Утверждаю
Генеральный директор
АО «Центр развития экономики»
А.А Бойко

РЕГЛАМЕНТ
ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ ЭТП B2B-CENTER, ОБЕСПЕЧИВАЮЩЕЙ ПРОВЕДЕНИЕ ЗАКУПОК В ЭЛЕКТРОННОЙ ФОРМЕ ДЛЯ НУЖД ГОСУДАРСТВЕННОЙ КОРПОРАЦИИ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»

ОГЛАВЛЕНИЕ

1 Общие положения

1.1. Настоящий Регламент организации электронного документооборота и использования электронной подписи (далее – Регламент) определяет следующие нормы при проведении закупок в электронной форме для нужд Государственной Корпорации по атомной энергии «Росатом» (ГК «Росатом») и организаций ГК «Росатом»:

- принципы взаимодействия пользователей ЭТП B2B-Center при проведении закупок в электронной форме;
- требования к использованию электронной подписи;
- порядок использования электронной подписи в информационной Системе ЭДО ЭТП B2B-Center;
- требования к формированию электронных документов;
- правовые условия, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной.

1.2. Регламент разработан в соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи» от 06.04.2011 г. и требованиями ГК «Росатом» по использованию ЭП на ЭТП.

1.3. Регламент размещен (опубликован) в сети Интернет на сервере по адресу: http://www.b2b-center.ru/help/Регламент_организации_электронного_документооборота_и_использования_электронной_подписи_в_процедурах_Росатом.

1.4. Регламент не определяет порядок получения сертификатов ключей проверки электронной подписи Участниками ЭТП. Данный порядок определяется договорами, правилами и иными нормативными документами между Участником ЭТП и третьей стороной (Удостоверяющим центром, поставщиком средств электронной подписи), осуществляющей функции по созданию и выдаче сертификатов ключей проверки электронной подписи.

1.5. Требования к программно-аппаратным средствам Участника ЭТП, необходимым для работы в Системе ЭДО, размещены в сети Интернет на сервере по адресу: http://www.b2b-center.ru/requirements.html.

1.6. Регламент может включать в себя дополнения и приложения, раскрывающие и детализирующие различные положения организации электронного документооборота и использования электронной подписи. Дополнения, приложения к Регламенту, публикуемые на ЭТП, являются неотъемлемой частью Регламента.

1.7. Субъект Регламента признает Регламент полностью, без изъятий, безусловно и безоговорочно, присоединяется к нему и никогда, ни при каких условиях не будет ссылаться в оправдание своих действий на незнание или непонимание Регламента.

1.8. Исключительное право на внесение изменений и дополнений в Регламент в порядке, изложенном в Регламенте, имеет Администратор ЭДО.

2 Термины и определения

Для целей Регламента используются следующие термины и определения:

Администратор ЭДО – Акционерное общество «Центр электронных расчетов и программ финансирования», обеспечивающее функционирование Системы ЭДО на ЭТП.

Аккредитованный УЦ – удостоверяющий центр, признанный уполномоченным федеральным органом соответствующим требованиям Федерального закона от 06.04.2011 г. № 63-ФЗ.

Владелец сертификата ключа проверки ЭП – лицо, являющееся уполномоченным представителем Участника Системы, которому удостоверяющим центром выдан сертификат ключа проверки электронной подписи.

Квалифицированный сертификат ключа проверки ЭП (квалифицированный сертификат) – сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной

Ключ проверки ЭП - уникальная последовательность символов, однозначно связанная с ключом электронной подписи, предназначенная для проверки подлинности электронной подписи.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

Оператор ЭТП (Оператор) – юридическое лицо, которое на законных основаниях осуществляет предпринимательскую деятельность по обеспечению проведения закупочных процедур в электронной форме на ЭТП. Акционерное общество «Центр развития экономики» (АО «ЦРЭ»).

Партнерский УЦ – подключенный удостоверяющий центр, заключивший договор с Администратором ЭДО.

Подключенный УЦ – удостоверяющий центр, информация о корневых сертификатах и точках распространения списков отозванных сертификатов которого внесена в Систему ЭДО B2B-Center.

Подтверждение подлинности ЭП в электронном документе – положительный результат проверки средством электронной подписи с использованием сертификата ключа проверки электронной подписи принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки электронной подписи и отсутствия изменений в подписанном данной электронной подписью электронном документе после его подписания.

Пользователь – представитель (сотрудник) Участника Системы, либо непосредственно Участник Системы (в случае физического лица), наделенный надлежащими полномочиями по совершению действий в рамках Системы от имени Участника Системы.

Пользователь электронной подписи – пользователь, обладающий правами на использование функциональности ЭП и наделенный владельцем сертификата ключа проверки ЭП надлежащими документированными полномочиями по использованию ЭП в рамках Системы.

Сертификат ключа проверки ЭП – электронный документ или документ на бумажном носителе, выданный УЦ либо доверенным лицом УЦ и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключ проверки ЭП.

Система B2B-Center (Система) - совокупность технических и организационных средств Оператора, включая программно-аппаратные комплексы, обеспечивающая оптимизацию взаимодействия организаций с партнерами и контрагентами, и размещенная во всемирной компьютерной сети Интернет по адресу http://www.b2b-center.ru.

Система ЭДО – система электронного документооборота, представляющая собой совокупность программного обеспечения, а также вычислительных средств и баз данных, предназначенных для передачи зашифрованных и подписанных ЭП электронных документов. Система ЭДО является неотъемлемой функциональной частью общей Системы.

Служба актуальных статусов сертификатов (OCSP-служба) – сервис ЭП, обеспечивающий получение статуса сертификата в режиме реального времени с использованием соответствующего протокола OCSP.

Список отозванных сертификатов - электронный документ с электронной подписью удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей

проверки электронной подписи, которые на определенный момент времени были аннулированы (отозваны) или действие которых было приостановлено[1].

Средство криптографической защиты информации (**СКЗИ**) – средство вычислительной техники, осуществляющее криптографические преобразования информации для обеспечения ее безопасности.

Средство ЭП – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из ю следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Удостоверяющий центр (УЦ) – юридическое лицо или индивидуальный предприниматель, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронной подписи, по распространению средств электронной подписи, а также иные функции, связанные с использованием электронной подписи, предусмотренные действующим законодательством.

Уполномоченное лицо УЦ - физическое лицо, являющееся сотрудником удостоверяющего центра и наделенное удостоверяющим центром надлежащими полномочиями по подписанию от лица удостоверяющего центра электронной подписью удостоверяющего центра сертификатов ключей проверки электронной подписи и списков отозванных сертификатов.

Участник Системы – физическое или юридическое лицо, в том числе, индивидуальный предприниматель, получившее в порядке, установленном Оператором ЭТП, право использования функций Системы в соответствии с уровнем доступа.

Электронная подпись (ЭП, подпись) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронная торговая площадка (ЭТП) – Система электронных торгов B2B-Center, расположенная в сети Интернет на сервере по адресу http://www.b2b-center.ru/ и являющаяся корпоративной информационной системой, порядок использования электронной подписи в которой устанавливается Администратором ЭДО.

Электронное сообщение – информация, представленная в электронной форме, переданная или полученная Пользователем, представляющая собой совокупность структурированных данных, и позволяющая обеспечить ее обработку программно-аппаратным обеспечением Системы ЭДО.

Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. Электронное сообщение, подписанное ЭП и способное быть преобразованным средствами Системы ЭДО в форму, пригодную для однозначного восприятия его содержания.

3 СУБЪЕКТЫ РЕГЛАМЕНТА

Субъектами настоящего Регламента являются:

- Администратор ЭДО, выступающий в лице ответственных сотрудников организации;
- Участники Системы, выступающие в лице владельцев ключей и сертификатов ключей проверки ЭП и пользователей ЭП;
- Удостоверяющие центры, выступающие в лице уполномоченных лиц.

[1] Момент времени формирования списка отозванных сертификатов определяется по значению поля *ThisUpdate* списка отозванных сертификатов. Момент времени, до которого действителен список отозванных сертификатов, определяется по значению поля *NextUpdate* списка отозванных сертификатов.

4 Общий порядок подключения к Системе ЭДО

1. Администратор ЭДО размещает в Системе информацию, необходимую для подключения к Системе ЭДО.

2. Администратор ЭДО предоставляет участникам Системы следующую инфраструктуру Системы ЭДО для получения и обслуживания электронной подписи:

- справочная информация и документы, необходимые для получения ЭП, настройки средств ЭП, установки сертификата ключа проверки ЭП на рабочем месте участника Системы (пользователя ЭП) и иная дополнительная информация;
- проверка работоспособности средств ЭП, установленных на стороне (рабочих местах) участника Системы (пользователя ЭП);
- перечень подключенных УЦ и их текущих статусов;
- перечень партнерских УЦ, предоставляющих участникам Системы услуги по выпуску сертификатов ключей проверки ЭП;
- регистрация в Системе ЭДО сертификатов ключей проверки ЭП.

3. Участник Системы:

- изучает вышеуказанную информацию и документы;
- принимает решение о подключении к Системе ЭДО;
- выбирает партнерский УЦ;
- выбирает пользователя ЭП и направляет администратору ЭДО заявку на получение ЭП.

4. Администратор ЭДО регистрирует заявку участника Системы и немедленно направляет информацию об участнике Системы в выбранный участником Системы УЦ.

5. Участник Системы заключает договор с выбранным УЦ или присоединяется к регламенту работы выбранного УЦ, приобретает сертификат ключа проверки ЭП, ключ ЭП на ключевом носителе и средства ЭП.

6. УЦ регистрирует сертификат для пользователя ЭП участника Системы в Системе ЭДО и передает информацию о выпуске сертификата ключа проверки подписи и его владельце администратору ЭДО.

7. Администратор ЭДО регистрирует участника Системы в Системе ЭДО.

На участнике Системы, получившем ЭП не через ЭТП лежит обязанность самостоятельно зарегистрировать полученный сертификат ключа проверки ЭП для работы на ЭТП.

5 Удостоверяющие центры. Создание ключей и сертификатов ЭП

Договор администратора ЭДО с УЦ не является публичной офертой.

Статус подключенного УЦ может получить только аккредитованный УЦ, выпускающий квалифицированные сертификаты ключей проверки ЭП, удовлетворяющие требованиям создания ЭП усовершенствованного формата.

Приобретение статуса партнерского УЦ включает в себя подключение к Системе ЭДО.

Подключение к Системе ЭДО заключается в регистрации в Системе ЭДО корневых сертификатов УЦ и проверке соответствия формата сертификата ключа проверки ЭП, выпущенного данным УЦ, требованиям, предъявляемым к сертификатам ключей проверки ЭП, используемым в Системе ЭДО.

В случае поступления в адрес Администратора ЭДО обоснованных претензий со стороны Участников Системы на действия партнерского УЦ Администратор ЭДО вправе прекратить статус партнерского УЦ данного УЦ.

Статус партнерского УЦ прекращается при расторжении договора Администратора ЭДО с УЦ.

Сертификаты ключей проверки ЭП, изготовленные УЦ, статус партнерского УЦ которого прекращен, начиная со дня расторжения договора с Администратором ЭДО[2], не могут быть использованы в Системе.

Администратор ЭДО обеспечивает работу участников Системы с действительными сертификатами ключей проверки ЭП, удовлетворяющими требованиям к сертификатам ключей проверки ЭП, используемым в Системе ЭДО в торгах атомной отрасли и выданными подключенными УЦ, выполняющими требования Регламента.

Администратор ЭДО осуществляет регистрацию в Системе ЭДО сертификатов ключей проверки ЭП участников Системы. Необходимыми условиями для регистрации сертификата ключа проверки ЭП на ЭТП для участия в торгах атомной отрасли являются следующие:

- на момент регистрации сертификат ключа проверки подписи не внесен в список
- проверки подписи, отозванных сертификатов, зарегистрированных в Системе ЭДО;
- корневой сертификат подключенного УЦ, выдавшего данный сертификат ключа зарегистрирован в Системе ЭДО;
- сертификат ключа проверки подписи выдан до даты прекращения статуса партнерского УЦ либо организации, представляющей интересы подключенного УЦ.

Формирование ключа ЭП и сертификата ключа проверки ЭП осуществляется в аккредитованном УЦ с помощью сертифицированных средств ЭП на основании заявления владельца сертификата ключа проверки ЭП.

Для возможности использования сертификатов в Системе аккредитованный УЦ создает квалифицированные сертификаты ЭП, технически пригодные для формирования усовершенствованной ЭП.

В сертификате ключа проверки ЭП расширение «Улучшенный ключ» содержит OID 1.2.643.6.7 (Использование в работе систем электронного документооборота и электронных торговых систем B2B-CENTER), устанавливающий правомерность использования сертификата ключа проверки подписи на ЭТП (в Системе электронных торгов B2B-Center).

Сертификат ЭП содержит сведения о протоколе определения состояния сертификата через сеть (OID 1.3.6.1.5.5.7.48.1) с указанием URL-адресов OCSP-служб действующих статусов сертификатов.

Аккредитованный УЦ обеспечивает работоспособность служб онлайновой проверки сертификатов (OCSP-служб) и служб штампов времени (TSP-служб).

6 ТРЕБОВАНИЯ К ФОРМАТУ И СОДЕРЖАНИЮ СЕРТИФИКАТОВ ЭП

Сертификат ключа проверки ЭП, используемый в Системе, должен соответствовать требованиям Приказа ФСБ РФ от 27.12.2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Сертификат ключа подписи должен соответствовать следующей структуре:

Название	Описание	Содержание
Базовые поля сертификаты		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algoritm	Алгоритм подписи	Действующий ГОСТ
Issuer	Издатель сертификата	CN (общее имя)

[2] Момент изготовления сертификата определяется по значению поля *notBefore раздела Validity Period* сертификата ключа проверки подписи.

		C (страна) S (регион) L (населенный пункт) O (организация) OU (подразделение) E (e-mail) ОГРН (ОГРН организации) ИНН (ИНН организации)
Validity Period	Срок действия сертификата	Дата и время начала действия сертификата (notBefore) Дата и время окончания действия сертификата (notAfter)
Subject	Владелец сертификата	CN (общее имя) C (страна) S (регион) L (населенный пункт) STREET (адрес: улица, дом) O (организация) OU (подразделение) T (должность) E (e-mail) SNILS (СНИЛС) INN (ИНН) OGRN (ОГРН)
Publik Key	Ключ проверки ЭП	Открытый ключ
Issuer Signature Algoritm	Алгоритм подписи издателя сертификата	Действующий ГОСТ
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ
Расширения сертификата		
Private Key Validity Period	Срок действия ключа ЭП, соответствующего сертификату	Действителен с (notBefore) Действителен по (notAfter)
Key Usage	Использование ключа	Информация об использовании ключа. Должно обеспечивать использование ключа

		для формирования ЭП и шифрования данных
Extended Key Usage	Улучшенный ключ	Указываются идентификаторы областей использования ключей ЭП и сертификатов ключей проверки ЭП: Проверка подлинности клиента (OID 1.3.6.1.5.5.7.3.2) Защищенная электронная подпись (OID 1.3.6.1.5.5.7.3.4) Использование в работе систем электронного документооборота и электронных торговых систем B2B-CENTER (1.2.643.6.7)
Subject Key Identifier	Идентификатор ключа владельца сертификата	
Authority Key Identifier	Идентификатор ключа издателя сертификата	
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResousceServer/Path/Name.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, Name - имя файла списка отозванных сертификатов
Authority Information Access	Доступ к сведениям центра сертификации	Метод доступа = Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ResousceServer2/Path2/Name2.crf, где ResousceServer2 – имя сервера, Path2 – путь к службе OCSP, Name2 – имя службы OCSP.
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 5280

Поле «Субъект» сертификата ключа подписи, идентифицирующего владельца сертификата ключа подписи, должно содержать следующие компоненты имени:

- компонент «общее имя» (commonName). В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую имя, фамилию и отчество (если имеется) – для физического лица, или наименование – для юридического лица;
- компонент «фамилия» (surName). В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую фамилию физического лица;

- компонент «приобретенное имя» (givenName). В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую имя и отчество (если имеется) физического лица;
- компонент «наименование страны» (countryName). В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую двухсимвольный код страны;
- компонент «наименование штата или области» (stateOrProvinceName). В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование соответствующего субъекта Российской Федерации;
- компонент «наименование населенного пункта» (localityName). В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование соответствующего населенного пункта;
- компонент «название улицы, номер дома» (streetAddress). В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую часть адреса места нахождения соответствующего лица, включающую наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется);
- компонент «наименование организации» (organizationUnitName). В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование подразделения юридического лица;
- компонент «должность» (title). В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование должности лица;
- компонент «электронная почта» (E, EMail). В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую адрес электронной почты владельца сертификата ключа подписи (обязательный к заполнению).

К дополнительным атрибутам имени, необходимость которых устанавливается в соответствии с Федеральным законом, относятся:

OGRN (ОГРН). Значением атрибута OGRN является строка, состоящая из 13 цифр и представляющая ОГРН владельца квалифицированного сертификата – юридического лица. Объектный идентификатор типа атрибута OGRN имеет вид 1.2.643.100.1.

SNILS (СНИЛС). Значением атрибута SNILS является строка, состоящая из 11 цифр и представляющая СНИЛС владельца квалифицированного сертификата – физического лица. Объектный идентификатор типа атрибута SNILS имеет вид 1.2.643.100.3.

INN (ИНН). Значением атрибута INN является строка, состоящая из 12 цифр и представляющая ИНН владельца квалифицированного сертификата. Объектный идентификатор типа атрибута INN имеет вид 1.2.643.3.131.1.1.

В сертификате ключа подписи расширение «Улучшенный ключ» (OID 2.5.29.37) должно содержать значения: «Проверка подлинности клиента» (OID 1.3.6.1.5.5.7.3.2) и «Защищенная электронная почта» (OID 1.3.6.1.5.5.7.3.4).

Список отозванных сертификатов, издаваемых удостоверяющим центром, должен соответствовать стандарту X.509v2 согласно RFC 5280 «Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile» с учетомRFC 4491 «Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algoritms with the Internet X.509 Public Key Infrastructure Certificate and Profile».

7 СРЕДСТВА ЭЛЕКТРОННОЙ ПОДПИСИ

Средство электронной подписи (СКЗИ), используемое участниками Системы, должно обеспечивать применение ЭП и шифрования в соответствии с нормами действующего законодательства Российской Федерации и осуществлять выполнение следующих основных функций и соответствующих документов:

- генерацию и управление ключевой информацией;

- подсчет значения хэш-функции в соответствии с ГОСТ Р 34.11-94;
- шифрование и расшифрование данных в соответствии с ГОСТ 28147-89;
- формирование закрытых и открытых ключей ЭП и шифрования;
- идентификацию, аутентификацию, шифрование, имитозащиту TLS соединений.

СКЗИ должно реализовывать ГОСТ Р 34.10-2001, ГОСТ Р 34.10-94, ГОСТ Р 34-11-94 и ГОСТ 281-89 с учетом RFC 4357 «Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-2001 and GOST R 34.11-94 Algorithms».

СКЗИ должно поддерживать сертификаты открытых ключей стандарта X.509 v3 согласно RFC 3280 «Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile» с учетом RFC 4491 «Using the GOST R 34.10-94, GOST R 34.10-2001 and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile».

СКЗИ должно поддерживать формат криптографических сообщений согласно RFC 3852 «Cryptographic Message Syntax (CMS)» с учетом RFC 4490 «Using the GOST 28147-89, GOST 34.11-94 GOST 34.10-94 and GOST 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».

В состав СКЗИ должно входить средство сетевой аутентификации, обеспечивающее реализацию сетевого протокола SSL/TLS с использованием российских криптографических стандартов ЭП, подсчета хэш-функции и шифрования. Сертификат соответствия ФСБ России должен распространяться на данное средство сетевой аутентификации, реализующее протокол SSL/TLS и входящее в состав СКЗИ.

СКЗИ должно обеспечивать выполнение следующих сервисных функций:

- установка сертификатов открытых ключей на компьютере пользователя ЭП с обеспечением связи сертификата открытого ключа с соответствующим указанному сертификату закрытым ключом;
- копирование и удаление закрытых ключей;
- установка, изменение и удаление пароля на доступ к закрытому ключу;
- сохранение пароля в операционной системе.

Не позднее 31 декабря 2018 г. СКЗИ должно обеспечить использование стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012.

8 ТРЕБОВАНИЯ К ПРИМЕНЕНИЮ ЭП

В Системе ЭДО применяется **квалифицированная электронная подпись в ее усовершенствованном формате**, обеспечивая:

- определение лица, подписавшего электронный документ;
- целостность электронного документа;
- отсутствие необходимости сетевых обращений при проверке ЭП;
- архивное хранение электронных документов;
- доказательное подтверждение момента создания ЭП, предоставляемое полученным на нее штампом времени;
- доказательное подтверждение действительности сертификата ключа ЭП на момент создания подписи, предоставляемое информацией о статусе сертификата, полученной в режиме реального времени.

Отношения в области использования квалифицированной ЭП при совершении юридически значимых действий регулируются Федеральным законом №63-ФЗ «Об электронной подписи».

Квалифицированная ЭП в Системе отвечает установленным Федеральным законом №63-ФЗ «Об электронной подписи» требованиям.

Электронная подпись представляет собой структурированную двоичную запись в формате ASN.1, закодированную в соответствии с правилами DER, описанными в разделе 8.7 X.209.

Подписываемый документ (далее – файл) представляет собой двоичный файл, содержащий подписываемые данные.

Формат ЭП соответствует CAdES стандарта ETSI TS 101 733 Electronic Signature and Infrastructure (ESI) – CMS Advanced Electronic Signature (CAdES) и RFC 5126 «CMS Advanced Electronic Signatures (CAdES)».

В Системе ЭДО при использовании квалифицированных ЭП пользователи ЭП:

- сохраняют в тайне ключ своей ЭП;
- самостоятельно принимают решение о факте или угрозе компрометации своих ключей ЭП и немедленно информируют УЦ о факте их компрометации;
- немедленно прекращают использование колюча ЭП в случае его компрометации;
- соблюдают требования эксплуатационной документации на средство ЭП;
- самостоятельно направляют на регистрацию в Системе сертификаты ЭП, предназначенные для работы в Системе.

Компрометацией ключа ЭП в Системе является угроза доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие события:

- - нарушение конфиденциальности ключа ЭП;
- - потеря ключа ЭП с последующим обнаружением;
- - увольнение работников, имевших доступ к ключам ЭП;
- - нарушение правил хранения и уничтожения ключа ЭП.

При подозрении на компрометацию ключа ЭП пользователь может обратиться в УЦ для осуществления приостановления действия сертификата.

9 ФОРМИРОВАНИЕ И ПРОВЕРКА ЭП

Формирование ЭП электронного документа осуществляется с использованием применяемого средства электронной подписи и программного обеспечения Системы ЭДО.

Формирование электронной подписи осуществляется только владельцем сертификата ключа проверки ЭП, соответствующий ключ ЭП которого действует на момент формирования ЭП.

Создание квалифицированной ЭП на рабочем месте участника Системы производится следующим образом:

1. Выбирается квалифицированный сертификат ключа проверки ЭП из списка сертификатов, зарегистрированных на рабочем месте, который соответствует ключу ЭП.
2. Определяется статус выбранного квалифицированного сертификата ключа проверки ЭП. Если статус сертификата является недействительным, то процедура создания ЭП прекращается, а пользователю выдается сообщение, содержащее причину признания недействительного статуса и рекомендуемые действия пользователя ЭП. В системном журнале формируется сообщение, содержащее код ошибки и расшифровку кода ошибки. Статус квалифицированного сертификата ключа проверки ЭП является действительным, если одновременно выполнены следующие действия:
   - сертификат ключа ЭП действует на текущий момент времени;
   - сертификат ключа ЭП не является аннулированным (отозванным) или приостановленным;
   - сертификат ключа ЭП изготовлен аккредитованным УЦ.

   В противном случае, статус сертификата ЭП признается недействительным.
3. ЭП в электронном документе формируется средством ЭП с использованием ключа ЭП, соответствующего выбранному сертификату ключа ЭП. В случае сбоя или ошибки в работе средства ЭП процедура создания ЭП прекращается, а пользователю выдается сообщение, содержащее код ошибки и расшифровку кода ошибки, а также

рекомендуемые действия пользователя. В системном журнале формируется сообщение, содержащее код ошибки и расшифровку кода ошибки.

4. Сертификат ЭП, использующийся для создания ЭП, сохраняется в атрибутах ЭП.

При создании ЭП клиентские компоненты Системы:

1. Показывают лицу, подписывающему электронный документ, содержание информации, которую он подписывает.
2. Создают ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП.
3. Однозначно показывают, что ЭП создана.
4. В случае сбоя или ошибки в работе средств ЭП при создании ЭП – показывают пользователю ЭП код ошибки и расшифровку кода ошибки, а также рекомендуемые действия пользователя.
5. В случае получения недействительного статуса выбранного сертификата ключа ЭП - показывают причину признания недействительного статуса и рекомендуемые действия пользователя.

Проверка ЭП на рабочем месте участника Системы производится следующим образом:

1. Выбирается сертификат ЭП из атрибутов ЭП.
2. ЭП в электронном документе проверяется средством ЭП с использованием выбранного сертификата ключа ЭП. В случае сбоя или ошибки в работе средства ЭП процедура проверки ЭП прекращается, а пользователю выдается сообщение, содержащее код ошибки и расшифровку кода ошибки, а также рекомендуемые действия пользователя.
3. Определяется статус выбранного сертификата ключа ЭП. Если статус сертификата ключа ЭП является недействительным, то процедура проверки ЭП прекращается, а пользователю выдается сообщение, содержащее причину признания недействительного статуса и рекомендуемые действия пользователя. Статус сертификата ключа ЭП является действительным, если одновременно выполнены следующие условия:
    - сертификат ключа ЭП действует на текущий момент времени;
    - сертификат ключа ЭП не является аннулированным (отозванным) или приостановленным;
    - сертификат ключа ЭП изготовлен аккредитованным УЦ.

В противном случае статус сертификата ключа ЭП признается недействительным.

ЭП документа признается действительной, если получен положительный результат проверки соответствующим сертифицированным средством ЭП с использованием сертификата ключа принадлежности ЭП в электронном документе владельцу сертификата ключа ЭП и отсутствия искажений в подписываемом данной ЭП электронном документе, в противном случае пользователю выдается сообщение, содержащее причину признания ЭП недействительной.

При проверке ЭП клиентские компоненты Системы:

1. Показывают содержимое электронного документа, подписываемого ЭП.
2. Показывают информацию о внесении изменений в подписанный ЭП электронный документ.
3. Указывают на лицо, с использованием ключа ЭП которого подписан электронный документ.
4. В случае сбоя или ошибки в работе средства ЭП при проверке ЭП - показывают код ошибки и расшифровку кода ошибки, а также рекомендуемые действия пользователя.

В случае получения недействительного статуса сертификата ключа ЭП – показывают причину признания недействительного статуса и рекомендуемые действия пользователя.

10 Регистрация событий, связанных с созданием и проверкой ЭП

В Системе регистрация событий, связанных с проверкой ЭП и установлением статуса сертификатов ключей проверки ЭП, осуществляется в журналах событий компонент Системы.

При регистрации событий неудачных попыток проверки ЭП с применением средства ЭП, в журнал событий Системы заносится следующая информация:

- идентификатор события;
- дата и время события (с точностью до секунды, время московское);
- идентификатор документа, к которому относится событие;
- код ошибки результата работы средства ЭП.

При регистрации событий неудачных попыток, связанных с установлением статуса сертификата ключа проверки ЭП при проверке ЭП, в журнал событий Системы заносится следующая информация:

- идентификатор события;
- дата и время события (с точностью до секунды, время московское);
- идентификатор документа, к которому относится событие;
- коды причины неудачных попыток, определяющих какое-либо событие из следующих событий:
  - сертификат ключа проверки ЭП не действует на текущий момент времени (срок действия сертификата ещё не наступил или уже окончен);
  - серийный номер сертификата ключа проверки ЭП находится в списке отозванных сертификатов или получен соответствующий ответ службы актуальных состояний сертификатов;
  - список отозванных сертификатов или служба актуальных состояний сертификатов не доступен;
  - сертификат ключа проверки ЭП изготовлен неаккредитованным удостоверяющим центром.

Применяемые в Системе ЭДО средства защиты информации достаточны для защиты информации от несанкционированного доступа, для подтверждения авторства, подлинности и целостности электронных документов, а также для разрешения конфликтных ситуаций по ним.

11 Содержание и порядок проведения экспертизы ЭП электронного документа

Проведение компьютерно-технической экспертизы по подтверждению подлинности ЭП в электронном документе осуществляется УЦ, изготовившим сертификат ключа ЭП, который использовался при создании ЭП.

УЦ обеспечивает подтверждение подлинности ЭП в электронном документе с ЭП формата, соответствующего стандарту криптографических сообщений Cryptographic Message Syntax (CMS). Решение о соответствии электронного документа стандарту CMS принимает УЦ.

Для подтверждения подлинности ЭП в электронных документах лицо подает заявление в УЦ. Заявление должно содержать следующую информацию:

- дату и время подачи заявления;
- идентификационные данные пользователя, подлинность ЭП которого необходимо подтвердить в электронном документе;
- время и дата формирования ЭП электронного документа;
- время и дата, на момент наступления которых требуется установить подлинность ЭП.

Обязательным приложением к заявлению на подтверждение подлинности ЭП в электронном документе является электронный носитель, содержащий:

- сертификат ключа ЭП, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе – в виде файла стандарта CMS;
- электронный документ в виде одного файла (стандарта CMS), содержащего данные и значение ЭП этих данных.

Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа работников УЦ.

Результатом проведения работ по подтверждению подлинности ЭП в электронном документе является заключение УЦ.

Заключение содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- результат проверки ЭП электронного документа;
- данные, представленные комиссии для проведения проверки;
- отчет по выполненной проверке.
- Отчет по выполненной проверке содержит:
- время и место проведения проверки;
- содержание и результаты проверки;
- обоснование результатов проверки.

Заключение УЦ по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью УЦ. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

Срок проведения работ по подтверждению подлинности ЭП в одном электронном документе и предоставлению заявителю заключения по выполненной проверке не должен превышать десяти рабочих дней с момента поступления заявления в УЦ.

12 РАЗГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

Администратор ЭДО, Оператор не несут ответственность за какой-либо ущерб, потери и прочие убытки, которые понес Участник Системы по причине несоответствия указанных в п. 1.5 Регламента программно-технических средств Участника Системы, необходимых для работы в Системе ЭДО, требованиям Администратора ЭДО.

Администратор ЭДО, Оператор не несут ответственность за какой-либо ущерб, потери и прочие убытки, которые понес Участник Системы по причине ненадлежащего исполнения Регламента, несоблюдения руководств, правил, памяток, инструкций, информационных сообщений на сайте Системы и ЭТП, информации, размещенной в новостях ЭТП, касающихся работы Участника Системы в Системе ЭДО, использования и применения ЭП.

Администратор ЭДО, Оператор не несут ответственность перед Участником Системы в случае, если информация, размещенная Участником Системы в Системе ЭДО, по вине самого Участника Системы (Пользователя) станет известна третьим лицам, которые использовали ее с целью нанести ущерб Участнику Системы.

Администратор ЭДО, Оператор не несут ответственности перед Участником Системы за какой-либо ущерб, потери и прочие убытки, которые понес Участник м по причине нарушений в работе ЭП, которые имели место в Системе ЭДО и которые привели к проблемам в подписании электронных документов.

При этом на Участнике Системы (пользователе ЭП) лежит ответственность постоянно поддерживать работоспособность ЭП в процессе эксплуатации на рабочем компьютере Участника Системы. В том числе на Участнике Системы (пользователе ЭП) лежит ответственность обеспечить работоспособность электронной подписи за 2 (два) часа до планируемого использования ЭП на ЭТП.

Администратор ЭДО, Оператор не несут ответственность перед Участником Системы за любые нарушения УЦ режима круглосуточного информирования Участника Системы и

Администратора ЭДО об актуальном статусе сертификата ключа проверки подписи с использованием службы актуальных статусов (OCSP-службы), включая временную или частичную недоступность OCSP-служб.

Администратор ЭДО несет ответственность за надлежащее хранение и своевременное уничтожение электронных документов в соответствии с действующим законодательством РФ.

13 Прочие условия

Регламент действует и является обязательным для исполнения субъектами Регламента на весь период времени, в течение которого субъект Регламента имеет в своем составе зарегистрированных в Системе ЭДО пользователей.

Не менее чем за 5 календарных дней до начала действия новой версии Регламента Администратор ЭДО уведомляет об этом субъектов Регламента посредством публикации новости или направлением информационных сообщений по адресам электронной почты пользователей Системы.

Субъект Регламента считается признавшим юридическую обязательность новой версии Регламента, если Администратор ЭДО до даты вступления в силу Регламента не получил от субъекта Регламента сообщения об обратном. Если такое сообщение поступило в устной форме, Субъект Регламента в течение 24 часов после направления устного сообщения должен продублировать это сообщение в письменной форме (по почте или курьером). В день получения Администратором ЭДО сообщения Субъекта Регламента об отказе принять новую версию Регламента, Субъект Регламента отключается от Системы ЭДО. К тем сделкам и действиям (операциям), выполнение которых не завершено на момент отключения Субъекта Регламента от Системы ЭДО, и которые должны быть закончены после вступления в силу новой версии Регламента, применяется версия Регламента, действовавшая на момент заключения таких сделок и/или начала выполнения соответствующих действий (операций).