

## **Об удостоверяющем центре службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза**

Решение Коллегии Евразийской экономической комиссии от 25 сентября 2018 года № 154.

В целях реализации пункта 18 Протокола об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза (приложение № 3 к Договору о Евразийском экономическом союзе от 29 мая 2014 года) Коллегия Евразийской экономической комиссии **решила:**

1. Утвердить прилагаемое Положение об удостоверяющем центре службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза.

2. Настоящее Решение вступает в силу по истечении 30 календарных дней с даты его официального опубликования.

*Председатель Коллегии  
Евразийской экономической комиссии*

*Т. Саркисян*

УТВЕРЖДЕНО  
Решением Коллегии  
Евразийской экономической  
комиссии  
от 25 сентября 2018 г. № 154

## **ПОЛОЖЕНИЕ**

### **об удостоверяющем центре службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза**

#### **I. Общие положения**

1. Настоящее Положение определяет назначение и основные задачи удостоверяющего центра службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза (далее соответственно – служба ДТС, Союз), создаваемого в Евразийской экономической комиссии (далее – Комиссия), а также его права, обязанности, ответственность и порядок прекращения деятельности.

2. Основным назначением удостоверяющего центра службы ДТС является обеспечение сертификатами ключей проверки электронной цифровой подписи уполномоченных доверенных третьих сторон Комиссии и государств – членов Союза (далее – государства-члены) с целью организации электронного взаимодействия

доверенных третьих сторон Комиссии и государств-членов в составе службы ДТС для обеспечения с применением электронной цифровой подписи юридической силы электронных документов при международном (трансграничном) обмене электронными документами в рамках Союза.

3. Для целей настоящего Положения используются понятия, которые означают следующее:

"криптографический стандарт" – совокупность технических спецификаций, устанавливающих правила и алгоритмы преобразования информации с использованием криптографического ключа (криптографическое преобразование), в том числе формирования и проверки ЭЦП;

"сертификат ключа проверки ЭЦП" – электронный документ, изданный удостоверяющим центром, подписанный ЭЦП удостоверяющего центра с использованием ключа ЭЦП и содержащий информацию, подтверждающую принадлежность указанного в сертификате ключа проверки ЭЦП определенному субъекту электронного взаимодействия, и иную информацию, предусмотренную соответствующими криптографическими стандартами и требованиями к созданию, развитию и функционированию трансграничного пространства доверия, утверждаемыми Советом Комиссии;

"удостоверяющий центр" – уполномоченный орган или организация, обеспечивающие в соответствии с актами Комиссии, законодательством государства-члена предоставление услуг по изданию, распространению, хранению сертификатов ключей проверки ЭЦП и проверке действительности этих сертификатов;

"электронная цифровая подпись (электронная подпись)", "ЭЦП" – информация в электронном виде, которая присоединена к другой информации в электронном виде или иным образом связана с такой информацией, служит для контроля целостности и подлинности этой информации, обеспечивает невозможность отказа от авторства, вырабатывается путем применения в отношении данной информации криптографического преобразования с использованием закрытого (личного) ключа (ключа ЭЦП) и проверяется с использованием открытого ключа (ключа проверки ЭЦП).

Иные понятия, используемые в настоящем Положении, применяются в значениях, определенных Протоколом об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза ( приложение № 3 к Договору о Евразийском экономическом союзе от 29 мая 2014 года), Концепцией использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов, утвержденной Решением Совета Евразийской экономической комиссии от 18 сентября 2014 г. № 73, и требованиями к созданию, развитию и функционированию трансграничного пространства доверия.

4. Оформление электронных документов осуществляется в соответствии с требованиями к созданию, развитию и функционированию трансграничного пространства доверия и Положением об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, утвержденным Решением Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125.

5. Функции удостоверяющего центра службы ДТС осуществляет Департамент информационных технологий Комиссии.

## **II. Основные задачи удостоверяющего центра службы ДТС**

6. Основными задачами удостоверяющего центра службы ДТС являются:

а) удостоверение соответствия открытого ключа проверки ЭЦП закрытому (личному) ключу, а также подтверждение подлинности сертификатов ключей проверки ЭЦП доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов;

б) обеспечение гарантий доверия к сертификатам ключей проверки ЭЦП доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов при международном (трансграничном) обмене электронными документами в рамках службы ДТС;

в) издание, распространение и хранение сертификатов ключей проверки ЭЦП по запросам доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов, а также проверка действительности этих сертификатов;

г) подтверждение достоверности сведений, указанных в сертификатах ключей проверки ЭЦП, по запросам доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов.

7. Функционирование удостоверяющего центра службы ДТС осуществляется в соответствии с Регламентом удостоверяющего центра службы ДТС согласно приложению (далее – Регламент).

## **III. Права, обязанности и ответственность удостоверяющего центра службы ДТС**

8. В целях осуществления своих функций удостоверяющий центр службы ДТС имеет право:

а) проводить проверку сведений, предоставляемых пользователями (представителями доверенных третьих сторон Комиссии и государств-членов) с целью получения сертификатов ключей проверки ЭЦП;

б) отказывать пользователям в получении сертификатов ключей проверки ЭЦП в случае предоставления ими недостоверных сведений или сведений не в полном объеме для получения сертификатов ключей проверки ЭЦП;

в) прекращать или аннулировать действие выданных сертификатов ключей проверки ЭЦП в следующих случаях:

получение достоверных сведений о нарушении конфиденциальности ключа проверки ЭЦП и (или) иных сведений, которые могут существенным образом сказаться на возможности дальнейшего использования сертификатов ключей проверки ЭЦП;

утрата юридической силы ключей проверки ЭЦП;

утрата соответствующих средств ЭЦП;

изменение сведений о владельце сертификата;

иные случаи, установленные Регламентом или актами органов Союза;

г) обеспечивать и контролировать выполнение пользователями требований к информационной безопасности при эксплуатации средств удостоверяющего центра службы ДТС;

д) принимать участие в разработке и согласовании документов, регламентирующих вопросы деятельности удостоверяющего центра службы ДТС;

е) устанавливать срок действия корневого сертификата ключа проверки ЭЦП удостоверяющего центра службы ДТС и сертификатов ключей проверки ЭЦП пользователей.

9. При осуществлении своих функций удостоверяющий центр службы ДТС обязан:

а) обеспечить регистрацию в установленном порядке пользователей в удостоверяющем центре службы ДТС на основании представленных ими документов (с обязательной проверкой указанных в них сведений);

б) информировать в письменной форме доверенные третьи стороны Комиссии и государств-членов об условиях и порядке использования ЭЦП и средств ЭЦП, о рисках, связанных с использованием ЭЦП, и мерах, необходимых для обеспечения безопасности ЭЦП и ее проверки;

в) ознакомить доверенные третьи стороны Комиссии и государств-членов с порядком работы удостоверяющего центра службы ДТС;

г) актуализировать информацию, содержащуюся в реестре сертификатов ключей проверки ЭЦП доверенных третьих сторон Комиссии и государств-членов, и обеспечивать ее защиту от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий;

д) предоставлять любому лицу по его обращению информацию, содержащуюся в реестре сертификатов ключей проверки ЭЦП доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов, в том числе информацию об аннулировании сертификатов ключей проверки ЭЦП;

е) обеспечивать конфиденциальность созданных удостоверяющим центром службы ДТС сертификатов ключей проверки ЭЦП;

ж) обеспечивать выполнение в полном объеме технических процедур выпуска, проверки статуса, прекращения, возобновления действия и аннулирования сертификатов ключей проверки ЭЦП, а также опубликование информации об аннулированных сертификатах ключей проверки ЭЦП;

з) участвовать по запросам пользователей в разрешении конфликтных ситуаций, связанных с применением сертификатов ключей проверки ЭЦП доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов;

и) обеспечивать хранение в течение не менее 15 лет созданных удостоверяющим центром Комиссии сертификатов ключей проверки ЭЦП, документов на бумажном носителе, на основании которых выпущены сертификаты ключей проверки ЭЦП, и иных документов удостоверяющего центра службы ДТС (с соблюдением установленного в Комиссии порядка уничтожения документов с истекшим сроком архивного хранения);

к) хранить в течение не менее 15 лет реквизиты основного документа, удостоверяющего личность пользователя;

л) аннулировать сертификат ключа проверки ЭЦП удостоверяющего центра службы ДТС в случае компрометации ключа ЭЦП, соответствующего данному сертификату.

10. Удостоверяющий центр службы ДТС несет ответственность в соответствии с актами органов Союза в случае причинения третьим лицам вреда в результате:

а) неисполнения или ненадлежащего исполнения обязанностей, предусмотренных настоящим Положением и актами органов Союза в области регулирования применения ЭЦП;

б) ненадлежащих организации работ и контроля безопасности информации при использовании средств ЭЦП и средств удостоверяющего центра службы ДТС;

в) несоблюдения удостоверяющим центром службы ДТС правил пользования аппаратными и программно-техническими средствами удостоверяющего центра службы ДТС.

#### **IV. Взаимодействие удостоверяющего центра службы ДТС с иными лицами**

11. Удостоверяющий центр службы ДТС взаимодействует со структурными подразделениями Комиссии по вопросам, отнесенным к компетенции удостоверяющего центра службы ДТС.

12. В целях осуществления своих функций в соответствии с Регламентом удостоверяющий центр службы ДТС взаимодействует с иными участниками инфраструктуры открытых ключей (доверенными третьими сторонами государств-членов) от своего имени.

## **V. Прекращение деятельности удостоверяющего центра службы ДТС**

13. Деятельность удостоверяющего центра службы ДТС прекращается по решению Коллегии Комиссии.

14. Удостоверяющий центр службы ДТС в случае принятия решения о прекращении его деятельности информирует об этом доверенную третью сторону Комиссии и доверенные третьи стороны государств-членов не позднее чем за 1 месяц до даты прекращения его деятельности.

15. В случае передачи функций удостоверяющего центра службы ДТС другому удостоверяющему центру передается также реестр сертификатов ключей проверки ЭЦП доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов, выпущенных на дату прекращения деятельности удостоверяющего центра службы ДТС.

16. В случае ликвидации информационных систем удостоверяющего центра службы ДТС реестр сертификатов ключей проверки ЭЦП доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов, а также другие электронные документы и документы на бумажном носителе удостоверяющего центра службы ДТС передаются на архивное хранение в установленном в Комиссии порядке.

ПРИЛОЖЕНИЕ  
к Положению об  
удостоверяющем центре  
службы доверенной третьей  
стороны интегрированной  
информационной системы  
Евразийского экономического  
союза

## **РЕГЛАМЕНТ**

### **удостоверяющего центра службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза**

#### **I. Общие положения**

1. Настоящий Регламент устанавливает порядок взаимодействия участников инфраструктуры открытых ключей, использующих сертификаты, выданные удостоверяющим центром службы доверенной третьей стороны (ДТС) интегрированной информационной системы Евразийского экономического союза (далее соответственно – УЦ службы ДТС, интегрированная система), описание основных процедур и организационно-технических мероприятий, используемых УЦ службы ДТС при выпуске сертификатов ключей проверки электронной цифровой

подписи (электронной подписи) (далее – ЭЦП), сопровождения указанных сертификатов, форматы данных и протоколы работы.

Настоящий Регламент подготовлен в соответствии с рекомендациями RFC 3647. "Certificate Policy and Certification Practices Framework" (Рекомендации по политике выдачи сертификатов и сертификационным практикам).

### 1.1. Наименование документа и идентификация

Наименование документа: Регламент удостоверяющего центра службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза.

Сокращенное наименование: Регламент УЦ службы ДТС.

### 1.2. Участники инфраструктуры открытых ключей интегрированной системы

В соответствии с Рекомендацией МСЭ-Т X.509 "Информационные технологии – Взаимосвязь открытых систем – Справочник: Структуры сертификатов открытых ключей и атрибутов" под инфраструктурой открытых ключей интегрированной системы (далее – ИОК) понимается инфраструктура, способная поддерживать управление открытыми ключами для поддержки услуг аутентификации, шифрования, целостности или фиксации авторства в рамках единого пространства доверия Союза.

#### 1.2.1. Удостоверяющий центр

УЦ службы ДТС – отдел в составе Департамента информационных технологий Евразийской экономической комиссии (далее – Комиссия), осуществляющий функции по обеспечению сертификатами ключей проверки ЭЦП для взаимодействия уполномоченных ДТС интеграционного сегмента Комиссии и национальных сегментов государств – членов Союза (далее – государства-члены).

К основным функциям УЦ службы ДТС относятся:

регистрация доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов;

создание и выдача сертификатов ключей проверки ЭЦП по запросам доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов;

определение полномочий лиц, выступающих от имени доверенной третьей стороны Комиссии или доверенных третьих сторон государств-членов при обращении за получением сертификата ключа проверки ЭЦП, и хранение информации об указанных полномочиях в соответствии с утверждаемыми Комиссией документами, регламентирующими функционирование удостоверяющего центра службы доверенной третьей стороны;

подтверждение владения ключом ЭЦП, который соответствует ключу проверки ЭЦП, указанному соответствующей доверенной третьей стороной в запросе на создание и получение сертификата ключа проверки ЭЦП, и отказ в создании указанного сертификата в случае отрицательного результата при подтверждении владения данным ключом;

установление сроков действия сертификатов ключей проверки ЭЦП. Сертификат ключа проверки ЭЦП действует с момента его выдачи, если иная дата начала действия такого сертификата не указана в самом сертификате, при этом информация о сертификате ключа проверки ЭЦП должна быть внесена удостоверяющим центром службы доверенной третьей стороны в реестр выданных, прекративших действие и аннулированных сертификатов ключей проверки ЭЦП (далее – реестр сертификатов) не позднее указанной в нем даты начала действия такого сертификата;

прекращение действия и аннулирование сертификатов ключей проверки ЭЦП;

ведение реестра сертификатов с включением в него информации, содержащейся в выданных удостоверяющим центром службы доверенной третьей стороны сертификатах ключей проверки ЭЦП, а также информации о дате прекращения действия или аннулирования таких сертификатов и об основаниях прекращения действия или аннулирования;

ведение списка прекративших действие и аннулированных сертификатов ключей проверки ЭЦП (далее – список отозванных сертификатов);

уведомление владельца сертификата ключа проверки ЭЦП об аннулировании его сертификата до внесения соответствующих изменений в реестр сертификатов и список отозванных сертификатов;

проверка уникальности ключей проверки ЭЦП в реестре сертификатов и отказ в создании сертификата ключа проверки ЭЦП случае отрицательного результата проверки уникальности ключа проверки ЭЦП, указанного в запросе доверенной третьей стороны Комиссии или доверенной третьей стороны государства-члена;

актуализация информации, содержащейся в реестре сертификатов и списке отозванных сертификатов, а также ее защита от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий;

хранение информации, внесенной в реестр сертификатов, в течение всего срока деятельности удостоверяющего центра службы доверенной третьей стороны;

доступ на безвозмездной основе доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов к реестру сертификатов с использованием средств интегрированной системы в любое время;

осуществление проверок ЭЦП по обращениям доверенной третьей стороны Комиссии или доверенных третьих сторон государств-членов;

создание штампов времени на квитанциях доверенной третьей стороны Комиссии и квитанциях доверенных третьих сторон государств-членов при обращении таких доверенных третьих сторон с целью подтверждения времени создания электронных документов и их подписания соответствующей ЭЦП;

осуществление иной деятельности, связанной с управлением выданными сертификатами ключей проверки ЭЦП.

### 1.2.2. Пользователи инфраструктуры открытых ключей



Пользователи инфраструктуры открытых ключей (ИОК) делятся на две категории: владельцы сертификатов и доверяющие стороны.

Владельцами сертификатов ключей проверки ЭЦП, выдаваемых УЦ службы ДТС, являются следующие субъекты (осуществляющие генерацию ключевых пар, формирование запроса на получение сертификата, установку на своем рабочем месте сертификата УЦ службы ДТС и другие операции в соответствии с правами и обязанностями владельцев сертификатов ключей проверки ЭЦП):

доверенная третья сторона Комиссии;

доверенные третьи стороны государств-членов (уполномоченные организации – операторы соответствующих сервисов);

УЦ службы ДТС.

Операции, связанные с формированием криптографических ключей, формированием запросов на изготовление сертификатов ключей проверки электронных цифровых подписей (электронных подписей), получением сертификатов ключей проверки электронных цифровых подписей (электронных подписей), получением запросов на прекращение действия и аннулирование сертификатов ключей проверки электронных цифровых подписей (электронных подписей) от имени указанных владельцев сертификатов ключей проверки электронных цифровых подписей (электронных подписей) выполняют уполномоченные лица, полномочия которых подтверждаются в порядке, описанном в пункте 23.2 настоящего Регламента.

Владельцы сертификатов ключей проверки ЭЦП при проведении процедур проверки ЭЦП других пользователей ИОК являются доверяющими сторонами, запрашивающими в УЦ службы ДТС информацию о статусе сертификатов и открытых ключей (полагаясь на нее при проверке ЭЦП и принятии решения о подлинности электронного документа).

Других доверяющих сторон в ИОК интеграционного сегмента интегрированной системы нет.

1.2.2.1. Доверенная третья сторона Комиссии и доверенные третьи стороны государств-членов

Совокупность сервисов ДТС, функционирующих в составе интеграционного сегмента Комиссии и национальных сегментов государств-членов, обеспечивающих единое трансграничное пространство доверия ЭЦП при электронной форме взаимодействия субъектов средствами интегрированной информационной системы Союза, представляет собой единую службу ДТС интегрированной информационной системы (далее – служба ДТС).

В рамках службы ДТС сервисы ДТС предоставляются государствами-членами в лице ДТС государств-членов и Комиссией в лице ДТС Комиссии.

Операторами сервисов ДТС государств-членов являются уполномоченные органы или определенные (аккредитованные) ими организации.

Оператором сервисов ДТС Комиссии является Комиссия.

Основными задачами службы ДТС в рамках интегрированной системы являются:

подтверждение подлинности и актуальности электронных документов и ЭЦП субъектов информационного взаимодействия – владельцев сертификатов, выпущенных удостоверяющими центрами в рамках интегрированной системы, в фиксированный момент времени;

обеспечение гарантий доверия в международном (трансграничном) обмене электронными документами;

обеспечение правомерности применения ЭЦП в исходящих и (или) входящих электронных документах в соответствии с законодательством государств-членов и актами Комиссии.

Сертификат сервера сервиса ДТС (сертификат сервера СДТС) включается в состав квитанций и запросов и используется для проверки ЭЦП в данных квитанциях и запросах, а также идентификации сервера сервиса ДТС.

#### 1.2.2.2. Сервис штампов времени

В инфраструктуре открытых ключей интегрированной системы реализованы сервисы штампов времени. Сервисы штампов времени генерируют штампы времени в соответствии с рекомендациями RFC 3161 (Time-Stamp Protocol) – протоколом штампов времени. Каждый штамп времени удостоверяется исключительно при помощи ключей ЭЦП, созданных специально для сервисов штампов времени.

#### 1.2.2.3. Сервис проверки статуса сертификата

В инфраструктуре открытых ключей интегрированной системы, кроме метода проверки статуса сертификата по списку отозванных сертификатов, предоставляется сервис по проверке статуса сертификата в онлайн-режиме (OCSP). Все ответы сервиса проверки статуса сертификата подписываются при помощи ключей ЭЦП, созданных специально для сервиса проверки статуса сертификата.

#### 1.2.3. Использование сертификатов

Сертификаты, выпускаемые УЦ службы ДТС, используются операторами ДТС в целях обеспечения функционирования службы ДТС.

Области использования сертификатов зависят от политик, в соответствии с которыми выданы сертификаты, утверждаемых руководителем УЦ службы ДТС.

УЦ службы ДТС выдает сертификаты в соответствии со следующими политиками сертификатов ключей проверки ЭЦП:

- сертификаты ключей проверки ЭЦП сервиса сертификации УЦ службы ДТС (далее – сертификаты уполномоченных лиц УЦ, корневые сертификаты УЦ);
- сертификаты ключей проверки ЭЦП сервера сервиса ДТС (СДТС);
- сертификаты ключей проверки ЭЦП сервиса проверки статуса сертификата (СПСС)
- ;
- сертификаты ключей проверки ЭЦП сервиса штампов времени (СШВ).

Сертификаты ключей проверки ЭЦП уполномоченных лиц УЦ службы ДТС предназначены для проверки электронных цифровых подписей сертификатах и списках отозванных сертификатов (далее – СОС).

Сертификаты ключей проверки ЭЦП сервера СДТС предназначены для проверки ЭЦП в квитанциях и идентификации сервера сервиса ДТС. Сертификаты ключей проверки ЭЦП сервера СДТС также используются для проверки подписи запросов на выпуск и отзыв сертификатов, поступающих в УЦ службы ДТС от операторов ДТС.

Сертификаты ключей проверки ЭЦП СПСС предназначены для проверки электронных цифровых подписей в ответах, выдаваемых сервисом проверки статусов сертификатов.

Сертификаты ключей проверки ЭЦП СШВ предназначены для проверки электронных цифровых подписей в штампах времени, выдаваемых сервисом штампов времени, интеграционного и национальных сегментов интегрированной системы.

Не допускается использование сертификатов, выданных УЦ службы ДТС, не предусмотренное политиками, утверждаемыми руководителем УЦ службы ДТС, в соответствии с которыми выпущен сертификат, предусмотренный согласно приложению № 1.

### 1.3. Управление документом

Организация, управляющая Регламентом УЦ службы ДТС: Департамент информационных технологий Евразийской экономической комиссии.

Адрес удостоверяющего центра службы ДТС:

115114, г. Москва, ул. Летниковская, д. 2, стр. 1, стр. 2.

Телефон: +7 (495) 669-24-00, доб. \_\_\_\_\_

Факс: 8 (495) 669-24-15

e-mail: info@ecommission.org

Почтовый и юридический адрес удостоверяющего центра службы ДТС: 119121, г. Москва, Смоленский бульвар, д.3/5, стр. 1

Контактное лицо: \_\_\_\_\_

Процедура утверждения Регламента УЦ службы ДТС: утверждение, а также внесение изменений в настоящий Регламент УЦ службы ДТС и политик сертификатов осуществляются Комиссией в установленном порядке. Изменения публикуются в репозитории в виде новой версии документа.

### 1.4. Обозначения, термины и определения

В настоящем Регламенте используются понятия, приведенные в Протоколе об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза (приложение № 3 к Договору о Евразийском экономическом союзе от 29 мая 2014 года) и следующие термины и определения:

"доверяющая сторона" – участник информационного взаимодействия с использованием инфраструктуры открытых ключей, проверяющий ЭЦП;

"владелец сертификата ключа проверки электронной цифровой подписи" – лицо, которому выдан сертификат ключа проверки ЭЦП;

"заявитель" – физическое лицо, подающее заявление на выпуск сертификата в УЦ службы ДТС;

"ключ проверки электронной цифровой подписи (открытый ключ, ключ проверки ЭЦП)" – уникальная последовательность символов, однозначно связанная с ключом электронной цифровой подписи и предназначенная для проверки подлинности электронной цифровой подписи;

"ключ электронной цифровой подписи (ключ ЭЦП)" – уникальная последовательность символов, предназначенная для создания ЭЦП;

"ключевая пара" – ключ проверки ЭЦП и ключ ЭЦП;

"компрометация ключа ЭЦП" – факт, дающий основание полагать, что тайна ключа ЭЦП может быть раскрыта;

"пользователь УЦ" – владелец сертификата или заявитель;

"сертификат ключа проверки электронной цифровой подписи (сертификат)" – электронный документ, сформированный в соответствии со стандартом X.509 версии 3, содержащий открытый ключ и идентификационные данные его владельца и подписанный ЭЦП уполномоченного лица УЦ;

"список отозванных сертификатов, СОС" – список прекративших действие и аннулированных сертификатов ключей проверки ЭЦП;

"средства ЭЦП" – криптографические средства, используемые для реализации хотя бы одной из следующих функций: создание ЭЦП, проверка ЭЦП, создание ключа ЭЦП и ключа проверки ЭЦП;

"штамп времени" – это доказательства того, что данные существовали до определенного времени (согласно RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)");

"электронная цифровая подпись (электронная подпись) (ЭЦП)" – 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 подписавшего лица.

## **II. Перечень услуг УЦ службы ДТС**

2. Для обеспечения услуг УЦ службы ДТС, предоставляемых в соответствии с перечнем основных функций, предусмотренных пунктом 1.2.1 настоящего Регламента, в УЦ службы ДТС реализованы следующие функциональные компоненты (сервисы):

сервис сертификатов;

сервис штампов времени;  
сервис проверки статуса сертификата;  
сервис регистрации;  
сервис сертификации;  
система защиты информации;  
средства ЭЦП.

Сервис сертификатов обеспечивает доступ к реестру сертификатов ключей проверки ЭЦП и спискам отозванных сертификатов со стороны ДТС национальных сегментов государств-членов и ДТС Комиссии.

Сервис штампов времени предоставляет для ДТС национальных сегментов государств-членов и ДТС Комиссии интерфейс для получения штампов времени при выполнении операций формирования ЭЦП.

Сервис проверки статуса сертификата предоставляет для ДТС национальных сегментов государств-членов и ДТС Комиссии возможность проверки статуса сертификата без запроса списков аннулированных сертификатов в режиме реального времени с использованием протокола OCSP.

Сервис регистрации предоставляет возможность регистрации запросов на выдачу и изменение статуса сертификатов. Сервис обеспечивает хранение регистрационных данных ДТС национальных сегментов государств-членов и ДТС Комиссии, запросов на создание сертификатов ключей проверки ЭЦП.

Сервис сертификации обеспечивает хранение эталонной базы сертификатов ключей проверки ЭЦП и списков аннулированных сертификатов. Сервис используется для формирования ключей ЭЦП, записи ключевой информации на ключевые носители, создания и обработки запросов на изготовление и изменение статуса сертификатов ключей проверки ЭЦП, создания сертификатов ключей проверки ЭЦП и списков аннулированных сертификатов.

Система защиты информации обеспечивает защиту, в том числе криптографическую защиту конфиденциальной информации, обрабатываемой и сохраняемой на технических средствах УЦ, в том числе при резервном копировании.

Средства ЭЦП обеспечивают функции генерации пар ключей ЭЦП, хранения ключевой информации, проверки ЭЦП, генерации ЭЦП, отображения подписываемой и проверяемой информации.

Для обеспечения указанных услуг в УЦ службы ДТС в УЦ службы ДТС выделены следующие доверенные роли, которые может выполнить одно или несколько лиц:

руководитель УЦ службы ДТС – осуществляет общую координацию деятельности УЦ службы ДТС, организует работы по разработке и совершенствованию нормативных актов в области функционирования УЦ службы ДТС, использованию средств ЭЦП;

уполномоченное лицо УЦ службы ДТС (администратор сертификации) – обеспечивает хранение и использование ключа ЭЦП УЦ службы ДТС, принимает

участие в разработке нормативной базы УЦ службы ДТС и использованием средств ЭЦП, разрабатывает планы по обеспечению СДТС Комиссии сертификатами в соответствии с их потребностями, организует работы по разбору конфликтных ситуаций, проводит процедуры подтверждения подлинности ЭЦП в электронных документах по обращениям владельцев сертификатов, подтверждения подлинности ЭЦП уполномоченного лица УЦ службы ДТС в созданных сертификатах ключей проверки ЭЦП;

администратор информационной безопасности УЦ службы ДТС, должностные обязанности которого включают организацию работ по использованию СКЗИ, участие в выработке инструкций для пользователей, обеспечение доведения инструкций и необходимой документации на СКЗИ (в том числе организация периодического контроля целостности установленного ПО СКЗИ), контроль за исполнением их требований.

Средствами удостоверяющего центра реализуются следующие обязательные роли:

системный администратор, в полномочия которого входит администрирование специального ПО на сервере удостоверяющего центра и автоматизированном рабочем месте администратора;

администратор безопасности, обеспечивающий защиту информации и настройку средств защиты;

администратор сертификации, в полномочия которого входит создание сертификатов ключей проверки ЭЦП и списков отозванных сертификатов ключей проверки ЭЦП;

администратор аудита, в полномочия которого входят контроль системных событий и событий средств защиты информации по журналам аудита, а также разбор конфликтных ситуаций.

Одна функциональная роль может быть закреплена за одним или несколькими сотрудниками. Возможно закрепление нескольких функциональных ролей за одним сотрудником при соблюдении условия, что общее количество персонала УЦ службы ДТС не менее 2 человек.

По решению руководства Комиссии численность работников, выполняющих обязанности по эксплуатации УЦ службы ДТС, может быть увеличена пропорционально количеству и сложности решаемых задач.

### **III. Права и обязанности участников инфраструктуры открытых ключей**

#### **3. Права и обязанности УЦ службы ДТС**

УЦ службы ДТС имеет право:

отказать в принятии заявления и выпуске сертификата, если заявитель представил не все документы в соответствии с настоящим Регламентом, документы содержат неполную и (или) некорректную информацию, представленные документы имеют явные признаки фальсификации;

отказать в принятии запроса на сертификат, если средства ЭЦП, при помощи которых сгенерированы ключи и запрос, не совместимы со средствами ЭЦП УЦ службы ДТС;

отказать в отзыве сертификата ключа проверки ЭЦП, если владелец не прошел аутентификацию при запросе на отзыв;

отказать в отзыве сертификата ключа проверки ЭЦП, если истек установленный срок действия соответствующего ключа ЭЦП.

УЦ службы ДТС обязан:

использовать ключ ЭЦП администратора сертификации только для формирования ЭЦП в выпускаемых сертификатах и СОС;

обеспечить конфиденциальность ключа ЭЦП уполномоченного лица УЦ службы ДТС;

предоставить пользователям УЦ сертификат ключа ЭЦП уполномоченного лица в форме электронного документа;

поддерживать СОС в актуальном состоянии в соответствии с настоящим Регламентом;

обеспечить уникальность серийных номеров и ключей проверки ЭЦП в выдаваемых сертификатах;

отозвать сертификат пользователя в кратчайшие сроки по запросу его владельца в соответствии с настоящим Регламентом;

публиковать настоящий Регламент в действующей редакции в репозитории УЦ.

4. Пользователь УЦ службы ДТС имеет право:

обратиться в УЦ службы ДТС с заявлением на выпуск сертификата;

обратиться в УЦ службы ДТС с заявлением на отзыв сертификата;

получить сертификат ключа проверки ЭЦП уполномоченного лица УЦ службы ДТС в форме электронного документа;

получить сертификат из реестра УЦ службы ДТС в форме электронного документа;

получить сертификат из реестра УЦ службы ДТС на бумажном носителе;

обратиться в УЦ службы ДТС для проверки ЭЦП в сертификате, выданном УЦ;

обратиться в УЦ службы ДТС для проверки ЭЦП в документе, подписанном с использованием ключа, соответствующего сертификату, выданному удостоверяющим центром;

использовать СОС и СПСС для проверки статусов сертификатов;

использовать СШВ УЦ для простановки штампов времени.

Пользователь УЦ службы ДТС обязан:

ознакомиться с настоящим Регламентом;

обеспечить конфиденциальность собственного ключа ЭЦП;

использовать ключ ЭЦП только в течение срока его действия;

использовать ключ ЭЦП только в соответствии с политиками, указанными в соответствующем сертификате;

использовать СОС и СПСС для получения информации о статусах сертификатов;

не использовать ключ ЭЦП при наличии оснований полагать, что конфиденциальность ключа ЭЦП нарушена;

незамедлительно уведомить УЦ и запросить отзыв сертификата при компрометации ключа ЭЦП;

использовать для генерации ключевой пары и запросов на сертификаты средства ЭЦП, совместимые со средствами ЭЦП УЦ службы ДТС;

в случае оповещения о проведении внеплановой смены ключей ЭЦП УЦ службы ДТС получить новый корневой сертификат УЦ службы ДТС, созданный кросс-сертификат, выполнить их установку и осуществить обновление локальных списков отзыва на соответствующих серверах ДТС.

#### **IV. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг УЦ службы ДТС**

##### **5. Стоимость услуг**

УЦ службы ДТС осуществляет выпуск сертификатов для обеспечения функционирования службы ДТС на безвозмездной основе.

##### **6. Перечень ключевых носителей**

УЦ службы ДТС в качестве ключевых носителей использует:

доверенное вычислительное устройство (ДВУ) ЭЦП (информация хранится на SSD-диске из состава ДВУ) согласно модели угроз, утвержденной Решением Коллегии ЕЭК от 29.08.17 №101ДСП;

индивидуальные ключевые носители – специально подготовленные USB-flash носители.

Часть ключевой информации, необходимой для инициализации ключа ЭЦП сохраняется в ДВУ, а часть на USB-flash носителе. В ДВУ и на USB-flash носителях информация храниться в защищенном виде.

Инициализация ключей и работа с ключами ЭЦП выполняются исключительно в ДВУ ЭЦП и только при предъявлении соответствующего USB-flash носителя и успешной аутентификации владельца ключа ЭЦП.



## **7. Порядок плановой смены ключей ЭЦП УЦ службы ДТС**

Плановая смена ключей ЭЦП УЦ службы ДТС выполняется не ранее чем по истечении 1 года и не позднее чем по истечении 1 года и 3 месяцев с даты начала действия ключей ЭЦП УЦ в соответствии с требованиями используемого средства ЭЦП.

Процедура плановой смены ключа ЭЦП осуществляется в следующем порядке:

администратор сертификации УЦ службы ДТС совместно с администратором информационной безопасности УЦ службы ДТС формируют новый ключ ЭЦП и соответствующий ему ключ проверки ЭЦП;

формируется и сохраняется в реестре сертификатов самоподписанный сертификат УЦ службы ДТС;

сертификат сохраняется на съемный носитель и устанавливается на сервер УЦ службы ДТС.

Неактуальный ключ ЭЦП УЦ службы ДТС используется только для формирования списков отозванных сертификатов в электронной форме, изданных УЦ службы ДТС в период его действия.

Уведомление пользователей о плановой смене ключей ЭЦП УЦ службы ДТС осуществляется путем публикации нового сертификата УЦ службы ДТС в репозитории УЦ службы ДТС.

## **8. Порядок внеплановой смены ключей электронной подписи УЦ службы ДТС**

Внеплановая смена ключей ЭЦП УЦ службы ДТС выполняется в случае компрометации ключа ЭЦП УЦ службы ДТС или в случае возникновения физической неисправности аппаратной части средств ЭЦП (ДВУ и (или) USB-flash носителя) либо при сбое программного обеспечения, приводящего к невозможности использования средств ЭЦП.

При отсутствии подозрения на компрометацию ключа ЭЦП УЦ службы ДТС смена ключа выполняется в соответствии с порядком плановой смены ключей, указанном в пункте 7 настоящего Регламента.

Процедура смены ключа ЭЦП при его компрометации (или подозрения на компрометацию) осуществляется в следующем порядке:

администратором сертификации УЦ службы ДТС совместно с администратором информационной безопасности УЦ службы ДТС генерируется новая ключевая пара и изготавливается новый сертификат в соответствии с порядком плановой смены ключей, указанном в пункте 7 настоящего Регламента.

выполняется односторонняя кросс-сертификация соответствующего скомпрометированному ключу корневого сертификата УЦ службы ДТС (кросс-сертификат подписывается на новом ключе ЭЦП УЦ службы ДТС);

выполняется процедура аннулирования (отзыва) скомпрометированного корневого сертификата УЦ службы ДТС. Формируемый список отозванных сертификатов подписывается на новом ключе ЭЦП УЦ службы ДТС.

Информирование владельцев сертификатов о внеплановой смене ключей производится путем оповещения с использованием телефонной связи.

При внеплановой смене ключей ЭЦП УЦ службы ДТС администратор ДТС должен получить новый корневой сертификат УЦ службы ДТС, созданный кросс-сертификат, выполнить их установку и осуществить обновление локальных списков отзыва на соответствующих серверах ДТС.

## **9. Действия УЦ службы ДТС по сопровождению сертификатов**

### **9.1. Подача заявления на выпуск сертификата**

Заявление на выпуск сертификата подается в УЦ службы ДТС в форме документа на бумажном носителе, подлинность реквизитов которого проверяется согласно приложению № 2 к настоящему Регламенту. Заявление должно быть заверено подписью заявителя, а также печатью организации – оператора соответствующего ДТС, для которого запрашивается сертификат, либо заверено нотариально в соответствии с законодательством государства – члена по форме согласно приложению № 3 к настоящему Регламенту.

Перечень организаций-операторов сервисов службы ДТС определяется решением Комиссии.

Заявления на выпуск сертификата сервиса подтверждения подлинности ДТС и сертификата службы штампов времени ДТС могут подаваться только уполномоченными сотрудниками организации-оператора ДТС.

При подаче заявлений на выпуск сертификата сервиса подтверждения подлинности (СПП) ДТС и сертификата службы штампов времени ДТС уполномоченным сотрудником организации-оператора ДТС учитывается наличие в ДТС основного и резервного серверов сервисов ДТС. Для обеспечения сертификатами сервисов одной ДТС в УЦ службы ДТС подаются 4 заявления:

- для СПП основного сервера ДТС;
- для СПП резервного сервера ДТС;
- для СШВ основного сервера ДТС;
- для СШВ резервного сервера ДТС.

С заявлениями на выпуск сертификатов ключей проверки ЭЦП сервисов ДТС заявитель предоставляет в УЦ службы ДТС файлы запросов на сертификат ключа

проверки ЭЦП в формате PKCS#10 на отчуждаемом носителе (CD или DVD диске), сгенерированные заявителем непосредственно на сервере соответствующего ДТС.

При смене ключей ЭЦП, в случае, если персона заявителя не меняется, допускается упрощенная подача заявления без прибытия в Комиссию (кроме случаев компрометации ключа ЭЦП) путем пересылки в УЦ службы ДТС носителя с файлом запроса на выпуск сертификата. Запросы на выпуск сертификата, передаваемые в УЦ службы ДТС без личного прибытия в Комиссию, должны быть подписаны на действующем ключе ЭЦП сервиса подтверждения подлинности соответствующей подсистемы ДТС.

## 9.2. Обработка заявления на выпуск сертификата

После успешной аутентификации заявителя администратор сертификации совместно с администратором информационной безопасности УЦ службы ДТС проверяют соответствие идентификационной информации данным, содержащимся в заявлении на выпуск сертификата. Запрос на выпуск сертификата сохраняется в базе данных. При первоначальной регистрации идентификационная информация также заносится в базу данных и заявителю выдается парольная фраза для оперативной аутентификации при запросе отзыва сертификата по телефону.

Заявление на выпуск сертификата передается на обработку в случае, если выполнены следующие требования:

заявитель прошел процедуру аутентификации в соответствии с пунктом 23.2 настоящего Регламента;

файл запроса на сертификат соответствует установленному формату (формат запроса указан в приложении № 1 к настоящему Регламенту), идентификационные данные в запросе совпадают с данными, указанными в заявлении на бумажном носителе;

уникальное имя DN в запросе соответствует требованиям пункта 23.1.1 настоящего Регламента;

алгоритм генерации ключей и подписи запроса является совместимым с используемым в УЦ службы ДТС.

Если хотя бы одно из приведенных требований не выполнено, то заявление на выпуск сертификата отклоняется с обязательным уведомлением заявителя.

## 9.3. Срок обработки заявления на выпуск сертификата

Обработка заявления на выпуск сертификата производится в течение 1 рабочего дня. В случае если УЦ службы ДТС требуются дополнительные данные для аутентификации заявителя, срок обработки может быть увеличен.

# 10. Выпуск сертификата

## 10.1. Выпуск сертификата сервера СДТС

При выпуске сертификата сервера СДТС заявитель предоставляет в УЦ службы ДТС файл запроса в установленном формате, сгенерированный заявителем непосредственно на сервере СДТС. Администратор сертификации УЦ службы ДТС проверяет наличие идентификационной информации из заявления в базе данных УЦ службы ДТС и осуществляет выпуск сертификата на основе файла запроса по шаблону "Сервер СДТС".

Шаблоны сертификатов приведены в приложении № 1 к настоящему Регламенту.

#### 10.2. Выпуск сертификата сервера СПСС

При выпуске сертификата сервера СПСС заявитель предоставляет в УЦ ДТС файл запроса в установленном формате, сгенерированный заявителем непосредственно на сервере СПСС. Администратор сертификации УЦ службы ДТС проверяет наличие идентификационной информации из заявления в базе данных службы ДТС и осуществляет выпуск сертификата на основе файла запроса по шаблону "Сервер СПСС".

Шаблоны сертификатов приведены в приложении № 1 к настоящему Регламенту.

#### 10.3. Выпуск сертификата сервера СШВ

При выпуске сертификата сервера СШВ заявитель предоставляет в УЦ службы ДТС файл запроса в установленном формате, сгенерированный заявителем непосредственно на сервере функционирования СШВ. Администратор сертификации УЦ службы ДТС проверяет наличие идентификационной информации из заявления в базе данных УЦ и осуществляет выпуск сертификата на основе файла запроса по шаблону "Сервер СШВ".

Шаблоны сертификатов приведены в приложении № 1 к настоящему Регламенту.

#### 10.4. Уведомление владельца о выпуске сертификата

После выпуска сертификатов по запросу от оператора ДТС, переданного при личном прибытии уполномоченного представителя в УЦ, администратор УЦ службы ДТС уведомляет владельца о выпуске сертификата путем передачи представителю оператора сертификата на бумажном носителе и сертификата в электронном виде на съемном носителе.

После выпуска сертификата по запросу от оператора ДТС, переданному без личного прибытия уполномоченного представителя в УЦ, администратор УЦ службы ДТС уведомляет владельца о выпуске сертификата посредством телефонной связи либо отправкой почтового сообщения с приложением выпущенного сертификата в электронном виде. Дополнительно в адрес владельца сертификата высылается сертификат на бумажном носителе.

### **11. Приемка сертификата владельцем**

#### 11.1. Подтверждение принятия сертификата

Владельцу сертификата вместе с сертификатом в электронной форме выдается сертификат в форме бумажного документа. Владелец при приеме сертификата обязан ознакомиться с идентификационной информацией, включенной в состав сертификата. В случае если идентификационная информация корректна, владелец заверяет сертификат на бумажном носителе собственноручной подписью. Один экземпляр сертификата на бумажном носителе выдается владельцу, второй экземпляр передается на архивное хранение в УЦ службы ДТС.

Факт подписания сертификата в форме документа на бумажном носителе является подтверждением принятия сертификата.

#### 11.2. Публикация сертификата

Выданный сертификат публикуется на сервере УЦ службы ДТС.

#### 11.3. Срок создания и выдачи сертификата

Срок создания и выдачи сертификата не превышает одного рабочего дня с момента подачи заявления и подтверждающих документов.

## 12. Использование ключей и сертификатов

Цели использования ключей и сертификатов зависят от политики, в соответствии с которой выдан сертификат.

#### 12.1. Ключ и сертификат сервера СДТС

Ключ ЭЦП сервера СДТС используется исключительно для формирования ЭЦП в квитанциях проверки ЭЦП и запросах на проверку к СДТС национальных сегментов в автоматическом режиме.

Сертификат сервера СДТС включается в состав квитанций и запросов и используется для проверки ЭЦП в данных квитанциях и запросах, а также идентификации сервера СДТС.

#### 12.2. Ключ и сертификат сервера СПСС

Ключ ЭЦП сервера СПСС используется только для формирования ЭЦП в OCSP-ответах службы в режиме доверенного ответчика в автоматическом режиме.

Сертификат СПСС включается в структуру OCSP-ответов сервиса и используется для проверки ЭЦП в OCSP-ответе и идентификации СПСС.

#### 12.3. Ключ и сертификат сервера СШВ

Ключ ЭЦП сервера СШВ используется только для формирования ЭЦП в штампах времени, выдаваемых службой по запросам СДТС.

Сертификат СШВ включается сервером сервиса в структуру выдаваемых штампов времени и используется для проверки ЭЦП в штампах времени и идентификации службы.

## 13. Обновление сертификата

Обновление сертификата для существующей ключевой пары не производится. Каждый сертификат выпускается с новой ключевой парой.

## **14. Обновление ключей**

Обновление ключей подразумевает выдачу нового сертификата для новой ключевой пары зарегистрированного владельца сертификата. Процедуры идентификации и выпуска сертификата с новыми ключами аналогичны процедурам первоначальной регистрации и выполняются в соответствии с пунктом 23.2 настоящего Регламента.

## **15. Изменение данных, включаемых в сертификат**

УЦ службы ДТС не производит модификацию сертификатов. При изменении идентификационных данных, включаемых в сертификат, производится выпуск нового сертификата с новой ключевой парой в соответствии с пунктом 20.2 настоящего Регламента.

## **16. Отзыв и приостановление действия сертификата**

### 16.1. Основания для отзыва сертификата

Сертификат ключа проверки ЭЦП, выданный УЦ службы ДТС, подлежит отзыву в случае компрометации ключа ЭЦП согласно пункту 30.3 настоящего Регламента, а также в случае, когда информация, включаемая в сертификат, является неточной или неполной.

Приостановление действия сертификата не поддерживается.

### 16.2. Запрос на отзыв сертификата

Отзыв сертификата, выданного УЦ службы ДТС, может запросить владелец сертификата или руководитель УЦ службы ДТС в письменной форме.

### 16.3. Передача запроса на отзыв сертификата

Запрос на отзыв сертификата может быть передан в УЦ службы ДТС с использованием оптического съемного носителя CD/DVD. При этом запрос подписывается с использованием ключа отзываемого сертификата, выданного УЦ службы ДТС. Запрос на отзыв может быть передан в УЦ службы ДТС также по телефонной связи с аутентификацией владельца сертификата по парольной фразе, назначаемой при первоначальной регистрации.

После передачи запроса на отзыв в УЦ службы ДТС владелец сертификата должен предоставить заявление на отзыв сертификата на бумажном носителе, заверенное личной подписью владельца сертификата, подписью уполномоченного лица и печатью

органа (организации) оператора ДТС либо заверенное нотариально в соответствии с национальным законодательством. Форма заявления приведена в приложении № 4 к настоящему Регламенту.

16.4. Допустимые сроки задержки обработки запроса на отзыв сертификата  
Запрос на отзыв сертификата обрабатывается в течение 1 рабочего дня.

## **17. Требования к проверке статуса сертификата доверяющей стороной**

Доверяющая сторона, получив электронный документ с ЭЦП, обязана проверить сертификат ключа проверки ЭЦП по протоколу проверки статусов сертификатов в оперативном режиме либо по списку отозванных сертификатов, если СПСС недоступен. Если сертификат, при помощи которого проверяется ЭЦП документа, содержится в списке отозванных сертификатов, то такой документ отклоняется доверяющей стороной.

### **17.1. Частота выпуска СОС**

Список отозванных сертификатов выпускается УЦ службы ДТС сразу же после обработки запроса на отзыв сертификата, но не реже 1 раза в 3 месяца (даже при отсутствии изменений в списке), и публикуется в репозитории по адресам:

[http:// <XXX>00.DTS.EEC;](http://<XXX>00.DTS.EEC;)

[http:// <XXX>01.DTS.EEC.](http://<XXX>01.DTS.EEC;)

### **17.2. Максимальное время задержки публикации СОС**

Список отозванных сертификатов публикуется на сервере УЦ службы ДТС непосредственно после выпуска. Максимальное время задержки публикации составляет 1 час.

### **17.3. Сервис проверки сертификатов в режиме реального времени**

УЦ службы ДТС оказывает услуги проверки сертификатов в режиме реального времени. Услуга данного типа предоставляется по протоколу OCSP, описанному в RFC 6960.

Протокол OCSP позволяет получать информацию о статусе сертификата без необходимости получения и проверки полного списка CRL.

Протокол OCSP действует на основе модели запрос – ответ. В ответ на каждый запрос сервер СПСС, входящий в структуру УЦ службы ДТС, пересылает следующую стандартную информацию о статусе сертификата:

правильный (англ. good) – означает положительный ответ на запрос, который следует однозначно интерпретировать как удостоверение того, что сертификат является действительным;

отозванный (англ. revoked) – означает, что сертификат отозван;

неизвестный (англ. unknown) – означает, что проверяемый сертификат не был выдан УЦ службы ДТС.

Сервис OCSP генерирует ответ, основываясь на СОС УЦ службы ДТС.

## **18. Особые требования при замене скомпрометированной пары ключей**

При компрометации ключей соответствующий сертификат немедленно заносится в СОС и выдача нового сертификата производится в порядке, предусмотренном для первоначальной регистрации.

## **19. Основания приостановки действия сертификатов**

УЦ ДТС не приостанавливает действие выданных сертификатов.

## **20. Службы статусов сертификатов**

20.1. Способы информирования о статусе сертификатов, выданных УЦ службы ДТС

Информацию о статусе сертификатов, выданных УЦ службы ДТС, можно получить на основе СОС, публикуемых в репозитории УЦ службы ДТС, а также по протоколу OCSP. Информация о доступе к серверу службы OCSP содержится в каждом выданном сертификате.

20.2. Доступность сервиса

Услуги по проверке статуса сертификата доступны 24 часа в сутки, 7 дней в неделю

21. Депонирование и восстановление ключей

УЦ службы ДТС не осуществляет депонирование и восстановление ключей.

## **22. Репозиторий**

Репозиторий является совокупностью файлов и каталогов, размещенных на сервере УЦ службы ДТС. Репозиторий содержит сертификаты, списки отозванных сертификатов и настоящий Регламент.

Вся информация, опубликованная УЦ службы ДТС в его репозитории, доступна по следующим адресам:

<http://<XXX>00.DTS.EEC>,

<http://<XXX>01.DTS.EEC>

Репозиторий содержит следующую информацию:

все выданные УЦ службы ДТС сертификаты;

актуальные списки отозванных сертификатов;

политики управления сертификатами, утвержденные руководителем УЦ службы ДТС;

актуальную версию настоящего Регламента.

Информация в репозитории публикуется со следующей периодичностью:



сертификаты, выданные УЦ службы ДТС, – непосредственно сразу после выпуска нового сертификата;

списки отозванных сертификатов – не реже 1 раза в 3 месяца и немедленно в случае отзыва ранее выданных сертификатов;

новая версия настоящего Регламента – по факту ее утверждения.

УЦ службы ДТС использует механизмы защиты, предотвращающие несанкционированное добавление, удаление или изменение записей в репозитории.

Доступ к репозиторию обеспечивается 24 часа в сутки, 7 дней в неделю.

УЦ не ограничивает доступ к размещенным сертификатам и СОС по протоколу http.

## 23. Порядок идентификации и аутентификации

23.1. Требования к идентификационной информации, включаемой в состав сертификата

### 23.1.1. Типы имен

Идентификационные данные владельцев сертификатов, а также идентификационные данные УЦ службы ДТС, указываемые в сертификатах, должны представлять собой отличительное имя (DN), закодированное в соответствии с Рекомендациями X.500. Отличительное имя должно быть уникальным в рамках УЦ службы ДТС.

Состав и формат компонентов отличительного имени должны соответствовать рекомендациям X.501

Требования к компонентам имени (к идентификационной информации владельца сертификата) приведены в таблице 1.

Таблица 1

Атрибут	Требования
Distinguished name (DN)	отличительное имя должно быть уникальным в рамках РКІ службы ДТС
Country (C)	двухсимвольный код страны согласно ГОСТ 7.67-2003 (ИСО 3166-1:1997)
Organization (O)	сокращенное наименование организации в соответствии с уставными документами
Description	общее наименование организации
StateOrProvinceName(S)	область нахождения организации, в которой зарегистрирована организация-оператор ДТС
LocalityName (L)	наименование населенного пункта, в котором зарегистрирована организация-оператор ДТС
StreetAddress	адрес нахождения организации-оператора ДТС
Идентификатор информационной системы	
E-Mail Address (E)	адрес электронной почты представителя организации – оператора ДТС, службы или сервиса или адрес электронной почты администратора сертификации

CommonName (CN)	<p>значение поля зависит от политики, в соответствии с которой выдан сертификат:          &lt;псевдоним ДТС&gt; – сертификат сервера СДТС (например, СДТС интеграционного сегмента)          &lt;СПСС ИС &gt; – сертификат проверки статуса сертификата          &lt;псевдоним СШВ&gt; – сертификат службы штампов времени          &lt;фамилия, имя, отчество&gt; – сертификат администратора или оператора</p>
-----------------	--

Имя DN предлагается лицом, представляющим заявление в УЦ службы ДТС. Если данное имя соответствует общим требованиям и является уникальным, т.е. не совпадает с DN другого владельца сертификата, уже зарегистрированного в УЦ службы ДТС, то оно принимается в качестве идентификационных данных и заносится в УЦ службы ДТС при регистрации владельца сертификата.

Для обеспечения уникальности имени DN операторы УЦ службы ДТС могут добавлять различные символы в компонент CN отличительного имени.

### 23.1.2. Анонимные сертификаты

УЦ службы ДТС не выпускает анонимные сертификаты. В качестве псевдонимов используются наименования служб и сервисов.

## 23.2. Процедуры идентификации и аутентификации пользователей УЦ службы ДТС и первоначальной регистрации

Регистрация пользователей УЦ службы ДТС осуществляется, когда физическое лицо, подающее заявление на выпуск сертификата, не имеет ни одного действительного сертификата, выданного УЦ службы ДТС.

После успешной проверки предоставленных данных заявитель вносится в список уполномоченных пользователей УЦ службы ДТС и получает парольную фразу для оперативной идентификации при запросе на отзыв. Заявление на выпуск сертификата обрабатывается и осуществляется выпуск сертификата.

Процедура идентификации определяется утвержденными руководителем УЦ службы ДТС политиками сертификатов.

### 23.2.1. Порядок идентификации и аутентификации при запросе сертификата сервера сервиса подтверждения подлинности ДТС

При подаче заявления на выпуск сертификата идентификация заявителя осуществляется только при личном обращении в УЦ службы ДТС. Заявитель обязан предоставить следующие документы:

заявление на выпуск сертификата на бумажном носителе;

паспорт физического лица, предоставляющего заявку на сертификат;

доверенность на право получения сертификата, выданную организацией – оператором ДТС на имя заявителя;

копию приказа или выписку из приказа по организации о назначении ответственного за эксплуатацию программно-аппаратного комплекса (далее – ПАК) ДТС, заверенную руководителем организации.

Если паспорт, удостоверяющий личность заявителя, является подлинным и фотография в документе является фотографией предъявителя, а заявитель входит в список уполномоченных лиц ДТС (представленный ранее оператором ДТС по электронной почте), то заявитель считается аутентифицированным.

Полномочия заявителя считаются подтвержденными, если подписи и печати организации на доверенности и копии приказа (выписке) являются подлинными (либо доверенность заверена нотариально в соответствии с национальным законодательством), а организация, выдавшая доверенность, входит в перечень организаций – операторов ДТС.

Проверка подлинности документов производится в соответствии с приложением № 2 к настоящему Регламенту.

23.2.2. Порядок идентификации и аутентификации при запросе сертификата сервиса проверки статуса сертификата

При подаче заявления на выпуск сертификата идентификация заявителя осуществляется только при личном обращении в УЦ службы ДТС. Заявитель обязан предоставить следующие документы:

заявление на выпуск сертификата на бумажном носителе;

паспорт физического лица, предоставляющего заявку на сертификат;

доверенность на право получения сертификата СПСС, выданную организацией – оператором УЦ службы ДТС на имя заявителя;

копию приказа или выписку из приказа по организации о назначении ответственного за эксплуатацию СПСС, заверенную руководителем организации.

Если паспорт, удостоверяющий личность заявителя, является подлинным и фотография в документе является фотографией предъявителя, то заявитель считается аутентифицированным.

Полномочия заявителя считаются подтвержденными, если подписи и печати организации на копии приказа (выписке) являются подлинными (либо доверенность заверена нотариально в соответствии с национальным законодательством), а организация, выдавшая доверенность, входит в перечень организаций – операторов ДТС.

Проверка подлинности документов производится в соответствии с приложением № 2 к настоящему Регламенту.

23.2.3. Порядок идентификации и аутентификации при запросе сертификата сервиса штампов времени

При подаче заявления на сертификат СШВ идентификация заявителя осуществляется только при личном обращении в УЦ службы ДТС. Заявитель обязан представить следующие документы:

заявление на выпуск сертификата на бумажном носителе;

паспорт физического лица, предоставляющего заявку на сертификат;

доверенность на право получения сертификата СШВ, выданную оператором ДТС на имя заявителя;

копию приказа или выписку из приказа по организации о назначении ответственного за эксплуатацию СШВ (или ПАК ДТС), заверенную руководителем организации.

Если паспорт, удостоверяющий личность заявителя, является подлинным и фотография в документе является фотографией предъявителя, то заявитель считается аутентифицированным.

Полномочия заявителя считаются подтвержденными, если подписи и печати организации на доверенности копии (выписке) приказа являются подлинными (либо доверенность заверена нотариально в соответствии с национальным законодательством), заявитель назначен ответственным за эксплуатацию СШВ (ПАК ДТС), а организация является оператором СШВ (ПАК ДТС).

Проверка подлинности документов производится в соответствии с приложением № 2 к настоящему Регламенту.

#### 23.2.4. Идентификация и аутентификация при обновлении ключей

Идентификация и аутентификация при подаче заявления на выпуск сертификата при плановой смене ключей производится в порядке, аналогичном порядку первоначальной идентификации, описанному в данном пункте настоящего Регламента, в зависимости от политики сертификата.

#### 23.2.5. Идентификация и аутентификация при подаче запроса после отзыва сертификата

Идентификация и аутентификация при подаче запроса после отзыва сертификата производится в порядке, аналогичном порядку первоначальной идентификации, описанном в данном пункте настоящего Регламента, в зависимости от политики сертификата.

#### 23.2.6. Идентификация и аутентификация при отзыве сертификата

Аутентификация при подаче запроса на отзыв осуществляется по парольной фразе, выдаваемой в процессе первоначальной регистрации. Для оперативной обработки запроса на отзыв владелец сертификата при обращении в УЦ службы ДТС должен назвать свои имя, фамилию, должность и парольную фразу.

Если идентификационные данные владельца сертификата, содержащиеся в базе данных УЦ службы ДТС, и выданная парольная фраза совпадают с указанными при обращении, то владелец сертификата считается аутентифицированным и запрос на отзыв передается на обработку.

При подаче запроса на отзыв с использованием съемного носителя аутентификация пользователя осуществляется путем проверки ЭЦП запроса.

Если идентификационные данные владельца сертификата содержатся в базе данных УЦ службы ДТС и ЭЦП в сообщении верна, то пользователь считается аутентифицированным и запрос обрабатывается.

## **24. Физические, организационные и эксплуатационные меры обеспечения безопасности**

В данном разделе описаны основные мероприятия в области контроля средств физической, организационной защиты и действий персонала, проводимые в УЦ службы ДТС.

### **24.1. Физические меры обеспечения безопасности**

УЦ службы ДТС размещается в контролируемой зоне – пространстве, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

Физической границей контролируемой зоны УЦ службы ДТС являются ограждающие конструкции, периметры помещений, в которых размещены технические средства, используемые для получения сертификатов пользователей УЦ службы ДТС, расположенные в Комиссии по адресу размещения УЦ службы ДТС.

### **24.2. Физический доступ**

Помещения УЦ службы ДТС расположены в Комиссии и оборудованы системой контроля и управления доступом. Доступ в помещения УЦ службы ДТС разрешен только авторизованному персоналу и иным лицам в сопровождении ответственного сотрудника УЦ службы ДТС.

### **24.3. Электроснабжение и кондиционирование воздуха**

В случае пропадания основного питания система автоматически переходит на резервное питание от источников бесперебойного питания.

Серверное помещение УЦ службы ДТС оснащено системой кондиционирования воздуха и вентиляции, поддерживающей следующие параметры микроклимата:

температура воздуха в пределах от 18 до 24 °С (предельная скорость ее изменения – 3 °С в час);

влажность воздуха от 30 до 75 процентов без конденсации влаги (предельная скорость ее изменения – 6 процентов в час);

предельное содержание пыли – не более 10-6 г/м<sup>3</sup>.

### **24.4. Подверженность воздействию влаги**

Местоположение УЦ службы ДТС не подвержено природным рискам наводнения.

### **24.5. Противопожарные меры безопасности и защита**

Серверное помещение УЦ службы ДТС оборудовано системой автоматического пожаротушения в соответствии с ГОСТ Р 53246-2008 и Правилами противопожарного

режима в РФ, утвержденными Постановлением Правительства Российской Федерации от 2 апреля 2012 года № 390.

#### 24.6. Хранение носителей информации

Для резервного копирования в УЦ службы ДТС используются USB носители. Носители, на которых хранятся архивы, а также текущие копии данных хранятся в огнестойких сейфах, расположенных в административных помещениях.

#### 24.7. Утилизация носителей информации

Ключевые носители форматируются в соответствии с эксплуатационной документацией и вновь используются для хранения ключей.

Аппаратные криптографические модули (HSM) по окончании использования обнуляются в соответствии с эксплуатационной документацией производителя. Обнуление HSM производится также при передаче в сервисный центр в случае их выхода из строя.

### 25. Управление персоналом

#### 25.1. Квалификация персонала

Обслуживающий персонал должен уметь выполнять все необходимые процедуры, определяемые эксплуатационной документацией, разрабатываемой на стадии ввода в действие, и знать:

базовые понятия технологии открытых ключей;

нормативно-правовые основы деятельности удостоверяющих центров и юридически значимого электронного документооборота;

назначение, основные характеристики и реализуемые алгоритмы программного комплекса УЦ службы ДТС;

порядок организации работы с документами при обеспечении деятельности сервисов УЦ службы ДТС;

порядок обработки персональных данных.

#### 25.2. Документация, предоставляемая персоналу

Руководство УЦ службы ДТС предоставляет персоналу УЦ доступ к документам, необходимым для выполнения должностных обязанностей.

### 26. Ведение журналов аудита

#### 26.1. Типы регистрируемых событий

ПАК УЦ службы ДТС регистрирует следующие виды событий:

системные события общесистемного программного обеспечения;

помещение запроса на сертификат проверки ЭЦП;

принятие запроса на сертификат проверки ЭЦП;

выпуск сертификата ключа проверки ЭЦП;

отклонение запроса на сертификат проверки ЭЦП;  
выпуск списка отозванных сертификатов проверки ЭЦП;  
невыполнение внутренней операции программной компоненты.

Структуры записей событий соответствуют эксплуатационной документации программного обеспечения реализации целевых функций удостоверяющего центра и общесистемного программного обеспечения.

#### 26.2. Частота обработки записей регистрируемых событий

Анализ записей регистрируемых событий ежедневно проводится администратором аудита. В случае возникновения инцидентов безопасности анализ записей регистрируемых событий проводится в рамках расследования данных инцидентов.

#### 26.3. Срок хранения записей регистрируемых событий

Записи регистрируемых событий хранятся в файлах на системном диске до момента превышения заданных для них максимальных значений объема. В этот период времени они доступны в оперативном режиме по запросу уполномоченного лица или уполномоченного процесса. По истечении данного срока создается резервная копия журналов событий на отчуждаемых носителях.

Резервные копии журналов событий хранятся в течение установленного срока, не менее 7 лет.

#### 26.4. Защита записей регистрируемых событий

Журналы событий защищены от просмотра, модификации и удаления средствами прикладного и общесистемного программного обеспечения.

#### 26.5. Условия сбора записей аудита

Регистрируемые события автоматически записываются в журналы средствами прикладного и общесистемного программного обеспечения.

#### 26.6. Уведомление субъекта события, вносимого в журнал регистрации

При записи события в журнал регистрации уведомление субъекта этого события не производится.

## **27. Анализ уязвимостей**

Администратор аудита при периодическом просмотре журналов событий в соответствии с эксплуатационной документацией анализирует содержимое журналов на предмет отсутствия записей о попытках несанкционированного доступа (далее – НСД) к программно-техническим средствам УЦ. При наличии записей о попытках НСД о данном факте сообщается администратору информационной безопасности.

## **28. Ведение архива**

#### 28.1. Типы архивных записей

В УЦ службы ДТС архивации подлежат следующие типы данных:

получаемые заявки, выдаваемые сертификаты и СОС, имеющие электронную форму, которые поступили от конечного пользователя или были ему переданы в форме файла или электронного сообщения;

регистрационные данные пользователей;

реестр выданных сертификатов;

журналы аудита;

внутренняя и внешняя корреспонденция (в бумажной и электронной форме) УЦ службы ДТС с пользователями, а также доверяющими сторонами;

документы и данные, использованные в процессе удостоверения личности.

#### 28.2. Срок хранения архива

УЦ службы ДТС хранит архив на протяжении всего срока эксплуатации УЦ, от момента запуска УЦ службы ДТС в промышленную эксплуатацию до момента прекращения его деятельности.

#### 28.3. Защита архива

Архив УЦ службы ДТС размещается на контролируемой территории. Доступ к архиву имеют только уполномоченные лица, выполняющие доверенные роли в УЦ службы ДТС.

#### 28.4. Резервное копирование архива

Вся архивируемая информация в электронном виде копируется на внешние автономные носители.

#### 28.5. Восстановление данных из резервной копии архива

Восстановление данных из резервной копии выполняется оператором в соответствии с эксплуатационной документацией. Проверка целостности данных резервной копии выполняется автоматически штатными средствами программного обеспечения УЦ службы ДТС непосредственно перед восстановлением данных. При нарушении целостности восстановление данных из резервной копии не выполняется.

### **29. Замена ключей и сертификата уполномоченного лица УЦ службы ДТС**

Ключ ЭЦП уполномоченного лица УЦ службы ДТС заменяется не реже 1 раза в 3 года. Замена ключа сопровождается заменой сертификата ключа проверки ЭЦП уполномоченного лица.

Все владельцы сертификатов ключей проверки ЭЦП обязаны получить новый сертификат уполномоченного лица УЦ службы ДТС из репозитория УЦ службы ДТС и установить его на СДТС без удаления предыдущего сертификата.

### **30. Восстановление при компрометации и сбоях**

#### 30.1. Процедура восстановления в случае компрометации



При компрометации ключа ЭЦП уполномоченного лица УЦ службы ДТС УЦ службы ДТС изготавливает внеочередной список отзыва сертификатов, после чего производится смена ключей и сертификата уполномоченного лица УЦ службы ДТС.

УЦ службы ДТС обязан принять все возможные меры по информированию владельцев сертификатов и доверяющих сторон о факте компрометации и в кратчайшие сроки произвести замену всех выданных сертификатов, используя новый сертификат уполномоченного лица.

### 30.2. Случаи повреждения оборудования, программных и(или) аппаратных сбоев

В случае повреждения оборудования, программных и (или) аппаратных сбоев, сведения о происшествии сообщаются обнаружившим данный факт сотрудником Комиссии руководителю и администратору информационной безопасности УЦ службы ДТС, которая доводит эти сведения до руководства, расследует происшествие и принимает необходимые меры по устранению последствий с использованием резервных копий и запасного оборудования.

### 30.3. Компрометация ключа ЭЦП УЦ службы ДТС

К событиям, связанным с компрометацией, относятся следующие события:

потеря ключевых носителей, в том числе с их последующим обнаружением;

увольнение по любой причине сотрудников, имеющих доступ к ключевым носителям или к ключевой информации на данных носителях (возможность такого доступа определяется в зависимости от конкретной реализации системы со средствами ЭЦП и от технологии обработки информации данной системой);

возникновение подозрений об утечке информации или ее искажении в системе;

нарушение целостности печати на сейфе с ключевыми носителями или утрата контроля за ключом от такого сейфа;

утрата пользователем контроля за ограничением доступа к ключевому носителю в процессе эксплуатации им системы;

случаи, когда невозможно достоверно установить, что произошло с ключевым носителем (например, его разрушение и невозможность опровергнуть подозрение на то, что разрушение носителя произошло не в результате попытки доступа к нему злоумышленника);

другие виды разглашения ключевой информации, в результате которых ключи ЭЦП могут стать доступными несанкционированным лицам и (или) процессам.

При наступлении перечисленных событий владелец ключа ЭЦП, исполняющий доверенную роль в УЦ службы ДТС, в кратчайший срок уведомляет администратора УЦ службы ДТС и запрашивает отзыв сертификата. Получение нового сертификата осуществляется в порядке, описанном в настоящем Регламенте.

## **31. Восстановление работоспособности после аварии**

Персонал УЦ службы ДТС принимает все возможные меры по восстановлению работоспособности УЦ после аварии в течение не более чем 8 часов с использованием резервных копий данных и запасного оборудования.

## **32. Технические средства безопасности**

### **32.1. Генерация и установка ключевой пары**

#### **32.1.1. Генерация ключевой пары**

Ключевая пара УЦ службы ДТС генерируются на автоматизированном рабочем месте (АРМ) администратора в соответствии с эксплуатационной документацией. Генерация ключей УЦ осуществляется администратором сертификации совместно с администратором информационной безопасности УЦ службы ДТС.

Ключевые пары СПСС и СШВ УЦ службы ДТС генерируются на сервере УЦ в соответствии с эксплуатационной документацией. Генерация ключей УЦ осуществляется администратором сертификации УЦ службы ДТС.

Ключевые пары СПП и СШВ ДТС национальных сегментов и интеграционного сегмента интегрированной системы генерируются непосредственно на сервере ДТС уполномоченным сотрудником оператора ДТС в соответствии с эксплуатационной документацией на подсистему ДТС.

Для генерации ключей в УЦ и ДТС Комиссии используется доверенное вычислительное устройство средств ЭЦП (ДВУ ЭЦП). Для защиты сохраняемой ключевой информации дополнительно используются специально подготовленные USB-flash носители.

Для инициализации ключа ЭЦП в ДВУ кроме наличия информации, хранимой в ДВУ, дополнительно требуется ввод пароля доступа и данных, хранимых на USB-flash носителе.

#### **32.1.1.1. Предоставление личного ключа ЭЦП пользователю**

УЦ службы ДТС не имеет доступ к ключам ЭЦП пользователей, так как в соответствии с настоящим Регламентом каждый пользователь самостоятельно осуществляет генерацию ключевой пары.

#### **32.1.1.2. Передача ключа проверки ЭЦП в УЦ службы ДТС**

Пользователь осуществляет самостоятельную генерацию ключей и передает в УЦ службы ДТС ключ проверки ЭЦП в составе файла запроса на сертификат в электронном виде с использованием электронных носителей.

#### **32.1.1.3. Предоставление ключа проверки ЭЦП доверяющим сторонам**

Предоставление ключа проверки ЭЦП УЦ службы ДТС доверяющим сторонам осуществляется путем публикации сертификата ключа проверки ЭЦП, содержащего ключ проверки ЭЦП, в репозитории УЦ службы ДТС.

Все сертификаты, выданные УЦ службы ДТС включают расширение AuthorityInformationAccess, содержащее ссылку на файл корневого сертификата УЦ службы ДТС, опубликованного в репозитории УЦ службы ДТС.

#### 32.1.2. Размеры ключей

В соответствии с эксплуатационной документацией на используемые средства ЭЦП размеры ключей составляют:

длины ключей электронной цифровой подписи:

ключ электронной цифровой подписи – 512 бит;

ключ проверки электронной цифровой подписи – 1024 бит.

длины ключей, используемых при шифровании:

симметричный ключ – 256 бит.

#### 32.1.3. Параметры генерации ключа проверки ЭЦП и проверка качества ключей

Для генерации ключей пользователи УЦ службы ДТС используют ДВУ. Ключевым носителем при этом является SSD-диск из состава ДВУ. В качестве ключевых носителей также используются индивидуальные ключевые USB-носители.

Параметры генерации ключа проверки ЭЦП задаются используемым средством ЭЦП автоматически.

Алгоритм генерации ключей соответствует ГОСТ Р 34.10-2012 согласно Решению Коллегии ЕЭК от 2.06.16 №49ДСП.

При получении запроса на сертификат УЦ службы ДТС проверяет полученный в запросе ключ на совместимость с используемым средством ЭЦП, его разрядность, а также его уникальность. При совпадении полученного ключа с уже имеющимся в базе данных УЦ службы ДТС отклоняет запрос и уведомляет пользователя, подавшего запрос с повторным ключом, о необходимости генерации новой ключевой пары и запроса на сертификат.

#### 32.1.4. Цели использования ключей

Способ применения ключа определен в поле KeyUsage стандартных расширений сертификата, соответствующего X.509 v3.

Ключ ЭЦП уполномоченного лица УЦ службы ДТС может использоваться только для формирования ЭЦП в выпускаемых сертификатах (бит 5 keyCertSign) и СОС (бит 6 cRLSign).

Ключи конечных пользователей используются для формирования ЭЦП. Использование каждого бита в поле KeyUsage соответствует правилам, изложенным в RFC 5280.

#### 32.1.5. Защита ключа ЭЦП уполномоченного лица УЦ службы ДТС

Ключ ЭЦП уполномоченного лица (администратора сертификации) УЦ службы ДТС хранится в защищенном (зашифрованном) виде в ДВУ ЭЦП АРМ администратора УЦ службы ДТС.

Для инициализации в ДВУ ЭЦП ключа уполномоченного лица требуется последовательный ввод ключевых носителей администраторов УЦ (с вводом паролей доступа) и наличие служебных данных, хранимых на SSD-диске из состава ДВУ.

Ключ ЭЦП уполномоченного лица в период эксплуатации (от момента его создания до момента уничтожения) находится в ДВУ ЭЦП и не может быть отчужден на какие-либо внешние носители (функция депонирования ключей ДВУ ЭЦП не поддерживается).

#### 32.1.6. Стандарты криптографического модуля

Форматы ключей и криптографические операции, выполняемые аппаратным криптографическим модулем, соответствуют стандартам ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012.

#### 32.1.7. Депонирование ключей ЭЦП

УЦ службы ДТС не осуществляет депонирование ключей ЭЦП.

#### 32.1.8. Резервная копия ключа ЭЦП

УЦ службы ДТС не осуществляет резервирование ключей ЭЦП.

#### 32.1.9. Хранение ключа ЭЦП по окончании срока действия

Ключ ЭЦП по окончании срока действия подлежит удалению с использованием штатных функций средств ЭЦП и средств УЦ службы ДТС.

#### 32.1.10. Создание и уничтожение ключа ЭЦП УЦ службы ДТС

Ключ ЭЦП уполномоченного лица УЦ службы ДТС постоянно находится в ДВУ с момента его создания и до его удаления при выводе из эксплуатации.

#### 32.1.11. Хранение ключа ЭЦП в криптографическом модуле

Ключ ЭЦП уполномоченного лица УЦ службы ДТС хранится в аппаратном криптографическом модуле в зашифрованном виде.

#### 32.1.12. Способ активации ключа ЭЦП

Ключ ЭЦП уполномоченного лица УЦ службы ДТС инициализируется при последовательном предъявлении съемных ключевых носителей администраторов УЦ (с вводом паролей доступа) и наличии служебных данных, хранимых на SSD-диске из состава ДВУ.

#### 32.1.13. Резервное копирование репозитория

Репозиторий УЦ службы ДТС подвергается периодическому резервному копированию в соответствии с порядком резервного копирования, установленным в УЦ службы ДТС.

#### 32.1.14. Сроки действия сертификатов и ключей

Сроки действия ключей ЭЦП и сертификатов ключей проверки ЭЦП определяются эксплуатационной документацией используемого средства ЭЦП.

Сроки действия ключей и сертификатов УЦ службы ДТС:

максимальный срок действия ключей ЭЦП – до 3 лет;

максимальный срок действия ключей проверки ЭЦП – до 7 лет.

Сроки действия ключей и сертификатов пользователей:  
максимальный срок действия ключа ЭЦП – до 3 лет;  
максимальный срок действия ключа проверки ЭЦП – до 7 лет.

#### 32.1.15. Данные активации

Для ключей ЭЦП УЦ службы ДТС в качестве данных активации выступают:  
данные, считываемые ДВУ с USB-flash носителя;  
пароли доступа к USB-flash носителю;  
служебные данные, хранимые на SSD-диске ДВУ.

### **33. Безопасность программно-аппаратного обеспечения**

Мероприятия по обеспечению безопасности программно-аппаратного комплекса УЦ службы ДТС осуществляются администратором информационной безопасности УЦ службы ДТС.

Первоначальная установка и настройка программного обеспечения на АРМ и серверах УЦ осуществляется системным администратором УЦ службы ДТС с эталонного диска.

Корпуса серверов, АРМ администратора и ДВУ опечатываются личной печатью администратора информационной безопасности УЦ службы ДТС в соответствии с эксплуатационной документацией. Перед началом работы производится визуальный контроль целостности корпуса и печатей (пломб). При обнаружении вскрытия корпуса и/или повреждении печатей (пломб) дальнейшая работа запрещается, о данном факте докладывается руководителю УЦ.

В процессе эксплуатации технических средств УЦ запрещается вносить изменения в состав, конструкцию, электрическую и монтажную схемы УЦ службы ДТС.

Ремонт технических средств осуществляется на предприятии-изготовителе указанных средств. После проведения ремонта проводится процедура специальной проверки и специальных исследований технических средств.

Ввод в состав УЦ дополнительных аппаратных средств без проведения тематических исследований, специальных проверок и специальных исследований данных средств не допускается.

### **34. Средства контроля целостности среды функционирования**

Средства динамического контроля целостности программного обеспечения средств УЦ и среды функционирования входят в состав базовой операционной системы QR ОС.

Стартовый и периодический контроль целостности выполняется средствами АПМДЗ из состава ТС УЦ службы ДТС.

### **35. Сетевая безопасность**

Сетевая безопасность обеспечивается при помощи межсетевых экранов с фильтрацией трафика, а также сегментированием сети. На межсетевых экранах разрешены подключения по портам и протоколам, необходимым для бесперебойного функционирования системы. Все остальные порты и протоколы недоступны. Отдельный сегмент сети выделен для публикации общедоступных данных.

На внешнем сегменте используется средство обнаружения вторжений.

ПРИЛОЖЕНИЕ № 1  
к Регламенту  
удостоверяющего центра  
службы доверенной третьей  
стороны интегрированной  
информационной системы  
Евразийского экономического  
союза

## **ШАБЛОНЫ запросов на сертификаты, сертификатов и список отозванных сертификатов**

### Шаблон запроса на сертификат

Запрос на сертификат представляет собой структуру в формате PKCS#10 и является последовательностью трех полей, из которых первое содержит основное тело запроса (certificationRequestInfo), второе – информацию о типе алгоритма, использованного для подписания запроса на сертификат (signatureAlgorithm), а третье – электронную цифровую подпись, которой подписан запрос (signatureValue).

Запросы на сертификаты ЭЦП УЦ службы ДТС содержат как минимум следующие основные поля:

Version: первая версия (v1(0)) формата запроса на сертификат;

Subject: уникальное имя (DN) конечного пользователя, получающего сертификат;

SubjectPublicKeyInfo: значение открытого ключа вместе с идентификатором алгоритма;

Attributes: коллекция атрибутов, которые могут содержать информацию о расширениях, сохраняемых в сертификат.

Значения основных полей и расширений определяются в зависимости от политики, в соответствии с которой выдается сертификат ключа проверки ЭЦП.

### Запрос на сертификат сервера СДТС

Название поля	Значение или ограничения значения
Version (версия)	Version 1
Subject (субъект, имя DN)	имя DN соответствует требованиям X.501. Common Name (CN) = <Наименование сервиса ДТС>, Organization (O) = <Сокращенное наименование организации>,

	Organization Unit (OU) = <Наименование подразделения>, mailAddress (E) = <адрес электронной почты администратора ПАК ДТС>
Subject Public Key Info (открытый ключ субъекта)	кодированное поле соответствует требованиям, описанным в RFC 2986, и содержит информацию об открытых ключах ГОСТ 34.10-2012 (то есть с идентификатором ключа, длиной ключа в битах и значения открытого ключа)
KeyUsage (OID расширения 2.5.29.15) (использование ключа) – содержится в Attributes	digitalSignature, nonRepudiation
ExtendedKeyUsage (OID расширения 2.5.29.37) (расширенное использование ключа) – содержится в Attributes	Dvcs (OID 1.3.6.1.5.5.7.3.10)
SubjectKeyIdentifier (OID расширения 2.5.29.14) – содержится в Attributes	уникальный идентификатор открытого ключа субъекта
CertificatePolicy (OID расширения 2.5.29.32) (политика сертификата) – содержится в Attributes	идентификатор политики: iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-____(X) id-_____(X) id-_____(X) ...
Signature Algorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Signature (подпись)	подпись запроса на сертификат генерируется и кодируется в соответствии с требованиями, определенными в RFC 2986.

### Запрос на сертификат сервера СПСС

Название поля	значение или ограничения значения
Version (версия)	Version 1
Signature Algorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Subject (субъект, имя DN)	имя DN соответствует требованиям X.501. Common Name (CN) = <Псевдоним СПСС>, Organization (O) = <Сокращенное наименование организации>, Organization Unit (OU) = <Наименование подразделения>, mailAddress (E) = <адрес электронной почты администратора OCSP сервера>
Subject Public Key Info (открытый ключ субъекта)	кодированное поле соответствует требованиям, описанным в RFC 2986, и содержит информацию об открытых ключах ГОСТ 34.10-2012 (то есть с идентификатором ключа, длиной ключа в битах и значения открытого ключа).
KeyUsage	

(OID расширения 2.5.29.15) (использование ключа) – содержится в Attributes	digitalSignature, nonRepudiation,
ExtendedKeyUsage (OID расширения 2.5.29.37) (расширенное использование ключа) – содержится в Attributes	OCSPSigning (OID 1.3.6.1.5.5.7.3.9)
SubjectKeyIdentifier (OID расширения 2.5.29.14) – содержится в Attributes	уникальный идентификатор открытого ключа субъекта
CertificatePolicy (OID расширения 2.5.29.32) (политика сертификата) – содержится в Attributes	идентификатор политики: iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-____(X) id-_____(X) id-_____(X) ...
Signature Algorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Signature (подпись)	подпись сертификата генерируется и кодируется в соответствии с требованиями, определенными в RFC 2986.

### Запрос на сертификат сервера СШВ

Название поля	значение или ограничения значения
Version (версия)	Version 1
Subject (субъект, имя DN)	имя DN соответствует требованиям X.501. Common Name (CN) = <Псевдоним СШВ>, Organization (O) = <Сокращенное наименование организации>, Organization Unit (OU) = <Наименование подразделения>, mailAddress (E) = <адрес электронной почты администратора TSP сервера>
Subject Public Key Info (открытый ключ субъекта)	кодируемое поле соответствует требованиям, описанным в RFC 2986, и содержит информацию об открытых ключах ГОСТ 34.10-2012 (то есть с идентификатором ключа, длиной ключа в битах и значения открытого ключа).
KeyUsage (OID расширения 2.5.29.15) (использование ключа) – содержится в Attributes	digitalSignature, nonRepudiation,
ExtendedKeyUsage (OID расширения 2.5.29.37)	



(расширенное использование ключа) – содержится в Attributes	timestamping (OID 1.3.6.1.5.5.7.3.8)
SubjectKeyIdentifier (OID расширения 2.5.29.14) – содержится в Attributes	уникальный идентификатор открытого ключа субъекта
CertificatePolicy (OID расширения 2.5.29.32) (политика сертификата) – содержится в Attributes	идентификатор политики: iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-____(X) id-_____(X) id-_____(X) ...
Signature Algorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Signature (подпись)	подпись сертификата генерируется и кодируется в соответствии с требованиями, определенными в RFC 5280

### Шаблон сертификата ключа проверки ЭЦП

Сертификат ключа проверки ЭЦП в соответствии со стандартом X.509 v.3 является последовательностью трех полей, из которых первое содержит содержимое сертификата (tbsCertificate), второе – информацию о типе алгоритма, использованного для подписания сертификата (signatureAlgorithm), а третье – электронную цифровую подпись, которой подписан сертификат (signatureValue).

Сертификаты ключей проверки ЭЦП УЦ службы ДТС содержат как минимум следующие основные поля:

Version: третья версия (X.509 v.3) формата сертификата;

SerialNumber: серийный номер сертификата, уникальный в рамках удостоверяющего центра;

Signature Algorithm: идентификатор алгоритма, применяемого удостоверяющим центром, выдающим сертификаты для подписания сертификата;

Issuer: уникальное имя (DN) Удостоверяющего центра;

Validity: срок действия сертификата, определенный началом (notBefore) и окончанием (notAfter) действия сертификата;

Subject: уникальное имя (DN) конечного пользователя, получающего сертификат;

SubjectPublicKeyInfo: значение открытого ключа вместе с идентификатором алгоритма;

Signature: подпись генерируется и кодируется в соответствии с RFC 5280.

Значения основных полей и расширений определяются в зависимости от политики, в соответствии с которой выдается сертификат ключа проверки ЭЦП.

### Сертификат сервера СДТС

--	--

Название поля	значение или ограничения значения
Version (версия)	Version 3
Serial Number (серийный номер)	уникальное значение во всех сертификатах, выдаваемых УЦ службы ДТС
Signature Algorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (издатель, имя DN)	Common Name (CN) = УЦ службы ДТС, Organization (O) = ЕЭК, Organization Unit (OU) = ИТ, Country (C) = RU
Not before (начало срока действия)	основное время согласно UTC (Universal Coordinate Time)
Not after (окончание срока действия)	основное время согласно UTC (Universal Coordinate Time)
Subject (субъект, имя DN)	имя DN соответствует требованиям X.501. Common Name (CN) = <Наименование сервиса ДТС>, Organization (O) = <Сокращенное наименование организации>, Organization Unit (OU) = <Наименование подразделения>, mailAddress (E) = <адрес электронной почты администратора ПАК ДТС>
Subject Public Key Info (открытый ключ субъекта)	кодируемое поле соответствует требованиям, описанным в RFC 5280, и содержит информацию об открытых ключах ГОСТ 34.10-2012 (то есть с идентификатором ключа, длиной ключа в битах и значения открытого ключа)
KeyUsage (OID расширения 2.5.29.15) (использование ключа)	digitalSignature, nonRepudiation
ExtendedKeyUsage (OID расширения 2.5.29.37) (расширенное использование ключа)	Dvcs (OID 1.3.6.1.5.5.7.3.10)
CertificatePolicy (OID расширения 2.5.29.32) (политика сертификата)	идентификатор политики: iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-_____(X) id-_____(X) id-_____(X) ...
AuthorityInformationAccess (OID расширения 1.3.6.1.5.5.7.1.1) (Доступ к сертификату УЛ УЦ службы ДТС)	<b>URL файла сертификата УЛ УЦ службы ДТС следующего вида:</b> http:// <XXX>00.DTS.EEC/RootТТРСА.crt, http:// <XXX>01.DTS.EEC/RootТТРСА.crt <b>URL сервера СПСС следующего вида:</b> http:// <XXX>00.DTS.EEC/<псевдоним_СПСС>/ocsp.srf, http:// <XXX>01.DTS.EEC/<псевдоним_СПСС>/ocsp.srf
CRLDistributionPoint (OID расширения 2.5.29.31) (точка распространения СОС)	<b>URL файла СОС УЦ службы ДТС:</b> http:// <XXX>00.DTS.EEC/RootТТРСА.crl, http:// <XXX>01.DTS.EEC/RootТТРСА.crl
BasicConstraints	

(OID расширения 2.5.29.19)	конечный субъект
SubjectKeyIdentifier (OID расширения 2.5.29.14)	уникальный идентификатор открытого ключа субъекта
Signature (подпись)	подпись сертификата генерируется и кодируется в соответствии с требованиями, определенными в RFC 5280

### Сертификат сервера СПСС

Название поля	значение или ограничения значения
Version (версия)	Version 3
Serial Number (серийный номер)	уникальное значение во всех сертификатах, выдаваемых УЦ службы ДТС
Signature Algorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (издатель, имя DN)	Common Name (CN) = УЦ службы ДТС, Organization (O) = ЕЭК, Organization Unit (OU) = ИТ, Country (C) = RU
Not before (начало срока действия)	основное время согласно UTC (Universal Coordinate Time)
Not after (окончание срока действия)	основное время согласно UTC (Universal Coordinate Time)
Subject (субъект, имя DN)	имя DN соответствует требованиям X.501. Common Name (CN) = <Псевдоним СПСС>, Organization (O) = <Сокращенное наименование организации>, Organization Unit (OU) = <Наименование подразделения>, mailAddress (E) = <адрес электронной почты администратора OCSP сервера>
Subject Public Key Info (открытый ключ субъекта)	кодируемое поле соответствует требованиям, описанным в RFC 5280, и содержит информацию об открытых ключах ГОСТ 34.10-2012 (то есть с идентификатором ключа, длиной ключа в битах и значения открытого ключа)
KeyUsage (OID расширения 2.5.29.15) (использование ключа)	digitalSignature, nonRepudiation,
ExtendedKeyUsage (OID расширения 2.5.29.37) (расширенное использование ключа)	OCSPSigning (OID 1.3.6.1.5.5.7.3.9)
CertificatePolicy (OID расширения 2.5.29.32) (политика сертификата)	идентификатор политики: iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-_____(X) id-_____(X) id-_____(X) ...
AuthorityInformationAccess (OID расширения 1.3.6.1.5.5.7.1.1)	<b>URL файла сертификата УЛ УЦ службы ДТС следующего вида:</b> http:// <XXX>00.DTS.EEC/RootTTPCA.crt, http:// <XXX>01.DTS.EEC/RootTTPCA.crt URL сервера СПСС следующего вида:

(Доступ к сертификату УЦ службы УЦ ДТС)	http:// <XXX>00.DTS.EEC/<псевдоним_СПСС>/ocsp.srf, http:// <XXX> 01.DTS.EEC/<псевдоним_СПСС>/ocsp.srf
SubjectKeyIdentifier (OID 2.5.29.14)	уникальный идентификатор открытого ключа субъекта
CRLDistributionPoint (OID расширения 2.5.29.31) (точка распространения СОС)	URL файла СОС УЦ службы ДТС: http:// <XXX>00.DTS.EEC/RootТТРСА.crl, http:// <XXX>01.DTS.EEC/RootТТРСА.crl
Signature (подпись)	подпись сертификата генерируется и кодируется в соответствии с требованиями, определенными в RFC 5280

### Сертификат сервера СШВ

Название поля	значение или ограничения значения
Version (версия)	Version 3
Serial Number (серийный номер)	уникальное значение во всех сертификатах, выдаваемых УЦ службы ДТС
Signature Algorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (издатель, имя DN)	Common Name (CN) = УЦ службы ДТС, Organization (O) = ЕЭК, Organization Unit (OU) = ИТ, Country (C) = RU
Not before (начало срока действия)	основное время согласно UTC (Universal Coordinate Time)
Not after (окончание срока действия)	основное время согласно UTC (Universal Coordinate Time)
Subject (субъект, имя DN)	имя DN соответствует требованиям X.501. Common Name (CN) = <Псевдоним СШВ>, Organization (O) = <Сокращенное наименование организации>, Organization Unit (OU) = <Наименование подразделения>, mailAddress (E) = <адрес электронной почты администратора TSP сервера>
Subject Public Key Info (открытый ключ субъекта)	кодируемое поле соответствует требованиям, описанным в RFC 5280, и содержит информацию об открытых ключах ГОСТ 34.10-2012 (то есть с идентификатором ключа, длиной ключа в битах и значения открытого ключа)
KeyUsage (OID расширения 2.5.29.15) (использование ключа)	digitalSignature, nonRepudiation
ExtendedKeyUsage (OID расширения 2.5.29.37) (расширенное использование ключа)	timestamping (OID 1.3.6.1.5.5.7.3.8)
CertificatePolicy (OID расширения 2.5.29.32) (политика сертификата)	идентификатор политики: iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-_____(X) id-_____(X) id-_____(X) ...
SubjectKeyIdentifier	

(OID расширения 2.5.29.14)	уникальный идентификатор открытого ключа субъекта
<b>AuthorityInformationAccess</b> (OID расширения 1.3.6.1.5.5.7.1.1) (Доступ к сертификату УЛ УЦ службы ДТС)	URL файла сертификата УЛ УЦ службы ДТС следующего вида: http:// <XXX>00.DTS.EEC/RootТТРСА.crt, http:// <XXX>01.DTS.EEC/RootТТРСА.crt URL сервера СПСС следующего вида: http://<XXX>00.DTS.EEC/<псевдоним_СПСС>/ocsp.srf,      http://<XXX>01.DTS.EEC/<псевдоним_СПСС>/ocsp.srf
<b>CRLDistributionPoint</b> (OID расширения 2.5.29.31) (точка распространения СОС)	URL файла СОС УЦ службы ДТС: http:// <XXX>00.DTS.EEC/RootТТРСА.crl, http:// <XXX>01.DTS.EEC/RootТТРСА.crl
Signature (подпись)	подпись сертификата генерируется и кодируется в соответствии с требованиями, определенными в RFC 5280

### Номер версии

Все сертификаты ключей проверки ЭЦП выдаются УЦ службы ДТС в соответствии с версией X.509 v.3.

### Расширения сертификата ключа проверки ЭЦП

Функция каждого расширения определена стандартным значением связанного с ним идентификатора объекта (OBJECT IDENTIFIER). Расширение в зависимости от опции, выбранной УЦ службы ДТС, выдающее сертификат ключа проверки ЭЦП может быть критическим или некритическим. Если расширение обозначено как критическое, тогда приложение, использующее сертификаты ключей проверки ЭЦП, должно отклонять каждый сертификат ключа проверки ЭЦП, в котором после обнаружения критического расширения оно не сможет его распознать. Каждое некритическое расширение может игнорироваться.

### Использование ключа (Key Usage)

Разрешение использование ключа - может быть критическим или некритическим. Данное расширение определяет способ применения ключа (например ключ для шифрования данных, ключ для ЭЦП и т.д.). Значение данного расширения зависит от политики, в соответствии с которой выдан сертификат ключа проверки ЭЦП.

### Сертификат сервера СДТС

В сертификате сервера ДТС расширение "Использование ключа" помечается как критическое и имеет следующие значения:

digitalSignature (0) – ключ для реализации цифровой подписи (идентификации субъекта или данных);

nonRepudiation (1) – ключ, связанный с реализацией неотрекаемости.

### Сертификат сервиса проверки статуса сертификата ключа проверки ЭЦП

В сертификате СПСС расширение "Использование ключа" помечается как критическое и имеет следующие значения:

digitalSignature (0) – ключ для реализации цифровой подписи (идентификации субъекта или данных);

nonRepudiation (1) – ключ, связанный с реализацией неотрекаемости.

Сертификат сервиса штампов времени

В сертификате СШВ расширение "Использование ключа" помечается как критическое и имеет следующие значения:

digitalSignature (0) – ключ для реализации цифровой подписи (идентификации субъекта или данных);

nonRepudiation (1) – ключ, связанный с реализацией неотрекаемости.

Улучшенный ключ (ExtendedKeyUsage)

Уточнение (ограничение) использования ключа – расширение может быть критическим. Данное поле определяет одну или более областей в дополнение к основному применению, установленному в поле keyUsage, в пределах которых может быть использован сертификат. Данное поле следует интерпретировать как ограничение допустимой области применения ключа, определенного в поле keyUsage. Конкретные значения расширения зависят от политики, в соответствии с которой выдан сертификат ключа проверки ЭЦП.

Сертификат сервиса проверки статуса сертификата

В сертификате СПСС расширение помечается как некритическое и содержит объектный идентификатор OCSPSigning: 1.3.6.1.5.5.7.3.9.

Сертификат сервиса штампов времени

В сертификате СШВ расширение помечается как некритическое и содержит объектный идентификатор Timestaping: 1.3.6.1.5.5.7.3.8.

Политики сертификата (Certificate Policy)

Расширение политики применения сертификатов (CertificatePolicies) содержит идентификаторы политик и ее квалификаторы, вносимые в сертификат ключа проверки ЭЦП в соответствии с правилами, описанными в Регламенте УЦ службы ДТС. Данное расширение не является критическим расширением.

Основные ограничения (Basic Constraints)

Расширение является критическим в сертификатах ключей проверки ЭЦП удостоверяющих центров и может быть критическим или некритическим в сертификатах конечных пользователей. Расширение позволяет определить, является ли субъект сертификата удостоверяющим центром (поле CA), а также сколько максимально (принимая иерархическую систематизацию удостоверяющих центров) может быть удостоверяющих центров на пути, ведущем от рассматриваемого удостоверяющего центра до конечного пользователя (поле pathLength).

Значение поля pathLength, равное 0, означает, что сертификат принадлежит удостоверяющему центру, который может выдавать сертификаты только конечным пользователям.

В сертификатах в расширение BasicConstraints вносится пустая последовательность без указания в ней поля CA и поля pathLength.

Точки доступа к спискам отозванных сертификатов (CRL Distribution Points)

Расширение не является критическим. Расширение определяет протоколы и сетевые адреса, по которым можно получить актуальный список отозванных сертификатов, выданный издателем сертификата, в котором находится данное расширение.

Доступ к информации о центрах сертификации (AuthorityInformationAccess)

Расширение не является критическим. Поле указывает, каким образом передаются данные и услуги издателем сертификата, в сертификате которого данное расширение имеется. Данное расширение, если имеет место, то обычно содержит URL адрес файла сертификата удостоверяющего центра и URL адрес услуги OCSP проверки статуса сертификата, в котором указан этот адрес.

Идентификатор алгоритма

Поле signatureAlgorithm содержит идентификатор криптографического алгоритма, описывающего алгоритм, применяемый для реализации ЭЦП, которую ставит Удостоверяющий центр на сертификате.

Для сертификатов, выдаваемых УЦ службы ДТС, значение поля:

id-tc26-gost3410-2012-512 OBJECT IDENTIFIER ::= id-tc26-signwithdigest-gost3410-2012-512 OBJECT IDENTIFIER ::= { iso(1) member-body(2) ru(643) rosstandart(7) tc26(1) algorithms(1) signwithdigest(3) gost3410-2012-512(3) }

Формы имен

УЦ службы ДТС выдает сертификаты, содержащие имя издателя и субъекта, создаваемые в соответствии с правилами, описанными в Регламенте УЦ службы ДТС.

Идентификаторы политик сертификатов

Политика сертификата содержит информацию типа PolicyInformation (идентификатор, электронный адрес) о политике сертификата, которая реализуется УЦ службы ДТС, выдающим сертификаты – расширение не является критическим. В сертификатах, выдаваемых УЦ службы ДТС возможны следующие идентификаторы политик:

iso(1) member-body(2) ru(643) \_\_\_\_\_(X) id ЕЭК (XXX) id-\_\_\_\_\_(X) id-\_\_\_\_\_(X) id-\_\_\_\_\_(X) ... – политика сертификата службы статусов сертификата;

iso(1) member-body(2) ru(643) \_\_\_\_\_(X) id ЕЭК (XXX) id-\_\_\_\_\_(X) id-\_\_\_\_\_(X) id-\_\_\_\_\_(X) ... – политика сертификата службы штампов времени;

iso(1) member-body(2) ru(643) \_\_\_\_\_(X) id ЕЭК (XXX) id-\_\_\_\_\_(X) id-\_\_\_\_\_(X) id-\_\_\_\_\_(X) ... – политика сертификата администратора сертификации. Список отозванных сертификатов (CRL) состоит из последовательности трех полей. Первое поле (tbsCertList) содержит информацию об отозванных сертификатах, второе и третье поля (signatureAlgorithm и signatureValue) – соответственно информацию о типе алгоритма, примененного для подписания списка и ЭЦП, которая ставится на

сертификате удостоверяющим центром. Значение двух последних полей полностью совпадает, как в случае сертификата. Информационное поле tbsCertList является последовательностью обязательных и опциональных полей. Обязательные поля идентифицируют издателя списка отозванных сертификатов, а необязательные содержат отозванные сертификаты и расширения списка отозванных сертификатов.

Значения основных полей и расширений списка отозванных сертификатов приведены в таблице 2.

Таблица 2

Название поля	Значение или ограничения значения
Version (версия)	Version 2
Signature Algorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (издатель, имя DN)	Common Name (CN) = УЦ службы ДТС, Organization (O) = ЕЭК, Organization Unit (OU) = ИТ, Country (C) = RU
thisUpdate	дата и время выпуска списка отозванных сертификатов
nextUpdate	дата и время выпуска очередного списка отозванных сертификатов
revokedCertificates (Отозванные сертификаты)	информация о сертификатах, которые были отозваны, каждая запись, касающаяся сертификата, содержит следующие поля: userCertificate - серийный номер отозванного сертификата, revocationDate - дата отзыва сертификата, crlEntryExtensions - расширенный доступ к списку отозванных сертификатов (содержит дополнительную информацию об отозванных сертификатах - опционально), CRLReason (содержит информацию о причине отзыва сертификата – основные поля и расширения СОС – опционально) информация о вышеперечисленных полях записана в следующих трех строках этой таблицы
User Certificate (сертификат)	серийный номер сертификата, который был отозван
Revocation Date (Дата отзыва)	дата и время отзыва сертификата
CRL Reason (Причина отзыва)	причина отзыва сертификата. Допустимые значения: key Compromise; cessation Of Operation.
Extensions	набор расширений, определяющих дополнительную информацию, связанную с использованием сертификата (обязательные расширения: authority Key Identifier; crlNumber)
Signature (подпись)	подпись СОС генерируется и кодируется в соответствии с требованиями, определенными в RFC 5280

Номер версии

СОС, выпускаемые УЦ службы ДТС, соответствуют X.509 v2.

Расширения СОС

Среди многих расширений CRL самыми важными являются два, из которых первое (поле AuthorityKeyIdentifier) позволяет идентифицировать ключ проверки ЭЦП, соответствующий ключу ЭЦП, примененному для подписания списка отозванных



сертификатов, а второе (поле `cRLNumber`) содержит постепенно увеличиваемый номер списка CRL, издаваемого удостоверяющим центром (благодаря этому расширению пользователь списка может определить, когда один CRL заменил другой CRL).

### Шаблон OCSP

Протокол проверки статуса сертификата в оперативном режиме (OCSP) применяется удостоверяющими центрами и позволяет определить состояние сертификата. Структура запросов и ответов СПСС соответствует RFC 6960. В связи с этим единственным разрешенным номером версии является 0 (это соответствует версии v1). СПСС УЦ службы ДТС работает в режиме авторизованного ответчика.

Сертификат сервера СПСС должен содержать в себе расширение под названием `extKeyUsage`, определенное в RFC 5280. Данное расширение должно быть обозначено как критическое и означает, что удостоверяющий центр, выдавая сертификат серверу OCSP, подтверждает своей подписью факт передачи ему права выдачи от его имени удостоверений о статусе сертификатов клиентов данного центра.

Сертификат может содержать также информацию о способе контакта с сервером центра проверки статуса сертификата. Данная информация содержится в поле расширения `AuthorityInfoAccess`.

Информация о статусе сертификата вносится в поле `certStatus` структуры `SingleResponse`. Она может принимать одно из трех разрешенных значений, определенных в Регламенте УЦ службы ДТС.

### Шаблон запроса OCSP

OCSP-запрос принимает ASN.1-структуру в соответствии с RFC 6960 и имеет следующие ограничения.

Поле `requestExtensions` структуры `tbsRequest` содержит список расширений. Данный список должен содержать только расширение `ocspNonce` (OID 1.3.6.1.5.5.7.48.1.2).

Необязательное поле `singleRequestExtensions` структуры `tbsRequest`, содержащее список расширений для единичного запроса, должно отсутствовать.

В случае, если поле `optionalSignature` структуры `OCSPRequest` задано, то на него накладываются следующие ограничения:

поле `signatureAlgorithm` должно принимать значение "ГОСТ Р 34.11/34.10-2012" (OID 1.2.643.7.1.1.3.3);

поле `certs` должно включать сертификат для проверки ЭЦП запроса OCSP. Кроме того, поле `requestorName` из структуры `tbsRequest` должно присутствовать в обязательном порядке и представлять собой структуру `directoryName`, содержащую элемент `CommonName` (объектный идентификатор - 2.5.4.3).

### Шаблон ответа OCSP

OCSP-ответ принимает ASN.1-структуру в соответствии с RFC 6960 и имеет следующие ограничения.

Поле responseType содержит объектный идентификатор типа ответа, который имеет значение 1.3.6.1.5.5.7.48.1.1. Поле response содержит структуру BasicOCSPResponse.

В случае, если в соответствующем OCSP-запросе присутствовало расширение ocsponce, то в OCSP-ответе необязательное поле responseExtensions структуры ResponseData будет содержать расширение ocsponce с аналогичным значением.

Поле signatureAlgorithm принимает значение "ГОСТ Р 34.11/34.10-2012" (OID 1.2.643.7.1.1.3.3).

В списке сертификатов certs содержится сертификат СПСС, необходимый для проверки ЭЦП.

Необязательное поле singleExtensions структуры SingleResponse, которое может содержать расширения OCSP-ответа, отсутствует.

#### Шаблон штампов времени

СШВ УЦ службы ДТС подписывает ЭЦП выдаваемые им же штампы времени при помощи ключа ЭЦП, специально зарезервированного для этой цели. В соответствии с рекомендацией RFC 5280, совместимые с ними сертификаты ключей проверки ЭЦП СШВ содержат поле, уточняющее узкое допустимое применение ключа (ExtKeyUsage), обозначенное как критическое. Это означает, что сертификат может быть использован СШВ и только для формирования ЭЦП в выдаваемых им штампах времени.

Штамп времени, выданный СШВ УЦ службы ДТС содержит в себе информацию о штампе времени (структура TSTInfo), внесенную в структуру SignedData (в соответствии с RFC 2630), подписанную СШВ и закрепленную в структуре ContentInfo. Штампы времени, выдаваемые СШВ УЦ службы ДТС, соответствуют RFC 3161.

#### Шаблон запроса TSP

TSP-запрос представляет собой ASN.1-структуру в соответствии с RFC 2630 и имеет следующие ограничения:

необязательное поле reqPolicy структуры TimeStampReq должно отсутствовать либо содержать объектный идентификатор базовой политики (OID = 0.4.0.2023.1.1);

необязательное поле nonce должно отсутствовать либо содержать случайно сгенерированное 64-битное значение.

#### Шаблон ответа TSP

TSP-ответ представляет собой ASN.1-структуру в соответствии с RFC 2630 и имеет следующие ограничения:

поле digestAlgorithms структуры SignedData принимает значение "ГОСТ Р 34.11-2012 с длиной 512" (OID 1.2.643.7.1.1.2.3);

необязательное поле certificates структуры SignedData будет содержать сертификат службы TSP, если в TSP-запросе необязательное поле certReq структуры TimeStampReq содержало значение true;

необязательное поле crls структуры SignedData должно отсутствовать;

поле policy структуры TSTInfo должно содержать объектный идентификатор базовой политики (OID = 0.4.0.2023.1.1);

в случае, если в соответствующем TSP-запросе присутствовало необязательное поле nonce, то в TSP-ответе необязательное поле nonce структуры TSTInfo также будет содержать аналогичное значение;

необязательное поле tsa структуры TSTInfo отсутствует;

необязательное поле extensions структуры TSTInfo отсутствует;

поле digestAlgorithm структуры SignerInfo принимает значение "ГОСТ Р 34.11-2012 с длиной 512" (OID 1.2.643.7.1.1.2.3);

поле signedAttrs структуры SignerInfo будет содержать следующие объекты: тип подписываемого содержимого (OID 1.2.840.113549.1.9.16.1.4 (штамп времени)), значение хеш-функции штампа времени, информация о сертификате службы штампов времени;

поле signatureAlgorithm структуры SignerInfo принимает значение "ГОСТ Р 34.10-2-12 с длиной 512".

ПРИЛОЖЕНИЕ № 2  
к Регламенту  
удостоверяющего центра  
службы доверенной третьей  
стороны интегрированной  
информационной системы  
Евразийского экономического  
союза

## **ПЕРЕЧЕНЬ**

### **основных признаков подлинности документов**

Паспорт:

бланк паспорта соответствует утвержденной и действующей форме;

присутствуют все обязательные реквизиты, печати и штампы;

срок действия паспорта не истек;

имеются подписи должностных лиц;

даты рождения и выдачи паспорта соответствуют;

соответствуют записи о регионе, в котором производилась выдача паспорта, штампу о регистрации гражданина по месту жительства, на тот момент) и фотография в документе соответствует предъявителю (в т.ч. примерный возраст изображенного на фотокарточке лица соответствует указанному в документе).

Доверенность и копии приказов:

отсутствуют грамматические ошибки в оттиске печати, несимметрично расположенный текст, изломы, извилистость штрихов, общая бледность изображения

печати, деформация бумаги, упрощенный рисунок букв и цифр, буквы и цифры без засечек, овалы и полуовалы с угловатым строением.

ПРИЛОЖЕНИЕ № 3  
к Регламенту  
удостоверяющего центра службы доверенной  
третьей стороны интегрированной  
информационной системы Евразийского  
экономического союза

## ФОРМА

### заявления на создание и выдачу сертификата

Руководителю УЦ службы ДТС
115114, г. Москва, ул. Летниковская, д. 2, стр. 1
(наименование должности руководителя)
(полное наименование организации)
(Ф. И.О. руководителя) //

## ЗАЯВЛЕНИЕ

на изготовление сертификата ключа проверки ЭЦП

Прошу создать ключ ЭЦП и ключ проверки ЭЦП и изготовить сертификат ключа проверки ЭЦП в соответствии с указанными в настоящем заявлении данными:

Наименование  
организации (сокращ.)

Ф. И. О. (полностью):

Дата рождения

Место рождения (полностью)

Пол

мужской

женский

Паспортные данные (серия, номер):

( код  
 подразделения  
 )  
 (дата выдачи)  
 Должность:  
 Подразделение  
 :  
 e-mail/телефон  
 :  
 Юридический  
 адрес ( (полностью):  
 Рабочее место  
 по адресу:

### Назначение сертификата:

	Сертификат сервера СДТС
	Сертификат сервера СШВ
	Сертификат сервера СПСС

Ознакомлен с требованиями Регламента удостоверяющего центра службы ДТС и приложениями к нему и обязуюсь соблюдать все его положения.

Владелец сертификата ключа проверки ЭЦП		
	[личная подпись]	Ф.И.О.

Сведения представлены на основании подлинных документов и являются достоверными.

(Должность руководителя организации)	(подпись)	(Ф. И. О.)
"" г.		

М.П.

ПРИЛОЖЕНИЕ № 4

к Регламенту

удостоверяющего центра службы доверенной  
третьей стороны интегрированной  
информационной системы Евразийского  
экономического союза

## ФОРМА

### заявление на аннулирование сертификата

Руководителю УЦ службы ДТС
115114, г. Москва, ул. Летниковская, д. 2, стр. 1
(наименование должности руководителя)
(полное наименование организации)
(Ф.И.О. руководителя)
//

### Заявление на отзыв сертификата ключа подписи

Прошу Вас аннулировать сертификат, Назначение сертификата:

	Сертификат сервера СДТС
	Сертификат сервера СШВ
	Сертификат сервера СПСС

и внести аннулированный сертификат в список отозванных сертификатов:

(Должность, Ф.И.О. полностью)

(Причина аннулирования)

Сертификат №

(Серийный номер)

(Должность руководителя организации)

(подпись)

(Ф.И.О.)

"\_\_" \_\_\_\_\_ 20\_\_ г.

М.П.

ПРИЛОЖЕНИЕ № 5  
к Регламенту  
удостоверяющего центра  
службы доверенной третьей  
стороны интегрированной  
информационной системы  
Евразийского экономического  
союза

## ФОРМА

### доверенности на получение сертификата

Руководителю УЦ службы ДТС
115114, г. Москва, ул. Летниковская, д.2, стр.1
(Наименование должности руководителя)
(Наименование организации, полное)
(Ф. И. О. руководителя) //

### ДОВЕРЕННОСТЬ на получение сертификата ключа проверки ЭЦП

Прошу \_\_\_\_\_

—  
\_\_\_\_\_  
—  
\_\_\_\_\_  
—  
\_\_\_\_\_  
—  
\_\_\_\_\_

Сведения о лице, на имя которого выдана доверенность:

Ф. И. О. (полностью):	
Дата рождения	

Место рождения (полностью)		
Пол	<input type="text"/>	
	мужской	
Пол	<input type="text"/>	
	женский	
Паспортные данные (серия, номер):		
(код подразделения)		
(дата выдачи)		
Должность:		
Подразделение:		
e-mail/телефон:		
Юридический адрес (полностью):		
Рабочее место по адресу:		
Лицо, на имя которого выдана доверенность		
	[ личная подпись]	Ф.И.О.

Сведения представлены на основании подлинных документов и являются достоверными.

(Должность руководителя организации)	(подпись)	(Ф. И. О.)
" ____ " _____ 20__ г.		
М.П.		