УТВЕРЖДЕНО

приказом ГБУ СО «РЦУП»

от «22» апреля 2011 г. № 24/2-ОД

ИНТЕГРАЦИОННАЯ ШИНА ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА САМАРСКОЙ ОБЛАСТИ

СПЕЦИФИКАЦИЯ ТРЕБОВАНИЙ К МЕХАНИЗМАМ ПОСТАНОВКИ И ПРОВЕРКИ ЭЦП

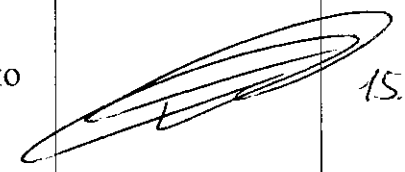
ЛИСТОВ 30

Самара 2011 г.

ЛИСТ СОГЛАСОВАНИЯ

Спецификация требований к механизмам постановки и проверки ЭЦП

ГБУ СО РЦУП

Должность	ФИО	Подпись	Дата
Заместитель директора	Д.П.Шевченко		15.04.2011
Начальник управления по развитию и сопровождению информационных систем и ресурсов	А.В.Ягупов		11.04.2011
Главный инженер проекта	С.А.Кузьминов		8.04.2011
Главный инженер проекта	Н.В.Кутузов		08.04.2011

Содержание

Введение

Данный документ описывает требования, предъявляемые к механизмам постановки и проверки электронной цифровой подписи (далее – ЭЦП), используемой для обеспечения целостности сообщений, участвующих в процессе информационного обмена.

1. Основные подходы при использовании ЭЦП

Для обеспечения целостности сообщения применяются следующие подходы:

1. Все данные запроса, водимые пользователем, рассматриваются как электронное заявление и подписываются ЭЦП пользователя. Результат подписания помещается в тело сообщения. ЭЦП пользователя формируется с использованием цифрового сертификата, выданного региональным удостоверяющим центром Правительства Самарской области (далее – РУЦ).
2. Сообщение, содержащее данные запроса и формируемое на основании действий пользователя в интерфейсе портала электронных услуг (далее – Портал), целиком подписывается ЭЦП Портала, результат подписания сообщения помещается в SOAP заголовок сообщения. Под ЭЦП Портала понимается ЭЦП уполномоченного лица организации, ответственной за эксплуатацию Портала. ЭЦП Портала формируется с использованием цифрового сертификата, выданного РУЦ. Подписание запроса осуществляется в соответствии с установленными правилами подписания [2].
3. Сообщение, содержащее данные ответа, целиком подписывается ЭЦП ведомственной информационной системой (далее – ВИС). Результат подписания сообщения помещается в заголовок сообщения. Подписание запроса осуществляется в соответствии с правилами [2] . Кроме того, ВИС подписывает данные ответа в теле сообщения для обеспечения целостности и неизменности передаваемых данных в третьи системы. Под ЭЦП ВИС понимается ЭЦП уполномоченного лица организации, ответственной за эксплуатацию ВИС. ЭЦП ВИС формируется с использованием цифрового сертификата, выданного РУЦ.

4. Сообщение, содержащее данные запроса или ответа, целиком подписывается ЭЦП интеграционной шины ЭП СО (далее – ИШ ЭП СО), результат подписания сообщения помещается в SOAP заголовок сообщения. Подписание сообщения осуществляется в соответствии установленными правилами [2]. Под ЭЦП ИШ ЭП СО понимается ЭЦП уполномоченного лица организации, ответственной за эксплуатацию ИШ ЭП СО. ЭЦП ИШ ЭП СО формируется с использованием цифрового сертификата, выданного РУЦ.
5. В случае, если сообщение, содержащее данные запроса, формируется системой, отличной от Портала, то сообщение целиком подписывается ЭЦП системы. Результат подписания сообщения помещается в SOAP заголовок сообщения. Подписание запроса осуществляется в соответствии с установленными правилами [2]. Под ЭЦП системы понимается ЭЦП уполномоченного лица организации, ответственной за эксплуатацию системы. ЭЦП системы формируется с использованием цифрового сертификата, выданного РУЦ.

Общая схема использования ЭЦП при обмене сообщениями представлена на рисунке 1:

1.0. Пользователь обращается на Портал для получения электронной услуги. При этом используется цифровой сертификат.

1.1. Портал на основании данных, содержащихся в цифровом сертификате, производит аутентификацию пользователя. При положительном результате аутентификации, пользователь продолжает работу. При отрицательном результате пользователю сообщается о причине отказа в доступе и работа на этом прекращается.

1.2. Пользователь на Портале формирует запрос и подписывает введенные данные ЭЦП пользователя (раздел 2.1 настоящего документа). При этом результат подписи и сертификат открытого ключа пользователя помещается в тело сообщения.

1.3. Запрос подписывается ЭЦП Портала (раздел 2.2 настоящего документа). При этом ЭЦП и сертификат открытого ключа Портала помещается в SOAP заголовок сообщения.

1.4. Запрос передается на ИШ ЭП СО.

1.5. На ИШ ЭП СО производится контроль сообщения. Контроль сообщения заключается в анализе ЭЦП, содержащейся в заголовке сообщения. Если сертификат принадлежит доверяемой системе (Портал) и ЭЦП действительна, производится дальнейшая обработка сообщения. В противном случае обработка прекращается и ИШ ЭП СО формирует и передает на Портал сообщение, содержащее код ошибки [1]. Данный контроль подтверждает целостность и неизменность сообщения с момента его отправки Порталом. Контроль сообщения осуществляется в соответствии с установленными правилами [2].

1.6. На ИШ ЭП СО производится проверка действительности сертификата и ЭЦП пользователя (раздел 3 настоящего документа). Если сертификат и ЭЦП пользователя действительны – производится дальнейшая обработка запроса. Если сертификат и/или ЭЦП не действительны – обработка прекращается и ИШ ЭП СО формирует и передает на Портал сообщение, содержащее код ошибки. Данный вид проверки служит для контроля целостности и неизменности передаваемых данных. Также эта проверка позволяет провести авторизацию пользователя и снизить нагрузку на саму ИШ ЭП СО и ВИС в случае передачи некорректных данных, или данных, несанкционированно измененных.

1.7. Сообщение подписывается ЭЦП ИШ ЭП СО (раздел 2.2 настоящего документа). ЭЦП и сертификат открытого ключа ИШ ЭП СО помещается в SOAP заголовок сообщения.

1.8. Сообщение передается в ВИС, ответственную за оказание электронной услуги.

1.9. ВИС производит контроль сообщения. Контроль сообщения заключается в анализе ЭЦП, содержащейся в заголовке сообщения. Если сертификат принадлежит ИШ ЭП СО и ЭЦП действительна, производится дальнейшая обработка сообщения. В противном случае обработка прекращается и ВИС формирует сообщение на ИШ ЭП СО, содержащее код ошибки. Данный контроль подтверждает целостность и неизменность сообщения с момента его отправки ИШ ЭП СО. Контроль сообщения осуществляется в соответствии с установленными правилами [2].

1.10. ВИС производит проверку действительности сертификата и ЭЦП пользователя (раздел 3 настоящего документа). Если сертификат и ЭЦП пользователя действительны – производится дальнейшая обработка запроса. Если сертификат и/или ЭЦП не действительны – обработка прекращается, ВИС формирует, содержащий только код ошибки. Ответ с ошибкой подписывается. Происходит переход на шаг 1.12.

1.11. ВИС на основании данных запроса формирует ответ.

1.12. ВИС подписывает своей ЭЦП данные ответа в теле сообщения для обеспечения целостности и неизменности передаваемых данных в третьи системы (раздел 2.1 настоящего документа). Так же ВИС подписывает все сообщение целиком ЭЦП ВИС (раздел 2.2 настоящего документа). ЭЦП ВИС помещается в SOAP заголовок сообщения.

1.13. Сообщение, содержащее данные ответа, передается на ИШ ЭП СО.

1.14. На ИШ ЭП СО производится контроль сообщения. Контроль сообщения заключается в анализе ЭЦП, содержащейся в заголовке сообщения. Если сертификат принадлежит доверяемой системе (ВИС) и ЭЦП действительна, производится дальнейшая обработка сообщения. В противном случае, обработка прекращается, и ИШ ЭП СО формирует и передает ВИС сообщение, содержащее код ошибки. Данный контроль подтверждает целостность и неизменность сообщения с момента его отправки ВИС.

1.15. На ИШ ЭП СО производится проверка действительности сертификата и ЭЦП ВИС (раздел 3 настоящего документа). Если сертификат и ЭЦП ВИС действительны – производится дальнейшая обработка запроса. Если сертификат и/или ЭЦП не действительны – обработка прекращается и ИШ ЭП СО формирует и передает на Портал сообщение, содержащее код ошибки. Данный вид проверки служит для контроля целостности и неизменности передаваемых данных.

1.16. Сообщение подписывается ЭЦП ИШ ЭП СО (раздел 3 настоящего документа). ЭЦП и сертификат открытого ключа ИШ ЭП СО помещается в SOAP заголовок сообщения.

1.17. Сообщение передается на Портал.

1.18. На Портале производится контроль сообщения. Контроль сообщения заключается в анализе ЭЦП, содержащейся в заголовке сообщения. Если сертификат принадлежит ИШ ЭП СО и ЭЦП действительна, производится дальнейшая обработка сообщения. В противном случае обработка прекращается и Портал формирует и передает ИШ ЭП СО сообщение, содержащее код ошибки. Данный контроль подтверждает целостность и неизменность сообщения с момента его отправки ИШ ЭП СО.

1.19. Данные ответа предоставляются пользователю в соответствующем интерфейсе.

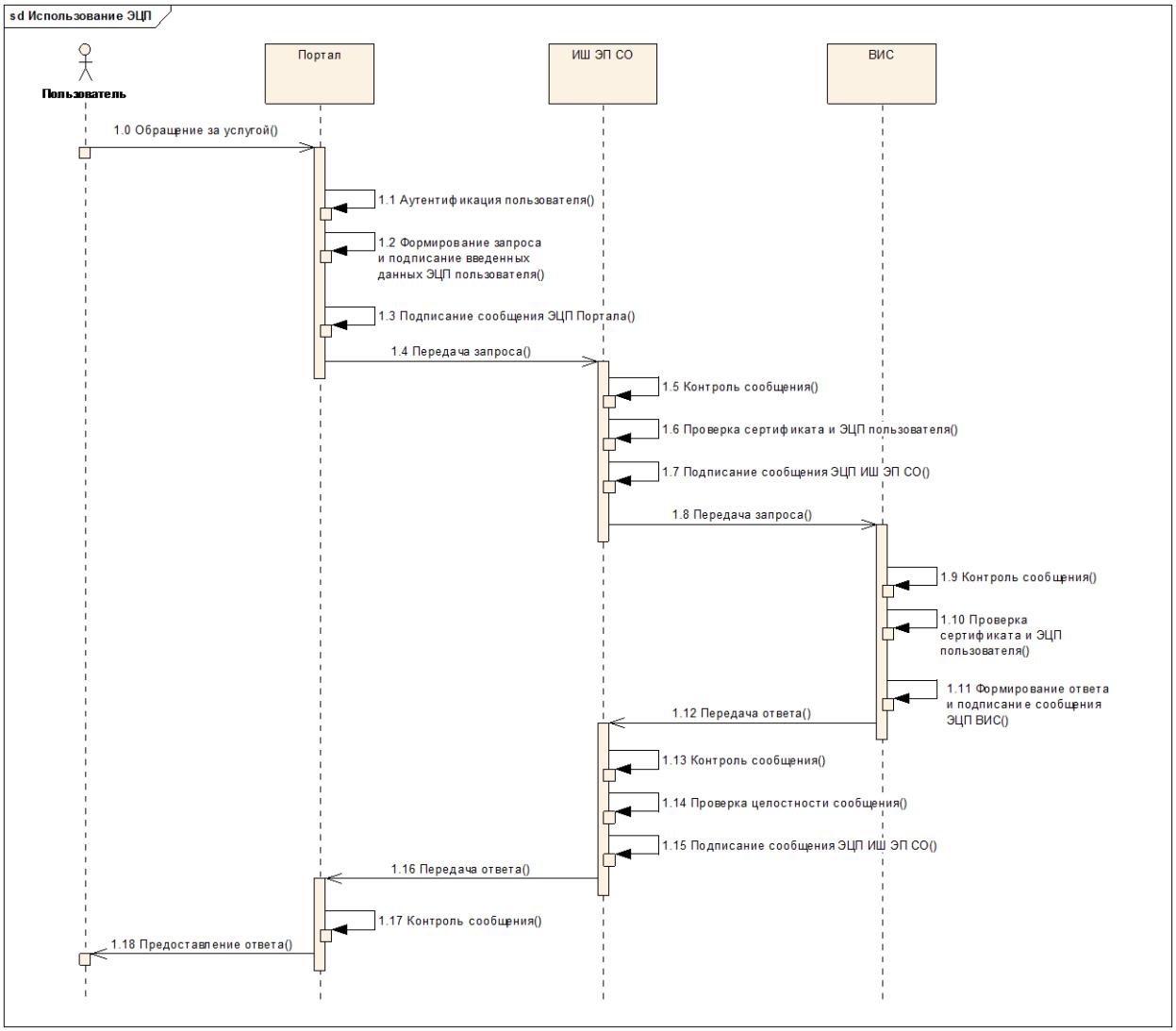


Рисунок 1 – Использование ЭЦП при обмене сообщениями

2. Требования к формированию ЭЦП

ЭЦП данных – ЭЦП, применяемая для обеспечения целостности и неизменности передаваемых данных. Формируется посредством сертификата пользователя или ВИС и помещается в тело сообщения.

ЭЦП сообщения – ЭЦП, применяемая для обеспечения целостности и неизменности сообщения с момента его отправки одной ИС до момента его приема другой ИС. Формируется посредством сертификата ИС (Портал, ИШ ЭП СО, ВИС) и помещается в SOAP заголовок сообщения. При формировании ЭЦП сообщения необходимо следовать установленным правилам [2].

ЭЦП данных и ЭЦП сообщения формируются в соответствии с ГОСТ Р 34.10-2001 [3]. Для формирования ЭЦП используется программное обеспечение ViPNet Криптопровайдер.

2.1. Формирование ЭЦП данных

Схема процесса формирования ЭЦП данных представлена на рисунке 2:

1.0. Информационная система формирует XML с данными.

1.1. Информационная система передает XML на подпись Приложению. Подписанию подлежит не весь документ, а только значения его атрибутов.

1.2. Приложение вызывает функцию подписания ViPNet Криптопровайдера для полученного XML.

1.3. ViPNet Криптопровайдер вычисляет ЭЦП для XML с использованием функции CPSingHash.

1.4. ViPNet Криптопровайдер передает вычисленное значение ЭЦП Приложению.

1.5. Приложение вставляет значение ЭЦП в тег "DigiSign" и передает полученный XML Информационной системе.

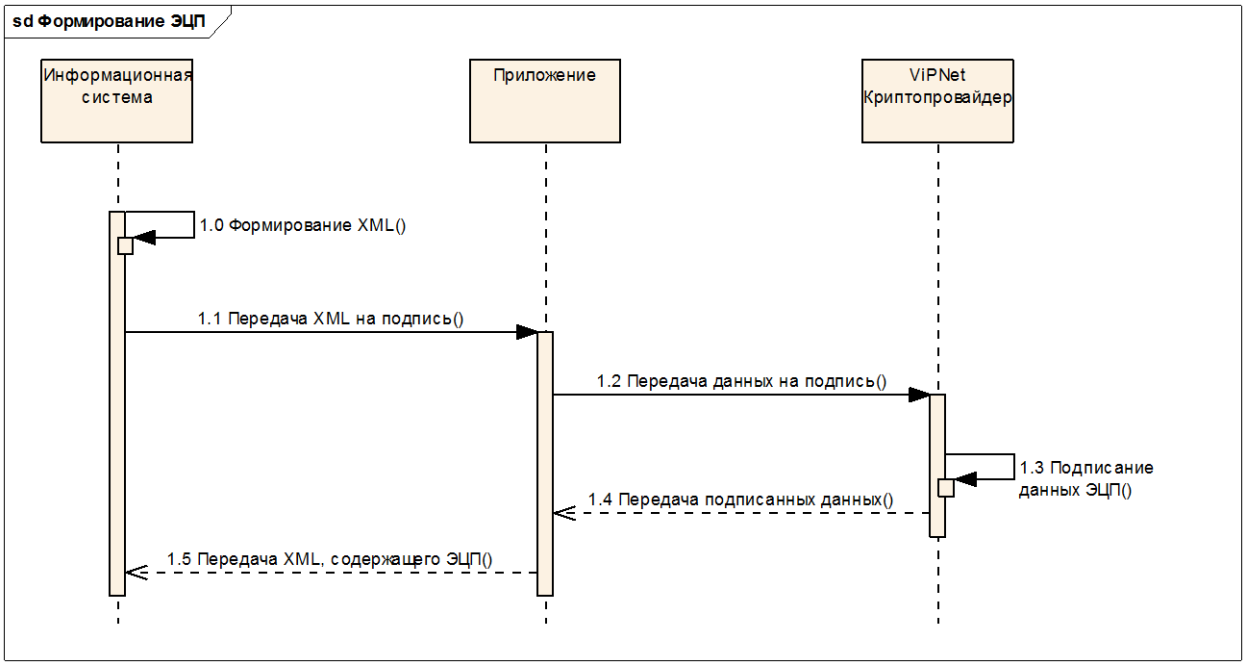


Рисунок 2 – Процесс формирования ЭЦП

2.2. Формирование ЭЦП сообщения

Схема процесса формирования ЭЦП аналогична представленной на рисунке 2:

1.0. Информационная система формирует XML с данными.

1.1. Информационная система передает XML на подпись Приложению.

1.2. Приложение вызывает функцию подписания ViPNet Криптопровайдера для полученного XML.

1.3. ViPNet Криптопровайдер вычисляет ЭЦП для XML с использованием функции CPSingHash.

1.4. ViPNet Криптопровайдер передает вычисленное значение ЭЦП Приложению.

1.5. Приложение вставляет значение ЭЦП в SOAP заголовок сообщения и передает полученный XML Информационной системе.

3. Требования к проверке сертификата и ЭЦП

Проверка действительности сертификатов должна проводиться с использованием списка отзыва сертификатов (CRL).

Проверка ЭЦП должна осуществляться в соответствии с алгоритмом ГОСТ Р 34.10-2001 [3]. Для проверки ЭЦП по алгоритму ГОСТ Р 34.10-2001 [3] используется программное обеспечение ViPNet Криптопровайдер.

Проверка ЭЦП сообщения должна осуществляться в соответствии с установленными правилами [2].

Схема процесса проверки ЭЦП представлена на рисунке 3:

1.0. Информационная система передает Приложению подписанный ЭЦП XML-файл для проверки сертификата и ЭЦП;

1.1. Приложение извлекает из ЭЦП сертификат;

1.2. Приложение запрашивает из удостоверяющего центра CRL;

1.3. Удостоверяющий центр предоставляет CRL;

1.4. Приложение проверяет нахождение в CRL сертификата. При отсутствии сертификата в CRL производится дальнейшая обработка. При обнаружении сертификата в CRL дальнейшая обработка прерывается и происходит переход к шагу 1.9;

1.5. Приложение осуществляет проверку цепочки сертификатов. Если цепочка действительна – производится дальнейшая обработка. При обнаружении недействительного сертификата в цепочке дальнейшая обработка прерывается и происходит переход к шагу 1.9;

1.6. Приложение выполняет запрос целостности ЭЦП к ViPNet Криптопровайдеру;

1.7. ViPNet Криптопровайдер производит проверку целостности ЭЦП с использованием функции CPVerifySignature и формирует ответ с результатом проверки ЭЦП;

1.8. ViPNet Криптопровайдер передает ответ с результатом проверки ЭЦП Приложению;

1.9. Приложение возвращает результат проверки сертификата и ЭЦП, содержащихся в XML-файле, Информационной системе.

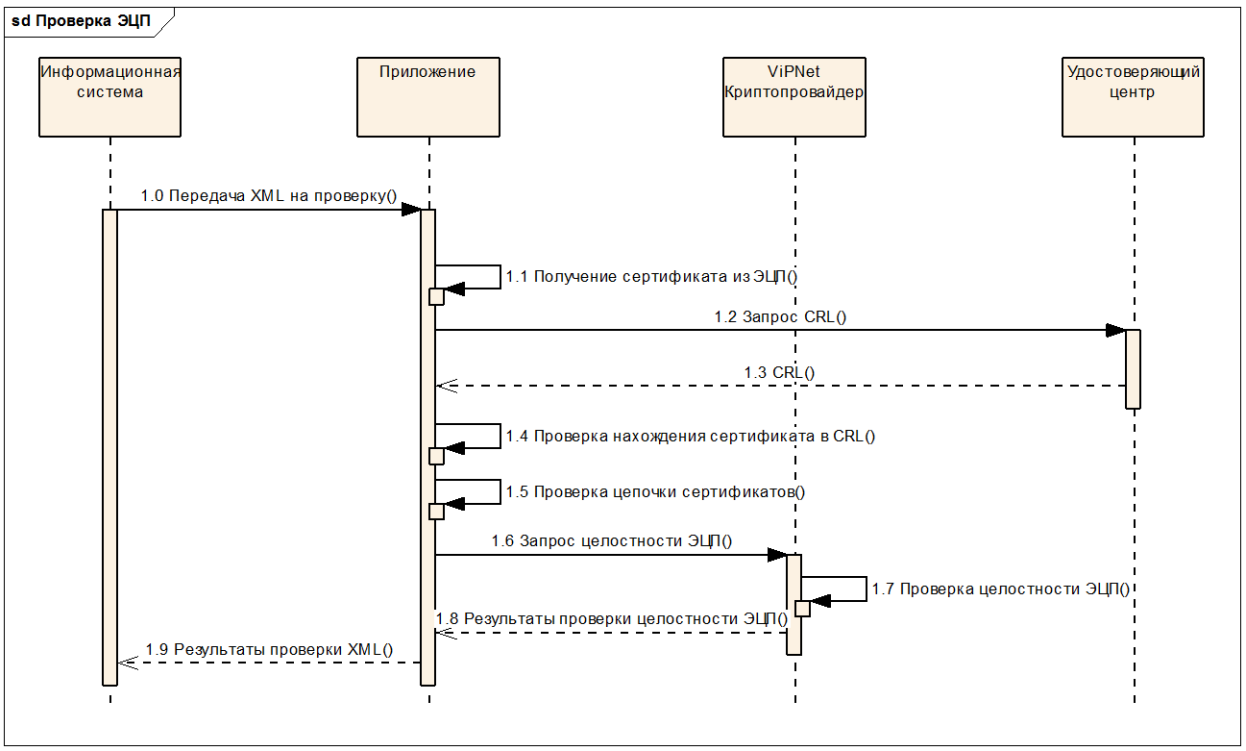


Рисунок 3 – Процесс проверки ЭЦП

4. Требования к структуре файла, подписанного ЭЦП

Структура подписанного ЭЦП XML-файла, должна соответствовать спецификации консорциума W3C «XML — Signature Syntax and Processing» («Синтаксис и обработка подписи XML»), см. ссылку http://www.w3.org/TR/xmldsig-core/.

Спецификация «XML — Signature Syntax and Processing» определяет, что подпись и информация о ней должны содержаться в тэге <Signature>, который имеет следующие части:

- метод канонизации (CanonicalizationMethod) определяет конкретный набор правил для упрощения и структурирования экземпляра XML до подписания. Эти сведения обеспечивают надлежащий вид подписываемых данных, чтобы алгоритм проверки дал положительный результат, если содержательные данные не были изменены;
- метод подписи (SignatureMethod) определяет алгоритм подписи дайджеста сообщения. Дайджест сообщения — это уникальная символьная строка фиксированного размера, она является результатом обработки данных с помощью односторонней хэш-функции, задаваемой методом дайджеста;
- метод дайджеста (DigestMethod) — алгоритм составления дайджеста сообщения, подписываемого с помощью заданного метода подписи. Задание определенного метода дайджеста гарантирует обработку данных одним и тем же способом;
- значение дайджеста (DigestValue) — собственно дайджест сообщения, то есть строка фиксированной длины, выдаваемая в результате обработки данных с помощью алгоритма дайджеста. Такая строка является уникальной и необратимой: ее практически невозможно получить из другого содержимого, как и невозможно воссоздать по ней исходные данные. Это как бы отпечаток пальцев для подписываемых данных; положительный результат сравнения значений дайджеста гарантирует

целостность содержимого;

- значение цифровой подписи (SignatureValue) — это закодированные в base64 [MIME] данные, содержащие значение цифровой подписи;
- информация о ключе (KeyInfo) — дополнительный элемент, позволяющий адресату получить открытый ключ для верификации ЭЦП. Элемент может содержать ключи, имена, сертификаты и информацию по управлению открытыми ключами.
    - тэг X509Data – тэг содержит идентификатор ключа или сертификат X509 (идентификатор сертификата или список отозванных сертификатов). Допускается наличие в тэге нескольких идентификаторов или сертификатов. В нашем случае, тэг X509Data содержит только элемент X509Certificate – сертификат, закодированный в base64.
- структура SignedInfo – структура включает алгоритм канонизации, алгоритм подписи, и один или несколько элементов Reference. SignedInfo может содержать дополнительный признак удостоверения, который позволит ссылаться на другие подписи и объект.
    - тэг Reference, может повторяться один или несколько раз. Тэг описывает алгоритм формирования цифровой подписи, список преобразований, может содержать идентификатор подписываемого объекта
    - тэг Transforms, представляет список элементов преобразования.

Пример формируемой подписи содержится в Приложении А.

5. Состав и назначение полей сертификата

Состав и назначение полей сертификата описываются в положениях и политиках РУЦ. Основные поля сертификата для справки приведены в таблице 1.

РУЦ оставляет за собой право изменять состав и назначение полей в процессе развития систем РУЦ.

Таблица 1 – Состав и назначение полей сертификата

Поле	Обязательность	Назначение	Значение
Version	Да	Версия сертификата ключа подписи	V3
Serial Number	Да	Уникальный регистрационный номер сертификата	
Signature Algorithm	Да	Используемый алгоритм ЭЦП	ГОСТ Р 34.10-2001
Valid From	Да	Дата и время начала срока действия сертификата	день/месяц/год часы/минуты/секунды
Valid To	Да	Дата и время окончания срока действия сертификата	день/месяц/год часы/минуты/секунды

Поле	Обязательность	Назначение	Значение
Subject Public Key Info	Да	Открытый ключ электронной цифровой подписи	
Issuer	Да	Организация, выпустившая сертификат	
country Name	Да	Наименование страны нахождения организации	RU
locality Name	Да	Наименование города нахождения организации	Самара
common Name	Да	Наименование организации	Региональный удостоверяющий центр Правительства Самарской области

Поле	Обязательность	Назначение	Значение
organization Name	Да	Наименование организации полное	Государственное бюджетное учреждение Самарской области «Региональный центр управления государственными и муниципальными информационными системами и ресурсами Самарской области»
postal Address	Нет	Юридический адрес организации	443068, Россия, г.Самара, ул.Н.Панова, д.16
serial Number	Нет	Идентификатор организации	
Subject	Да	Владелец сертификата	
country Name	Да	Наименование страны нахождения организации	RU
locality Name	Да	Наименование местности нахождения организации	Самара

Поле	Обязательность	Назначение	Значение
organization Name	Нет	Наименование организации	Заполняется в случае выдачи сертификата для формирования ЭЦП организации
organizational Unit Name	Нет	Наименование подразделения организации	Заполняется в случае выдачи сертификата для формирования ЭЦП организации
title	Нет	Должность владельца сертификата	Заполняется в случае выдачи сертификата для формирования ЭЦП организации
common Name	Да	Фамилия и имя владельца сертификата	*Иванов Иван*
given Name	Да	Отчество владельца сертификата	*Иванович*

Поле	Обязательность	Назначение	Значение
pseudonym	Да	Псевдоним владельца сертификата	Заполняется в случае выдачи сертификата для формирования ЭЦП информационным ресурсом организации. Содержит наименование или обозначение информационного ресурса.
serial Number	Нет	Идентификатор владельца	
postal Address	Нет	Адрес регистрации владельца сертификата	*443008, Россия, г.Самара, ул.Победы, д.98, кВ.10*
Key Usage	Да	Использование ключа	digitalSignature, nonRepudiation
CRL Distribution Point	Да	Точка распространения списка отозванных сертификатов	
Subject Key Identifier	Да	Идентификатор ключа субъекта	

Поле	Обязательность	Назначение	Значение
Authority Key Identifier	Да	Идентификатор ключа центра сертификации	

6. Список используемых сокращений

Сокращение	Расшифровка
CRL	Certificate Revocation List
XML	Extensible Markup Language
ВИС	Ведомственная информационная система
ИШ ЭП СО	Интеграционная шина электронного правительства Самарской области
РУЦ	Региональный удостоверяющий центр Правительства Самарской области
ЭП СО	Электронное правительство Самарской области
ЭЦП	Электронная цифровая подпись

7. Связанные документы

1. Общесистемные справочники и классификаторы, хранимые в информационной системе ИШ ЭП СО

2.Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)

3.ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

Приложение А. Пример подписи XML-документа

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

<SignedInfo xmlns="http://www.w3.org/2000/09/xmldsig#">

<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" xmlns="http://www.w3.org/2000/09/xmldsig#"/>

<SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gost34310-gost34311" xmlns="http://www.w3.org/2000/09/xmldsig#"/>

<Reference URI="" xmlns="http://www.w3.org/2000/09/xmldsig#">

<Transforms xmlns="http://www.w3.org/2000/09/xmldsig#">

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" xmlns="http://www.w3.org/2000/09/xmldsig#"/>

<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments" xmlns="http://www.w3.org/2000/09/xmldsig#"/>

</Transforms>

<DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gost34311" xmlns="http://www.w3.org/2000/09/xmldsig#"/>

<DigestValue xmlns="http://www.w3.org/2000/09/xmldsig#">**t/A+GU31vOcJ8+T1D8fxjeM8rRmqGea0hCykFo3XyQY=**</DigestValue>

</Reference>

</SignedInfo>

<SignatureValue xmlns="http://www.w3.org/2000/09/xmldsig#">**icWHwH7f56m9LYVEUZNPZKb8Xui21yj/YerQX7zuGSeK6pVrT0bog7dwftqrV4yFQIbJunH0nhC6ljL7SiGFQg==**

</SignatureValue>

<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">

<X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">

<X509Certificate xmlns="http://www.w3.org/2000/09/xmldsig#">

MIIEZDCCBA2gAwIBAgIgtcKQEcC9EJdKUm7gAODvbh8fS4CTr8ekOIT6OmWbkbIwDgYKKwYBBAG1

EQECAgUAMFgxCzAJBgNVBAYTAktaMQ8wDQYDVQQIEwZBTE1BVFkxDjAMBgNVBAoTBUdBTU1BMQ0w

CwYDVQQLEwRURVNUMRkwFwYDVQQDDBDQmtCe0KDQndCV0JLQntCZMCIYDzIwMDgwNTI3MTMzMjIx

WhgPMjAwOTA4MjMxMzMyMjFaMHAxCzAJBgNVBAYTAktaMRUwEwYDVQQHDAzQkNGB0YLQsNC90LAx

IjAgBgNVBAMMGdCa0LDRgNC40LzQvtCyINCg0LXQvdCw0YIxJjAkBgkqhkiG9w0BCQEWF2thcmlt

b3YuZ2FtbWFAZ21haWwuY29tMGMwDgYKKwYBBAG1EQEFCAUAA1EABgIAADqqAAAARUMxAAIAAMck

ifdI3m5wwnXERH718QJyou3Ne2PjlT6Mi8tOC9BwKmMvC7jO/4058hIIHEmKHftAg2fWTOZkZmBW

2TyRyDmjggJ9MIICeTApBgNVHQ4EIgQgtcKQEcC9EJdKUm7gAODvbh8fS4CTr8ekOIT6OmWbkbIw

CwYDVR0PBAQDAgbAMB0GA1UdJQQWMBQGCCsGAQUFBwMDBggr
BgEFBQcDBDAMBgNVHRMEBTADAgEA

MEIGCCsGAQUFBwEBBDYwNDAyBggrBgEFBQcwAYYmaHR0cDovLzE
5Mi4xNjguMTAuMTA6NjIyODAv

Y2dpL3N0YXR1cwAwga0GA1UdIwSBpTCBooAgft6vj68l1xOhQgQyrgt48I
ZCBqDlLWx+R4fqVpjP

YxuhXKRaMFgxCzAJBgNVBAYTAktaMQ8wDQYDVQQIEwZBTE1BVFk
xDjAMBgNVBAoTBUdBTU1BMQ0w

CwYDVQQLEwRURVNUMRkwFwYDVQQDDBDQmtCe0KDQndCV0JLQ
ntCZgiB+3q+PryXXE6FCBDKuC3jw

hkIGoOUtbH5Hh+pWmM9jGzB6BgNVHSAEczBxMG8GCisGAQQBtREL
AQUwYTAfBggrBgEFBQcCARYT

aHR0cDovL3d3dy5nYW1tYS5rejA+BggrBgEFBQcCAjAyMBIWC1Rlc3Qg
UG9saWN5MAMCAQEaHENl

cnRpZmljYXRlIFBvbGljZXMgU3RhdG1lbnQgaEGA1UdHwSBmTCBljC
Bk6AvoC2GK2h0dHA6Ly8x

OTIuMTY4LjEwLjEwOjYyMjgwL2NnaS9SZXZMaXN0LmNybACBAgFmo
lykWjBYMQswCQYDVQQGEwJL

WjEPMA0GA1UECBMGQUxNQVRZMQ4wDAYDVQQKEwVHQU1NQT
ENMAsGA1UECxMEVEVTVDEZMBcGA1UE

AwwQ0JrQntCg0J3QldCS0J7QmTAOBgorBgEEAbURAQICBQADQQB8K
B99CvW6fIl80A9OJJF2OCTA

Tm52HL571GNGPnm95HLeqN6gm8HWRDoQ5dLqHFIKzC8siQOyDJLysj
XFsllG

</X509Certificate>

</X509Data>

```
        </KeyInfo>
</Signature>
```

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Дата	Автор	Содержание изменения