовать в списке поддерживаемых алгоритмов подписи, если по решению администратора в ПАК "Jinn-Server" не установлен контейнер с ключами соответствующего алгоритма – вне зависимости от наличия поддержки ГОСТ Р 34.10–2001 в установленном СКЗИ.

В случае появления данного параметра в запросах на проверку без усиления – его значение игнорируется.

При обработке запросов на проверку с усилением до уровня, требующего формирования штампа времени, данный параметр определяет алгоритм для подписания штампа времени.

Параметры запроса:

dataBytes – обязательно, base64Binary, not empty, содержит данные для хэширования.

state – optional, base64Binary, not empty (если присутствует), содержит состояние контекста хэширования, полученное на приведенном ниже шаге (см. Сценарий взаимодействия).

paramoid – optional, содержит идентификатор параметров алгоритма хэширования. Имеет смысл только для старого алгоритма хэширования (ГОСТ Р 34.11-94), для других алгоритмов игнорируется. Допустимые значения (соответственно TestParamSet, CryptoProParamSet):

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

algorithmId – optional, определяет алгоритм хэширования. В случае если параметр опущен, будет использоваться алгоритм, указанный в настройках ПАК "Jinn-Server". Допустимые значения (соответственно ГОСТ Р 34.11–94, 34.11–2012–256, 34.11–2012–512):

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

Формат ответа:

- digest, base64Binary, содержит вычисленное значение хэша;
- state, base64Binary, содержит состояние контекста хэширования, пригодное для продолжения вычислений.

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.

```
<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>
```

Данный элемент будет содержать Base64-кодированное значение вычисленного хэша.

Sign

Данная операция в качестве входных данных принимает структуру, соответствующую следующему описанию:

```
<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:sequence>
</xs:complexType>
```

SigningRequestType::data – содержит Base64-кодированные данные, которые необходимо подписать.

SigningRequestType::signatureType – необязательный параметр, определяет необходимый формат подписи, допустимые значения:

- "cms" – должна быть сформирована подпись в формате CMS-SignedData (значение по умолчанию);
- "xmldsig" – должна быть сформирована подпись в формате XMLDsig;
- "wssecurity" – должна быть сформирована подпись в формате WS-Security;
- "cades-bes", "cades-c", "cades-t", "cades-a" – должна быть сформирована подпись в формате CMS-SignedData, усиленная в необходимом объеме (дополненная атрибутами) в соответствии с ETSI TS 101 733 (CAdES);
- "xades-bes", "xades-c", "xades-t", "xades-a" – должна быть сформирована 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" – должна быть сформирована подпись в формате WS-Security, усиленная в необходимом объеме (дополненная атрибутами) в соответствии с ETSI TS 101 903 (XadES).

  В случае если указан формат подписи, отличный от CMS-SignedData, контролируется корректность формата поля data.

SigningRequestType::detached – необязательный boolean-параметр, значение по умолчанию – "false", в случае указания значения "true" будет сформирована отсоединенная подпись.

SigningRequestType::xmlPartID – необязательный параметр, имеет смысл только при подписании xml-документов, позволяет подписать не весь документ, а заданный таким образом элемент.

SigningRequestType::actor – необязательный параметр, имеет смысл только при подписании в формате WS-Security, позволяет задать значение атрибута "actor", который будет установлен для родительского по отношению к создаваемой подписи элемента "wsse:Security".

В случае успешного завершения операция возвращает ответ следующего вида:

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

Данный элемент будет содержать Base64-кодированное значение сформированной подписи.

SignatureValidationService

Validate

Данная операция в качестве входных данных принимает структуру, соответствующую следующему описанию:

```
<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>
```

ValidationRequestType::signedData – Base64-кодированное значение подписи, которую необходимо проверить, позволяет единообразно передавать на проверку подписи любых поддерживаемых форматов, конкретный формат определяется автоматически при декодировании.

ValidationRequestType::externalData – необязательный параметр, необходим в случае проверки отсоединенной подписи и должен содержать Base64-кодированное значение исходных данных, соответствующих отсоединенной подписи, переданной в параметре signedData.

ValidationRequestType::createAdvanced – необязательный строковый параметр, значение по умолчанию – "false", определяет необходимость формирования усиленной подписи, а также уровень усиления в случае успешной проверки переданных данных. Множество допустимых значений обратно совместимо с типом xs:boolean и дополнительно содержит все значения для усиленных типов подписи, определенные в **SigningRequestType::signatureType**.

ValidationRequestType::xmlPartID – аналогично SigningRequestType::xmlPartId.

ValidationRequestType::actor – для проверки будет выбрана подпись, содержащаяся внутри элемента wsse::Security с атрибутом "actor", имеющим заданное значение.

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>
```

ValidationRes::gmtDateTime – время проверки по GMT.

ValidationRes::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, возможно в случае, если не найдены сертификаты авторов либо для них недоступны полные и актуальные СОС.
- "invalid" – все имеющиеся подписи недействительны.
- "partiallyValid" – часть подписей действительна, часть – нет.
- "valid" – в случае если все подписи проверены успешно.

ValidationRes::SignatureInfos – необязательный список с подробной информацией о результатах проверки каждой из имеющихся в проверяемых данных подписей. Список может отсутствовать либо быть пустым, в случае 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. В случае 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>
```

SignatureInfo::reference – справочное поле.

SignatureInfo::status – результат проверки, возможные значения:

- "unknown" – недостаточно информации для определения статуса подписи, возможно в случае, если не найден сертификат автора либо для него недоступны полные и актуальные СОС.
- "invalid" – подпись недействительна.
- "valid" – подпись проверена успешно.

SignatureInfo::failInfo – необязательное поле, раскрывающее причину отрицательного результата проверки, содержит тип причины и комментарий. Возможные значения типа причин:

```
"unknownDigestAlgorithm"
"unknownSignatureAlgorithm"
```

```
"signerCertificateNotFound"
"signerCertificateIssuerNotFound"
"signerCertificateSignatureInvalid"
"signerCertificateCRLNotFound"
"signerCertificateExpired"
"signerCertificateRevoked"
"invalidDigestValue"
"invalidSignatureValue"
```

SignatureInfo::signerCertInfo – необязательное поле, содержит сертификат автора, в случае если он найден.

ValidationResponseType::advanced – необязательное поле, содержит Base64-кодированное значение усиленной подписи, присутствует в ответе только в случае, если было запрошено усиление подписи и ValidationResponseType::globalStatus содержит значение "valid".

CertificateFormatValidate

Сценарий проверки:

При передаче сертификата осуществляется его проверка по следующим пунктам:

- проверка декодирования сертификата;
- проверка на наличие неизвестных путей/неверных значений (ANY_BROKEN);
- проверка на удовлетворение правилам для разных типов собственников на основе приказа № 795.

```
      <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>
```

Данные:

certificate – обязательно, base64Binary, not empty, содержит сертификат.

SubjectType – тип субъекта в сертификате (неизвестен – 0, физическое лицо – 1, организация – 2).

Формат ответа:

XML с отчетом (CFVReport), состоящим из записей (CFVNotice). В каждой записи 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.

NoticeClass – может принимать два значения:

- 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>
```

CertificateValidation

Сценарий проверки:

При передаче сертификата осуществляется его проверка по следующим пунктам:

- Актуальность сертификата на текущую дату.
- Актуальность сертификата на выбранную дату.
- Проверки формата.

```
<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>

<xs:complexType name="CVAttributes">
<xs:sequence>
<xs:element name="Attribute" type="cst:Attribute"
minOccurs="0" maxOccurs="unbounded" />
</xs:sequence>
</xs:complexType>

<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="atributes" type="tccs:CVAttributes"
minOccurs="0" />
</xs:sequence>
</xs:complexType>
```

Описание параметров запроса:

certificate – сертификат в формате base64.

validationDate – необязательный параметр, дата, на которую выполняется проверка сертификата, в числовом формате "unixtime". Если не указан, проверка выполняется за текущую дату.

subjectType – необязательный параметр, определяет тип субъекта: 0 – неизвестен, 1 – физическое лицо, 2 – юридическое лицо. По умолчанию – 0. Если указан, в ответ будет добавлен "attributes".

Описание параметров ответа:

certId – информация по проверяемому сертификату.

date – время, когда выполнена проверка, в числовом формате "unixtime".

params – содержит значение validationDate из запроса.

status – статус проверки, возможные значения: "valid", "invalid".

failInfo – выводится при получении статуса "invalid", содержит два тега: "type" – с типом ошибки, "comment" – с описанием ошибки.

attributes – появляется, если в запросе указан subjectType. Содержит информацию в формате CFVReport.

Примеры запросов и ответов к/от веб-сервисам

В приведенных примерах запросов вместо конкретных значений указаны "переменные" (выделены красным цветом), которые нужно заменить конкретным значением для указанного тега – описание тегов см. в разделе "Описание структур входных и выходных данных веб-сервисов". В примерах ответов вместо "переменных" будут сформированы значения – необходимо проверить, что они присутствуют в ответе.

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:algorithmId>1.2.643.7.1.1.3.2</sgv:algorithmId>
</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>
```

CreateAdvenced request #1

Запрос для усиления 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>
```

CreateAdvenced request #2

Запрос для усиления с выбором подписи, до которой требуется усилиться – вместо @value@ в теге 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>
```

CreateAdvenced response

Ответ на запрос для усиления подписи будет одинаков для двух вышеперечисленных примеров (разница будет в сформированной усиленной подписи):

```
<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 2
Обращение к ПАК "Jinn-Server"

Перед обслуживающим персоналом с ролевым признаком "программист" стоят следующие основные задачи, указанные ниже.

Контроль работоспособности технических и программных средств

Данный вид контроля выполняется наряду/совместно с обслуживающим персоналом с ролевым признаком "программист". Средствами контроля выступают штатные средства аппаратных платформ, общесистемного и прикладного программного обеспечения в соответствии с эксплуатационной документацией.

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

- Мониторинг прикладных и общесистемных журналов. Прикладные журналы расположены в директории /var/opt/tccs/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, а их периодичность зависит от настроек cron-таблицы, расположенной в конфигурационном файле /etc/crontab.
- Мониторинг общесистемных процессов, анализ которых выходит за рамки программы tccs_watchdog. Выполняется с помощью команды ps. Например: 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, которые, с одной стороны, выполняют автоматические попытки перезапустить зависшие процессы сервисов, а с другой – предоставляют способы оповещения обслуживающего персонала по транспорту электронной почты (дополнительно см. главу "Сообщения" настоящего документа), что в совокупности позволяет добиться высоких показателей готовности.

В случае нештатных ситуаций при невозможности автоматическими средствами обеспечить восстановление штатного функционирования ПК следует детализировать причину нештатной ситуации по прикладным и/или общесистемным журналам и, воспользовавшись сопроводительной документацией на модули (включая проприетарные и СПО компоненты), а также при необходимости (и возможности) анализом исходного кода, устранить причину и добиться нормального функционирования.

Ведение архивных копий прикладных и общесистемных журналов

Для задач упрощения последующего аудита функционирования ПК, а также минимизации времени восстановления штатного режима функционирования ПК в обязанности программиста входит задача ведения архивных копий журналов, а также наряду/совместно (взаимно дополняя персональные и групповые полномочия) с обслуживающим персоналом с ролевым признаком "программист" ведение архивных копий содержания таблиц и настроек СУБД.

Архивные копии журналов

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

Настройка logrotate определяется конфигурационным файлом /etc/logrotate.conf, в котором должны находиться следующие параметры:

```
/var/opt/tccs/log/cgi {
    rotate 10
    daily
    postrotate
    /usr/bin/killall -HUP syslogd
    endscript
}

/var/opt/tccs/log/online {
    rotate 10
    daily
    postrotate
    /usr/bin/killall -HUP syslogd
    endscript
}

/var/opt/tccs/log/offline {
    rotate 10
    daily
    postrotate
    /usr/bin/killall -HUP syslogd
    endscript
}

/var/opt/tccs/log/misc {
    rotate 10
    daily
    postrotate
    /usr/bin/killall -HUP syslogd
    endscript
}

/var/opt/tccs/log/access_log {
    rotate 10
    daily
    sharedscripts
    postrotate
    /usr/bin/killall -HUP httpd2.worker
    endscript
}

var/opt/tccs/log/error_log {
    rotate 10
    daily
    sharedscripts
    postrotate
    /usr/bin/killall -HUP httpd2.worker
    endscript
}
```

```
/var/opt/tccs/log/adm.access_log {
    rotate 10
    daily
    sharedscripts
    postrotate
    /usr/bin/killall -HUP httpd2
    endscript
}

var/opt/tccs/log/adm.error_log {
    rotate 10
    daily
    sharedscripts
    postrotate
    /usr/bin/killall -HUP httpd2
    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 директории /var/opt/tccs/log/.

Архивные копии СУБД

Архивные копии содержания таблиц и настроек СУБД рекомендуется выполнять после любых действий, связанных с управлением и администрированием сервиса CAS посредством графического гипертекстового интерфейса, направленных на изменение содержимого таблиц СУБД.

Для копирования таблиц СУБД требуется подключить отчуждаемый носитель и выполнить следующую команду:

```
su -c "/usr/bin/pg_dump -f /mnt/flash/db_cas1.sql csm"
postgres
```

Глава 3
Сообщения

Компоненты ПАК "Jinn-Server" содержат в своем составе специальные модули, обеспечивающие активный мониторинг процессов и автоматический перезапуск в случае их "падения". Оповещение обслуживающего персонала осуществляется транспортом электронной почты на указанные в конфигурации адреса. Программа информирует по факту следующих событий:

- Процесс не запущен ("упал").
- Попытка запустить процесс автоматически.
- Результат процедуры автоматического перезапуска.
- Дневной отчет по перечню контролируемых процессов.

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

Пример:

```
"watchedservice": [
        { "hostname": "tccs1.domain.ru" },
        { "port": 80 },
        { "socket": "" },
        { "action": "/opt/tccs/etc/init.d/tccs.admin" },
        { "description": "CSM WEB ADMIN" }
],
"watchedservice": [
        { "hostname": "tccs1.domain.ru" },
        { "port": 11112 },
        { "socket": "" },
        { "action": "/opt/tccs/etc/init.d/cas1d" },
        { "description": "CRL Archive Daemon" }
],
"watchedservice": [
        { "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"
```

Для создания объекта, описывающего процесс, который необходимо контролировать, описываются структуры с названием watchedservice, состоящие из:

- 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/выключение почтового уведомления;
- notification_email – адрес получателя почтового уведомления.

Более детальная настройка почтовых уведомлений выполняется в исполняемом shell-скрипте /opt/tccs/bin/notification.sh. Пример содержимого сценария выглядит следующим образом:

```
#!/bin/sh

FROM="robot@domain.ru"
TO="admin@domain.ru"
SERVER="mail.domain.ru"
NAME="CAS1"
COMPANY="COMPANY1"
PROG="/usr/local/bin/smtpclient"

touch /tmp/notification.start

if test "x$1" = "x" || ! test -f $1 || ! test -n "$FROM" || !
test -n "$TO" || ! test -n "$SERVER" || ! test -n "$NAME" || !
test -n "$COMPANY" || ! test -n "$PROG" || ! test -f $PROG;
then
        touch /tmp/notification.error
        exit 1
fi

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

SUBJECT="$NAME Robot of Process Notification ($COMPANY)"
cmd_check=`grep "OK" $1`
if [ -z "$cmd_check" ]; then
        SUBJECT="ПРЕДУПРЕЖДЕНИЕ! $NAME Robot of Process
Notification ($COMPANY)"
fi
cmd_check=`grep "!" $1`
if ! [ -z "$cmd_check" ]; then
        SUBJECT="ОШИБКА! $NAME Robot of Process Notification
($COMPANY)"
fi
cmd_check=`grep "service:" $1`
if ! [ -z "$cmd_check" ]; then
        SUBJECT="Daily: $NAME Robot of Process Notification
($COMPANY)"
fi
cmd_check=`grep "failed" $1`
if ! [ -z "$cmd_check" ]; then
        SUBJECT="Daily: ОШИБКА! $NAME Robot of Process
Notification ($COMPANY)"
fi

mail_send() {
        $PROG $CHARSET $MIME -s "$SUBJECT" -f $FROM -S $SERVER
-F $BODY $TO 2>/tmp/smtpclient.error
        RC=$?
```

```
        if [ $RC -eq 0 ]; then
                rm /tmp/smtpclient.error
        else
                sleep 1
                $PROG $CHARSET $MIME -s "$SUBJECT" -f $FROM -S
$SERVER -F $BODY $TO 2>/tmp/smtpclient.error
                RC=$?
                if [ $RC -eq 0 ]; then
                        rm /tmp/smtpclient.error
                else
                        DIR=`date -R`
                        mkdir -p /tmp/smtpclient-error/"$DIR"
                        mv /tmp/smtpclient.error
/tmp/smtpclient-error/"$DIR"/error.log
                        cp $BODY /tmp/smtpclient-error/"$DIR"/
                        echo "$PROG $CHARSET $MIME -s
\"$SUBJECT\" -f $FROM -S $SERVER -F $BODY $TO
2>/tmp/smtpclient.error" >/tmp/smtpclient-error/"$DIR"/cmdline
                fi
        fi
}

BODY=$1
CHARSET="-M UTF8"
mail_send

touch /tmp/notification.stop
exit 0
```

В данном сценарии рекомендуется настраивать параметры, приведенные в начале сценария, такие как:

- FROM – отправитель почтового уведомления;
- TO – получатель почтового уведомления. Этот параметр игнорируется в случае наличия параметра notification_email в конфигурационном файле /opt/tccs/etc/csm.conf;
- SERVER – почтовый сервер, через который будут отправляться почтовые уведомления;
- NAME – название сервиса;
- COMPANY – название компании/учреждения, в рамках которой будут отправляться почтовые уведомления.

Содержимое сценария, отличное от приведенных выше параметров, изменять не рекомендуется.

Приложение 1. Описание 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="xs:boolean" />
                    <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: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>
"watchedservice": [
        { "hostname": "tccs1.domain.ru" },
        { "port": 80 },
        { "socket": "" },
        { "action": "/opt/tccs/etc/init.d/tccs.admin" },
        { "description": "CSM WEB ADMIN" }
],
"watchedservice": [
        { "hostname": "tccs1.domain.ru" },
        { "port": 11112 },
        { "socket": "" },
        { "action": "/opt/tccs/etc/init.d/cas1d" },
        { "description": "CRL Archive Daemon" }
],
"watchedservice": [
        { "hostname": "tccs1.domain.ru" },
        { "port": 0 },
        { "socket": "/tmp/.s.PGSQL.5432" },
        { "action": "/opt/tccs/etc/init.d/psqld" },
```

```
        { "description": "PostgreSQL" }
],
```

Штатный режим работы программы **tccs_watchdog** определяется демоном crond и описан в конфигурационном файле /jail/XXX/etc/crontab (см. ниже).

```
*/1   *  *  *  *  root    /usr/local/libexec/process_analysis
>/dev/null
1     3  *  *  *  root    /usr/local/libexec/process_analysis
notifier >/dev/null
```

Демон crond вызывает программу **tccs_watchdog** в двух режимах – каждую минуту и один раз в сутки, с указанием параметра **notifier**.

Первый режим используется для ежеминутного отслеживания работоспособности сервисов. Если какой-либо сервис оказывается недоступным, то программа **tccs_watchdog** отправляет почтовое уведомление администратору системы (администраторам системы по списку) и автоматически пытается перезапустить сервис. После попытки перезапуска сервиса администратору(ам) отправляется повторное почтовое уведомление, информирующее его либо об успешном перезапуске сервиса, либо о том, что сервис запустить не удалось и требуется непосредственное участие администратора. Последующие попытки перезапустить такой сервис будут производиться, но при отрицательном результате уже не будут сопровождаться почтовыми уведомлениями. В случае если сервис был перезапущен автоматически или в ручном режиме, т.е. изменился статус работоспособности сервиса с "неработающий" на "работающий", автоматически будет создано почтовое уведомление с указанием наименования сервиса и его текущего статуса.

Второй режим используется для ежедневного итогового отчета о работоспособности всех отслеживаемых сервисов с указанием, какие из присутствующих сервисов на момент составления отчета находятся в работоспособном состоянии.

Документация

1	Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Server" версии 1.0. Руководство администратора
2	Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Server" версии 1.0. Руководство программиста
3	Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Server" версии 1.0. Руководство пользователя