Об удостоверяющем центре Евразийской экономической комиссии

Решение Коллегии Евразийской экономической комиссии от 09 июля 2018 года № 110

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) Евразийская экономическая коллегия **решила:**

1. Утвердить прилагаемое Положение об удостоверяющем центре Евразийской экономической комиссии.

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 9 июля 2018 г. № 110

ПОЛОЖЕНИЕ
об удостоверяющем центре Евразийской экономической комиссии

I. Общие положения

1. Настоящее Положение определяет назначение, основные задачи и функции удостоверяющего центра Евразийской экономической комиссии (далее – Комиссия), а также его права, обязанности, ответственность и порядок прекращения деятельности.

2. Основным назначением удостоверяющего центра Комиссии является создание сертификатов ключей проверки электронной цифровой подписи членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии для обеспечения возможности подписания ими электронных документов (в том числе документов ограниченного распространения, передаваемых по электронным каналам связи в пределах локальной вычислительной сети Комиссии).

3. Понятия, используемые в настоящем Положении, 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 электронной цифровой подписи;

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

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

"удостоверяющий центр Комиссии" – удостоверяющий центр, предназначенный для обеспечения сертификатами ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии;

"электронная цифровая подпись" – 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) и требованиях к созданию, развитию и функционированию трансграничного пространства доверия, утверждаемых Советом Комиссии.

4. Требования к оформлению электронных документов определяются в требованиях к созданию, развитию и функционированию трансграничного пространства доверия, утверждаемых Советом Комиссии, и в Положении об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, утвержденном Решением Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125.

5. Электронная цифровая подпись (далее – ЭЦП) членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии признается действительной при одновременном соблюдении следующих условий:

а) сертификат ключа проверки ЭЦП создан и выдан удостоверяющим центром Комиссии;

б) целостность данных, подписанных ЭЦП, не нарушена;

в) ЭЦП выработана с использованием закрытого (личного) ключа, соответствующий сертификат открытого ключа которого (сертификат ключа проверки ЭЦП) указан в составе этой ЭЦП;

г) сертификат ключа проверки ЭЦП действителен на момент подписания электронного документа;

д) сертификат удостоверяющего центра Комиссии действителен на момент подписания электронного документа.

II. Задачи и функции удостоверяющего центра Комиссии

6. Основными задачами удостоверяющего центра Комиссии являются:

а) удостоверение соответствия открытого ключа проверки ЭЦП закрытому (личному) ключу, а также подтверждение подлинности сертификата ключа проверки ЭЦП члена Коллегии Комиссии, должностного лица или сотрудника Комиссии;

б) обеспечение гарантий доверия к сертификатам ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии при международном (трансграничном) обмене электронными документами;

в) издание, распространение, хранение сертификатов ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии и проверка действительности этих сертификатов;

г) подтверждение достоверности сведений, указанных в сертификатах ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии .

7. Удостоверяющим центром Комиссии осуществляются в соответствии с правом Союза следующие функции:

а) создание и выдача сертификатов ключей проверки ЭЦП, соответствующих утверждаемым Комиссией требованиям, членам Коллегии Комиссии, должностным лицам и сотрудникам Комиссии;

б) обеспечение проверки личности членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии при выдаче сертификатов ключей проверки ЭЦП;

в) публикация в информационно-телекоммуникационной сети "Интернет" в режиме общего доступа информации об условиях пользования услугами удостоверяющего центра Комиссии, включая информацию об ограничениях по их использованию;

г) своевременное предоставление всем субъектам электронного взаимодействия информации о статусе (актуальности) всех выданных сертификатов ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии. Такая

информация должна быть доступна в любое время, в том числе и после прекращения действия сертификата ключа проверки ЭЦП члена Коллегии Комиссии, должностного лица или сотрудника Комиссии, и предоставляться автоматизированным способом;

д) внесение информации в реестр сертификатов ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии и список отозванных сертификатов ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии. Сертификат ключа проверки ЭЦП члена Коллегии Комиссии, должностного лица или сотрудника Комиссии считается отозванным с момента публикации списка отозванных сертификатов, содержащего информацию о соответствующем статусе (актуальности) такого сертификата и доступного в любое время субъектам электронного взаимодействия;

е) документирование и хранение информации о выдаче, получении и изменении статусов (актуальности) сертификатов ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии (в том числе после прекращения деятельности по обеспечению сертификатами ключей ЭЦП членов Коллегии Комиссии , должностных лиц и сотрудников Комиссии) для представления доказательств при разборе конфликтных ситуаций, связанных с применением выпущенных сертификатов ключей проверки ЭЦП. Хранение указанной информации может осуществляться в электронном виде;

ж) обеспечение конфиденциальности, целостности созданных и хранимых удостоверяющим центром Комиссии криптографических ключей;

з) информирование уполномоченных органов государств – членов Евразийского экономического союза о намерении прекратить деятельность по обеспечению сертификатами ключей ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии или об иных случаях прекращения деятельности.

8. Организацию работ по созданию, развитию и функционированию удостоверяющего центра Комиссии осуществляет структурное подразделение Комиссии, к сфере ведения которого отнесены данные вопросы. Функционирование удостоверяющего центра Комиссии осуществляется в соответствии с регламентом согласно приложению.

III. Права, обязанность и ответственность удостоверяющего центра Комиссии

9. Для выполнения своих функций удостоверяющий центр Комиссии имеет право:

а) проводить проверку сведений, представляемых членами Коллегии Комиссии, должностными лицами и сотрудниками Комиссии с целью получения сертификатов ключей проверки ЭЦП;

б) отказывать членам Коллегии Комиссии, должностным лицам и сотрудникам Комиссии 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) приостанавливать или аннулировать действие выпущенных сертификатов ключей проверки ЭЦП в случае разглашения сведений, которые могут существенным образом сказаться на возможности дальнейшего использования сертификатов ключей проверки ЭЦП, утраты их юридической силы, утраты соответствующих средств ЭЦП, прекращения действия документов, на основании которых оформлены сертификаты ключей проверки ЭЦП, и в иных случаях, установленных актами органов Союза;

г) организовывать, обеспечивать и контролировать выполнение должностными лицами и сотрудниками Комиссии требований информационной безопасности при эксплуатации средств удостоверяющего центра Комиссии;

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

е) устанавливать срок действия корневого сертификата ключа проверки ЭЦП удостоверяющего центра Комиссии и сертификатов ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии.

10. При выполнении своих функций удостоверяющий центр Комиссии обязан:

а) обеспечить порядок и сроки регистрации членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии в удостоверяющем центре Комиссии на основании представленных ими документов с обязательной проверкой указанных в них сведений;

б) информировать в письменной форме членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии об условиях и порядке использования ЭЦП и средств ЭЦП, о рисках, связанных с использованием ЭЦП, и о мерах, необходимых для обеспечения безопасности ЭЦП и ее проверки;

в) ознакомить членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии с порядком работы удостоверяющего центра Комиссии;

г) актуализировать информацию, содержащуюся в реестре сертификатов ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии , 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 членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии, в том числе информацию об аннулировании сертификатов ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии;

е) обеспечивать конфиденциальность созданных удостоверяющим центром Комиссии ключей ЭЦП;

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

з) участвовать в качестве третьей стороны при разрешении конфликтных ситуаций, связанных с применением сертификатов ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии;

и) обеспечивать хранение в течение не менее 15 лет созданных удостоверяющим центром Комиссии сертификатов ключей проверки ЭЦП, документов на бумажных носителях, на основании которых выпущены сертификаты ключей проверки ЭЦП, и иных документов удостоверяющего центра Комиссии 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 членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии;

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

11. Удостоверяющий центр Комиссии 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, а также актами органов Союза в области регулирования применения ЭЦП;

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

в) несоблюдения правил пользования средствами удостоверяющего центра Комиссии.

V. Прекращение деятельности удостоверяющего центра Комиссии

12. Деятельность удостоверяющего центра Комиссии прекращается по решению Коллегии Комиссии в связи с передачей функций удостоверяющего центра Комиссии другому удостоверяющему центру или в связи с ликвидацией информационных систем удостоверяющего центра Комиссии.

13. Удостоверяющий центр Комиссии в случае принятия решения о прекращении его деятельности оповещает об этом членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии за 1 месяц до даты прекращения деятельности.

14. В случае передачи функций удостоверяющего центра Комиссии другому удостоверяющему центру предается реестр сертификатов ключей проверки ЭЦП

членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии, выпущенных на дату прекращения деятельности удостоверяющего центра Комиссии.

15. В случае ликвидации информационных систем удостоверяющего центра Комиссии реестр сертификатов ключей проверки ЭЦП членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии и другие электронные и бумажные документы удостоверяющего центра Комиссии передаются на архивное хранение в установленном в Комиссии порядке.

ПРИЛОЖЕНИЕ
к Положению об удостоверяющем
центре
Евразийской экономической комиссии

РЕГЛАМЕНТ

удостоверяющего центра Евразийской экономической комиссии

1. Введение

1.1. Общие положения

Настоящий документ определяет:

а) правила применения сертификатов ключей проверки ЭЦП (далее сертификаты), выпущенных удостоверяющим центром Евразийской экономической комиссии (далее УЦ Комиссии), включая обязанности владельцев сертификатов;

б) порядок работы сервисов УЦ Комиссии;

в) принятые форматы данных и протоколы взаимодействия;

г) основные организационно-технические мероприятия, необходимые для безопасной работы УЦ Комиссии.

Данный документ составлен в соответствии с рекомендацией RFC 3647 "Internet X .509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". Структура, нумерация разделов и подразделов документа соответствуют рекомендации RFC 3647; некоторые подразделы состоят только из фразы "Нет условий", означающей, что для УЦ Комиссии не вводятся условия для данного подраздела.

1.2. Реквизиты регламента

Полное наименование документа: Регламент удостоверяющего центра Евразийской экономической комиссии.

Сокращенное наименование документа: Регламент УЦ Комиссии.

Объектный идентификатор документа: 1.2.643.3.294.1.1

Текущая версия: 1.0

Дата издания:

Участники инфраструктуры открытых ключей

Инфраструктура открытых ключей УЦ Комиссии включает в себя: УЦ Комиссии, владельцев сертификатов и пользователей сертификатов.

В состав Удостоверяющего центра входят:

Центр Сертификации (далее ЦС);

Центр Регистрации (далее ЦР);

Сервис публикации (далее СП);

Сервис информирования (далее СИ);

WEB-сервисы:

а) точки распространения списков отозванных сертификатов (далее CDP);

б) Служба проверки статусов сертификатов в режиме реального времени (далее OCSP-служба);

в) Служба простановки штампов времени (далее TSP-служба).

Центр сертификации

ЦС предназначен для выпуска сертификатов, списков аннулированных (отозванных) сертификатов (далее СОС), хранения эталонной базы сертификатов и СОС.

ЦС взаимодействует только с ЦР по отдельному сегменту локальной сети с использованием защищенного сетевого соединения ViPNet MFTP из состава ViPNet Client для обмена файлами формата SOK.

На ЦС находится база всех изготовленных сертификатов.

К функциям ЦС следующие основные функции:

выпуск сертификатов;

проверка уникальности ключей проверки ЭЦП;

ведение реестра сертификатов;

издание СОС;

аннулирование, приостановление и возобновление действия выпущенных сертификатов.

Центр регистрации

ЦР предназначен для хранения регистрационных данных владельцев сертификатов, запросов на сертификаты и сертификатов.

ЦР взаимодействует с ЦС по отдельному сегменту локальной сети с использованием защищенного сетевого протокола в виде передачи файлов формата SOK. ЦР является единственной точкой входа (регистрации) владельцев сертификатов в системе. Только зарегистрированные в ЦР пользователи УЦ Комиссии могут получить сертификат УЦ Комиссии.

К функциям ЦР относятся следующие функции:

ведение реестра владельцев сертификатов;

создание ключей ЭЦП и ключей проверки ЭЦП для членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии;

создание запросов на издание, аннулирование, приостановление и возобновление действия сертификатов в ЦС.

Сервис публикации

СП предназначен для публикации информации УЦ Комиссии в репозитории УЦ Комиссии.

СП взаимодействует с ЦС по отдельному сегменту локальной сети с использованием защищенного сетевого протокола.

К функциям СП относятся следующие функции:

публикация сертификатов;

публикация сертификатов Уполномоченного лица УЦ Комиссии;

публикация СОС.

Сервис информирования

СИ предназначен для информирования администраторов УЦ Комиссии и владельцев сертификатов.

СИ взаимодействует с базой данных ЦС. СИ на основании информации о сертификатах, полученной при опросе базы данных ЦС, формирует соответствующие сообщения для рассылки по электронной почте (с помощью почтового SMTP-сервера). Почтовые сообщения сохраняются на жестком диске ЦС в соответствующую папку и переносятся на компьютер с SMTP-сервером при помощи съемных носителей.

Сервис информирования предоставляет следующие возможности:

рассылка администраторам УЦ Комиссии уведомлений о событиях, связанных с сертификатами:

а) об истечении срока действия сертификатов;

б) об изменении статуса запросов на сертификаты;

в) о превышении заданного количества необработанных запросов на выпуск, приостановление действия, возобновление действия, отзыв сертификатов;

рассылка уведомлений владельцам сертификатов об истечении срока действия их сертификатов;

формирование отчетов о сертификатах, выпущенных в УЦ Комиссии.

WEB-портал

WEB-портал предназначен для обеспечения доступа к репозиторию УЦ с помощью сети общего пользования (подробнее про репозиторий УЦ см. раздел 2).

URL-адреса WEB-портала в сети общего пользования Internet:

http://ca.eecommission.org ,

https://ca.eecommission.org

Комплексом организационно-технических мер обеспечивается требуемые показатели доступности WEB-портала.

Служба проверки статусов сертификатов в режиме реального времени

OCSP-служба предназначена для выполнения функций установления статуса сертификатов на основе протокола OCSP (Online Certificate Status Protocol).

OCSP-служба обеспечивает использование международных рекомендаций в части построения ИОК, с учетом применения ГОСТ 2814789, ГОСТ Р 34.112012, ГОСТ Р 34.102012;

RFC 2560 "Internet X.509 Public Key Infrastructure. Online Certificate Status Protocol OCSP";

RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile".

Порядок работы OCSP-службы изложен в приложении № 1 к настоящему Регламенту.

Служба простановки штампов времени

TSP-служба обладает точным и надежным источником времени и выполняет функции по созданию штампов времени. Штамп времени подписанный ЭЦП документ, которым TSP-служба удостоверяет, что в указанный момент времени ей было предоставлено значение хэш-функции от другого документа. При этом значение хэш-функции так же указывается в штампе времени.

TSP-служба обеспечивает использование международных рекомендаций в части построения ИОК, с учетом применения ГОСТ 2814789, ГОСТ Р 34.112012, ГОСТ Р 34.102012;

RFC 3161 "Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)".

Порядок работы TSP-службы изложен в приложении № 1 к настоящему Регламенту

.

Владелец сертификата

Владельцами сертификатов являются:

члены Коллегии Комиссии, должностные лица и сотрудники Комиссии, которым в установленном настоящим Регламентом порядке выдан сертификат и которые владеют ключом ЭЦП, соответствующим ключу проверки ЭЦП, включенному в состав выданного сертификата;

должностные лица или сотрудники Комиссии, назначенные ответственными за хранение и использование сертификатов ключей проверки ЭЦП, предназначенных для обеспечения функционирования технологических сервисов (служб) Комиссии.

Пользователь сертификата

Пользователь сертификата – лицо, принимающее выпущенные согласно настоящему Регламенту сертификаты, и действующее, доверяя сертификатам Уполномоченного лица УЦ Комиссии.

Использование сертификатов

Допустимое использование

УЦ Комиссии выпускает следующие типы сертификатов:

сертификаты ключей проверки ЭЦП центра сертификации УЦ Комиссии;

сертификаты ключей проверки ЭЦП OCSP-службы;

сертификаты ключей проверки ЭЦП TSP-службы;

сертификаты аутентификации серверов;

сертификаты членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии, которым в установленном Регламентом УЦ Комиссии порядке выдан сертификат и которые владеют ключом ЭЦП, соответствующим ключу проверки ЭЦП, включенному в состав выданного сертификата;

сертификаты доверенной третьей стороны Комиссии.

Сертификаты могут быть использованы только в соответствии, с политиками применения сертификатов, идентификаторы которых указаны в сертификатах. При этом в сертификатах допускается указывать идентификаторы только тех политик применения сертификатов, которые соответствуют настоящему Регламенту.

Объектные идентификаторы политик применения сертификатов, соответствующие настоящему Регламенту, приведены в приложении № 2.

Запрещенное использование

Запрещается использовать сертификат в целях, не указанных ни в одной из политик применения сертификатов, идентификаторы которых указаны в сертификате.

Управление регламентом

Реквизиты УЦ Комиссии

Адрес УЦ Комиссии:

119121, г. Москва, Смоленский бульвар, д.3/5, стр. 1

Телефон: +7 (495) 6692400

Факс: 8 (495) 6692415

e-mail: info@eecommission.org

Контактное лицо

Лицо, определяющее соответствие настоящего Регламента политикам применения сертификатов

Процедура утверждения Регламента УЦ Комиссии и политик применения сертификатов

Утверждение Регламента УЦ Комиссии осуществляется одновременно с утверждением положения об УЦ Комиссии.

Утверждение политик применения сертификатов осуществляется приказом Председателем Коллегии Евразийской экономической комиссии по согласованию с Департаментом информационных технологий и Департаментом управления делами Евразийской экономической комиссии.

Исправления и/или дополнения публикуются в репозитории УЦ Комиссии в виде документов содержащих исправления и/или дополнения, либо в виде исправленных и/или дополненных новых версий документа.

Определения и акронимы

Определения

Аутентификация – процедура проверки подлинности пользователя путем сравнения предоставленных данных и признаков ранее зафиксированным уникальным данным или признакам.

Владелец сертификата – член Коллегии Комиссии, должностное лицо или сотрудник Комиссии, которому в установленном настоящим Регламентом порядке выдан сертификат, владеющий ключом ЭЦП, соответствующим ключу проверки ЭЦП, включенному в состав выданного сертификата.

Данные активации – закрытые данные, отличные от ключей, требуемые для управления ключевым носителем.

Ключ ЭЦП – уникальная последовательность символов, предназначенная для создания электронной цифровой подписи.

Заявитель – субъект, подавший заявление на выпуск сертификата.

Идентификация – процесс, устанавливающий однозначное соответствие субъекта отличительным признакам.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Инфраструктура открытых ключей или (ИОК) – архитектура, организация, методики, способы и процедуры, которые обеспечивают управление и применение криптографической системы, основанной на сертификатах.

Квалификатор политики – зависимая от политики применения сертификатов информация, которая может сопутствовать идентификатору политики применения сертификатов в сертификате X.509.

Ключевая пара – ключ ЭЦП и соответствующий ему ключ проверки ЭЦП.

Компрометация ключа электронной цифровой подписи – результат действий физического лица, повлекший за собой разглашение ключа ЭЦП.

Оператор ЦР УЦ Комиссии – физическое лицо, являющееся сотрудником Удостоверяющего центра Комиссии, занимающееся рассмотрением и обработкой заявлений на выпуск, приостановление действия, возобновления действия, отзыв сертификатов.

Ключ проверки электронной цифровой подписи – уникальная последовательность символов, однозначно связанная с ключом электронной цифровой подписи и предназначенная для проверки подлинности электронной цифровой подписи.

Политика применения сертификатов (Certificate Policy) – набор правил, определяющий использование сертификата некоторым сообществом и/или классом приложений с заданными требованиями безопасности.

Пользователь сертификата – лицо, принимающее выпущенные согласно настоящему Регламенту сертификаты и действующее, доверяя сертификатам Уполномоченного лица УЦ Комиссии.

Путь (цепочка) сертификации – упорядоченная последовательность сертификатов, которая может быть обработана вместе с ключом проверки ЭЦП начального объекта для признания ключа проверки ЭЦП конечного объекта.

Регламент удостоверяющего центра (Certification Practice Statement) – это документ, содержащий описание процедур и действий, которые УЦ использует при выпуске, управлении, отзыве и обновлении сертификатов.

Сертификат ключа проверки ЭЦП (сертификат) – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной цифровой подписи Владельцу сертификата.

Соглашение с пользователем УЦ Комиссии (Соглашение) – соглашение между УЦ Комиссии и пользователем УЦ, которое устанавливает права и обязанности сторон, относящиеся к использованию сертификатов и выраженное в присоединении пользователя УЦ к настоящему Регламенту путем подписания Заявления на изготовление сертификата.

Список аннулированных (отозванных) сертификатов или СОС – электронный документ, пописанный ЭЦП Уполномоченного лица УЦ Комиссии, содержащий список серийных номеров сертификатов, которые в определенный момент времени были отозваны, либо действие которых было приостановлено. Сертификаты, чьи номера присутствуют в списке файла СОС, являются отозванными из обращения УЦ Комиссии.

Средства электронной цифровой подписи (средства ЭЦП) – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭЦП, проверка ЭЦП, создание ключа ЭЦП и ключа проверки ЭЦП.

Уполномоченное лицо Удостоверяющего центра – сотрудник УЦ Комиссии, наделенный полномочиями по заверению сертификатов и СОС своей электронной цифровой подписью.

Электронный документ документ в электронном виде, заверенный электронной цифровой подписью (электронной подписью) и отвечающий требованиям общей инфраструктуры документирования информации в электронном виде.

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).

Запрос на выпуск, приостановление действия, возобновление действия или отзыв сертификата – файл, сформированный Оператором ЦР и заверенный ЭЦП Оператора ЦР. Подписанные ЭЦП Оператора ЦР Запросы обрабатываются Уполномоченным лицом УЦ Комиссии.

PKCS#10 (RFC 2986) – стандарт, определяющий формат и синтаксис запроса на выпуск сертификата.

Акронимы

CDP CRL Distribution Point (Точка распространения СОС);

CRL Certificate Revocation List (Список аннулированных (отозванных) сертификатов); PKCS Public-Key Cryptography Standard;

PKI Public Key Infrastructure (Инфраструктура ключа проверки электронной подписи);

RFC Request For Comments;

DN Distinguished Name (Отличительное имя);

ИОК Инфраструктура открытых ключей;

ПО Программное обеспечение;

СОС Список аннулированных (отозванных) сертификатов;

СКЗИ Средства криптографической защиты информации;

УЦ Удостоверяющий центр;

ЦР Центр регистрации;

ЭЦП Электронная цифровая подпись (электронная подпись).

Публикация и ответственность за актуальность информации в репозитории

Репозиторий

УЦ Комиссии поддерживает в актуальном состоянии репозиторий. В качестве репозитория используется выделенная директория на WEB-портале.

Публикация информации

Публикации подлежит:

сертификаты Уполномоченного лица УЦ Комиссии;

СОС;

политики применения сертификатов;

настоящий Регламент;

шаблоны Заявлений на выпуск, приостановление действия, возобновление действия , отзыв сертификата согласно приложению № 3 к настоящему Регламенту;

сопутствующая информация, уведомления, обновления и исправления.

Время и частота публикаций

Публикация информации осуществляется, как только она становится доступной и с частотой необходимой для поддержания ее в актуальном состоянии.

Доступ к репозиторию

Вся публикуемая информация является общедоступной для пользователей УЦ Комиссии. Администратор репозитория использует различные механизмы для предотвращения неавторизованного изменения, дополнения и/или удаления опубликованной информации.

Идентификация и аутентификация

Присваивание имен

Типы имен

В качестве имени в сертификате используется отличительное имя согласно стандарту X.500.

Требования к интерпретации имен

Имена, содержащиеся в сертификатах, однозначно идентифицируют субъектов.

Анонимные или заявители с псевдонимами

Выпуск сертификатов для анонимных заявителей недопустим.

Использование псевдонимов разрешено.

Правила интерпретации различных форм имен

Нет условий.

Уникальность имен

Возможно существование нескольких сертификатов с одинаковыми отличительными именами. При этом УЦ Комиссии гарантирует уникальность издаваемых сертификатов.

Признание, аутентификация и роль торговых марок

Имена, владельцем которых не является Заявитель, не могут быть использованы в сертификате. УЦ Комиссии может не проверять права Заявителя на владение доменными именами, торговыми марками и/или другими объектами интеллектуальной собственности, но в случае возникновения какого-либо спора за право владения таковыми должен приостановить действие сертификата до окончания разбирательства, и в соответствии с результатом спора, после окончания такового, определить статус сертификата.

Первоначальное подтверждение подлинности

Метод доказательства обладания ключом ЭЦП

Если ключевая пара создается удостоверяющим центром Комиссии, то доказательство не требуется.

Если ключевая пара создается заявителем самостоятельно, то методом доказательства обладания ключом ЭЦП является криптографическая демонстрация обладания ключом ЭЦП. Демонстрация обладания ключом ЭЦП осуществляется путем подписания заявителем определенного набора данных, предоставляемого со стороны УЦ Комиссии, с использованием собственного ключа ЭЦП, и передачи подписанных данных в УЦ Комиссии, где осуществляется проверка ЭЦП с использованием ключа проверки ЭЦП. Корректно завершенная процедура проверки ЭЦП является доказательством обладания ключом ЭЦП. Некорректно завершенная процедура проверки ЭЦП приводит к прекращению действия и отзыву сертификата.

Проверка идентификационной информации организации

Нет условий.

Проверка личной идентификационной информации

Личная идентификационная информация пользователя проверяется на основании документов, удостоверяющих личность, и кадровой информации.

Непроверяемая информация

Не допускается указание в сертификате непроверяемой или непроверенной информации.

Проверка полномочий

Проверка полномочий Заявителя осуществляется в порядке, предусмотренном политикой применения сертификатов, в соответствии с которой выпускается сертификат.

Критерии взаимодействия

Нет условий.

Аутентификация и идентификация для обновления ключей

Аутентификация и идентификация для плановых замены ключей

Аутентификация и идентификация осуществляется по действительному сертификату, документу, удостоверяющему личность, или с использованием систем двухфакторной аутентификации.

Аутентификация и идентификация для обновления ключей после отзыва

Аутентификация и идентификация осуществляется по документу, удостоверяющему личность, либо с использованием систем двухфакторной аутентификации.

Аутентификация и идентификация для запроса на отзыв

Аутентификация и идентификация осуществляется по документу, удостоверяющему личность, по действительному сертификату, одноразовому паролю, переданному любыми средствами связи, документально подтвержденному запросу на отзыв, либо с использованием систем двухфакторной аутентификации.

Функциональные требования жизненного цикла сертификата

В настоящем разделе описываются условия и порядок представления услуг УЦ Комиссии.

УЦ Комиссии предоставляет следующие виды услуг:

внесение в реестр УЦ Комиссии регистрационной информации о Заявителе;

формирование ключевой пары с последующей ее записью на ключевой носитель по запросу Заявителя;

изготовление сертификата для Заявителя в электронной форме;

изготовление копии сертификата для Владельца сертификата на бумажном носителе ;

ведение реестра изготовленных УЦ Комиссии сертификатов;

предоставление сертификатов в электронной форме из реестра выпущенных сертификатов по запросам Пользователей сертификатов;

аннулирование (отзыв) сертификатов по обращениям Владельцев сертификатов;

приостановление и возобновление действия сертификатов по обращениям Владельцев сертификатов;

предоставление Пользователям сертификатов информации сведений об аннулированных (отозванных) сертификатах и сертификатах с приостановленным сроком действия;

подтверждение подлинности ЭЦП в документах, представленных в электронной форме, по обращению Пользователя сертификата;

подтверждение подлинности ЭЦП Уполномоченного лица УЦ Комиссии в изготовленных им сертификатах по обращения Пользователя сертификата;

распространение средств ЭЦП.

Порядок проведения работ по подтверждению действительности ЭЦП и штампов времени приведен в приложении № 4 к настоящему Регламенту.

Заявление на выпуск сертификата

Заявление на выпуск сертификата

Заявление на выпуск сертификата может подать член Коллегии Комиссии, должностное лицо или сотрудник Комиссии.

Процесс регистрации и требования

Процесс регистрации осуществляется в порядке, предусмотренном политикой применения сертификатов, в соответствии с которой выпускается сертификат.

Перечень документов, представленных Заявителем для проведения процедуры его регистрации

Перечень документов определяется политикой применения сертификатов, в соответствии с которой выпускается сертификат.

Обработка Заявления на выпуск сертификата

Идентификация и аутентификация Заявителя

Аутентификация и идентификация осуществляется в соответствии с требованиями раздела 3.2 настоящего Регламента.

Принятие или отклонение Заявления на выпуск сертификата

УЦ Комиссии может отклонить Заявление на выпуск сертификата в следующих случаях:

Заявление было передано способом не соответствующим требованиям настоящего Регламента, политик применения сертификатов или в несоответствующем формате;

данные, указанные в заявлении, не соответствуют действительности;

данные, указанные в заявлении, не подтверждены соответствующими документами;

Заявитель не прошел процедуру аутентификации и идентификации;

выпуск сертификата может нанести какой-либо вред УЦ Комиссии.

Заявление на выпуск сертификата принимается, если отсутствуют вышеперечисленные причины для его отклонения.

Срок обработки Заявления на выпуск сертификата

Оператор ЦР должен начать обработку заявления на выпуск сертификата с момента его получения. Ограничение времени обработки Заявления может быть установлено в политике применения сертификатов, в соответствии с которой выпускается сертификат . Заявление считается активным до момента его принятия или отклонения.

Временем передачи Заявления на выпуск сертификата считается время личного его вручения Заявителем в Оператору ЦР.

Временем завершения обработки Заявления на выпуск сертификата считается время создания Запроса на выпуск сертификата либо отказа в приеме Заявления.

Если Оператор ЦР отказал в приеме Заявления на выпуск сертификата Заявитель должен быть проинформирован об отказе и его причинах.

Выпуск сертификата

Действия, предусмотренные во время выпуска сертификата

УЦ Комиссии выпускает сертификат по Запросу, заверенному ЭЦП Оператора ЦР. Сертификат выпускается на основании указанных в Заявлении данных, в порядке, предусмотренном политикой применения сертификатов, в соответствии с которой выпускается сертификат.

Сертификат выпускается в форме электронного документа, заверенного ЭЦП Уполномоченного лица УЦ Комиссии, и в форме документа на бумажном носителе, заверенного рукописной подписью Оператора ЦР.

Оповещение Заявителя о выпуске сертификата

УЦ Комиссии оповещает Заявителя о выпуске сертификата путем направления email-сообщения на адрес, указанный в Заявлении на выпуск сертификата.

Признание сертификата

Действия по признанию сертификата

Признанием сертификата является следующие действия Заявителя:

использование сертификата;

заверение рукописной подписью сертификата в бумажной форме.

Кроме того, если УЦ Комиссии не получает в течение 1 рабочего дня уведомления от Заявителя об отклонении сертификата, сертификат так же считается признанным.

Публикация сертификата удостоверяющим центром

УЦ Комиссии публикует выпущенные сертификаты в репозитории.

Уведомление третьей стороны о выпуске сертификата УЦ Комиссии

Нет условий.

Использование сертификата и ключевой пары

Использование сертификата и ключевой пары Владельцем сертификата

Владелец сертификата может использовать собственный сертификат после его признания и в соответствии с требованиями политик применения сертификата, настоящего Регламента и иных руководящих документов. Владелец сертификата должен защищать ключ ЭЦП от компрометации.

Разрешено использование только действительного сертификата, в соответствии с требованиями политик применения сертификатов, идентификаторы которых указаны в сертификате.

Использование сертификата и ключа проверки ЭЦП Пользователем сертификата

Перед использованием сертификата Пользователь сертификата обязан:

ознакомиться с политикой применения сертификатов и настоящим Регламентом, в соответствии с которыми выпущен сертификат;

проверить статус используемого сертификата и сертификата Уполномоченного лица УЦ Комиссии, входящего в Путь сертификации.

Пользователь сертификата может использовать только действительный сертификат, в соответствии с требованиями политики применения сертификатов, идентификатор которой указан в сертификате.

Обновление сертификата

Обновление сертификата является выпуском нового сертификата без изменения ключа проверки ЭЦП или другой информации в сертификате.

Обстоятельства обновления сертификата

УЦ Комиссии не осуществляет обновление сертификатов.

Кто может подать запрос на обновление сертификата

Нет условий.

Обработка запросов на обновление сертификатов

Нет условий.

Оповещение Заявителя о выпуске нового сертификата

Нет условий.

Действия по признанию обновленного сертификата

Нет условий.

Публикация обновленного сертификата

Нет условий.

Уведомление третьей стороны об обновлении сертификата

Нет условий.

Обновление ключей

Данный раздел описывает выпуск нового сертификата в случае обновления ключевой пары.

Обстоятельства обновления ключевой пары

Обновление ключевой пары возможно в случае компрометации ключа ЭЦП, а так же в случае истечения срока действия сертификата. Генерация ключевых пар осуществляется в соответствии с подразделом 6.2 настоящего Регламента.

Кто может подать Заявление на выпуск сертификата при обновлении ключевой пары

Заявление на выпуск сертификата при обновлении ключевой пары может подать Владелец сертификата.

Обработка Заявления на выпуск сертификата при обновлении ключевой пары

Одобрение Заявления на выпуск сертификата при обновлении ключевой пары осуществляется в соответствии с подразделом 4.2, а выпуск сертификата в соответствии с пунктом 4.3 настоящего Регламента.

Оповещение Владельца сертификата о выпуске нового сертификата

Оповещение выполняется в соответствии с пунктом 4.3.2 настоящего Регламента.

Действия по признанию нового сертификата при обновлении ключевой пары

Признание осуществляется в соответствии с пунктом 4.4.1 настоящего Регламента.

Публикация нового сертификата при обновлении ключевой пары

Публикация осуществляется в соответствии с пунктом 4.4.2 настоящего Регламента.

Уведомление третьей стороны о выпуске нового сертификата при обновлении ключевой пары

Нет условий.

Изменение сертификата

Изменение сертификата является выпуском нового сертификата при необходимости изменения информации, включенной в существующий сертификат. При этом старый сертификат отзывается.

Обстоятельства изменения сертификата

Изменение сертификата производится в случае, если информация, содержащаяся в сертификате, становится не актуальной или при ее внесении в сертификат была допущена ошибка.

Кто может подать Заявление на изменение сертификата

Заявление на изменение сертификата может подать Владелец сертификата.

Обработка Заявления на изменение сертификата

Одобрение Заявления на изменение сертификата осуществляется в соответствии с подразделом 4.2, а выпуск сертификата в соответствии с разделом 4.3.1 настоящего Регламента.

Оповещение Владельца сертификата о выпуске нового сертификата

Оповещение выполняется в соответствии с пунктом 4.3.2 настоящего Регламента.

Действия по признанию измененного сертификата

Признание осуществляется в соответствии с пунктом 4.4.1 настоящего Регламента.

Публикация измененного сертификата УЦ Комиссии

Публикация осуществляется в соответствии с пунктом 4.4.2.

Уведомление третьей стороны о выпуске измененного сертификата УЦ Комиссии

Нет условий.

Отзыв, приостановление действия и возобновление действия сертификата

По истечении срока действия сертификата сертификат автоматически считается аннулированным. Сертификат считается отозванным, приостановленным или возобновленным с момента публикации в репозитории УЦ Комиссии СОС, содержащего информацию об изменении статуса этого сертификата.

Обстоятельства отзыва сертификата

Сертификат может быть отозван при следующих обстоятельствах:

при компрометации ключа ЭЦП, соответствующему ключу проверки ЭЦП, указанному в сертификате;

при несоблюдении Владельцем сертификата требований настоящего Регламента;

при прекращении деятельности УЦ Комиссии;

дальнейшее использование сертификата может нанести вред УЦ Комиссии;

по запросу Владельца сертификата;

иных обстоятельствах, предусмотренных политикой применения сертификатов, в соответствии с которой выпущен сертификат.

Заявление на отзыв сертификата

Заявление на отзыв сертификата может быть подано:

Владельцем сертификата;

сотрудником УЦ Комиссии, если он располагает достоверной информацией, требующей отзыва сертификата;

иным лицом, предусмотренным политикой применения сертификатов, в соответствии с которой выпущен сертификат.

Процедура рассмотрения Заявления на отзыв сертификата

Заявление на отзыв сертификата может быть подано в бумажной или электронной форме, либо с использованием любых средств связи, но в любом случае с аутентификацией согласно подразделу 3.4 настоящего Регламента.

Заявление на отзыв сертификата должно содержать следующую информацию:

серийный номер сертификата или иную информацию, позволяющую однозначно идентифицировать сертификат;

причину отзыва сертификата;

необходимые комментарии.

После получения Заявления на отзыв сертификата Оператор ЦР производит верификацию Заявления, и если таковая прошла успешно, то формирует Запрос на отзыв сертификата и подписывает его своей ЭЦП. Уполномоченное лицо УЦ Комиссии на основании подписанного ЭЦП Оператора ЦР Запроса на отзыв сертификата отзывает сертификат. После отзыва сертификата УЦ Комиссии в течение одного часа публикует обновленный СОС, содержащий информацию об отозванном сертификате.

Срок передачи Заявления на отзыв сертификата

Заявление на отзыв сертификата должно быть передано Оператору ЦР так быстро, насколько это возможно.

Срок обработки Заявления на отзыв сертификата

Заявление на отзыв сертификата рассматривается в течение четырех часов рабочего дня с момента его подачи. Временем подачи Заявления считается:

при передаче по электронной почте время отправки сообщения в адрес Оператора ЦР;

при вручении лично или передачей иными способами время получения Оператором ЦР Заявления.

Требования к Пользователям сертификатов по проверке статуса сертификата

Пользователь сертификата обязан проверять статус сертификата перед каждым использованием, используя СОС, публикуемые УЦ Комиссии, или сервис проверки статуса сертификата в режиме реального времени, предоставляемой OCSP-службой УЦ Комиссии.

Частота выпуска списка отозванных сертификатов

УЦ Комиссии публикует актуальные СОС в рабочие дни с частотой один раз в 24 часа. В случае если за днем публикации СОС следуют выходные или праздничные дни, то срок действия СОС продлевается до ближайшего рабочего дня. В случае отзыва сертификата публикация СОС осуществляется в соответствии с процедурой, изложенной подпункте 4.9.3.

Если срок действия сертификата, включенного в СОС, истекает, то он может быть удален из него после истечения срока действия.

Максимальное время задержки публикации списка отозванных сертификатов

Максимальное время задержки публикации СОС составляет 6 часов.

Доступность OCSP-службы

OCSP-служба УЦ Комиссии доступна по URL-адресу:

https://ca-ocsp.eecommission.org:8877

Комплексом организационно-технических мер обеспечиваются требуемые показатели доступности OCSP-службы.

Требования к OCSP-службе

OCSP-служба обеспечивает использование международных рекомендаций в части построения ИОК, с учетом применения ГОСТ 2814789, ГОСТ Р 34.112012, ГОСТ Р 34.102012;

RFC 2560 "Internet X.509 Public Key Infrastructure. Online Certificate Status Protocol OCSP";

RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile".

Другие доступные формы извещения об отзыве сертификата

Не предусмотрены.

Специальные требования, относящиеся к компрометации ключей

В случае компрометации ключа ЭЦП Уполномоченного лица УЦ Комиссии, OCSP-службы или TSP-службы участники ИОК оповещаются посредством рассылки соответствующих email-сообщений.

Обстоятельства приостановления действия сертификата

Действие сертификата должно быть приостановлено при следующих обстоятельствах:

по запросу Владельца сертификата;

возникновения какого-либо разбирательства, не позволяющего на текущий момент принять решение о действительности сертификата;

иных обстоятельствах, предусмотренных политикой применения сертификатов, в соответствии с которой выпущен сертификат.

Заявление на приостановление действия сертификата

Заявление на приостановление действия сертификата может быть подано:

Владельцем сертификата;

сотрудником УЦ Комиссии, если он располагает достоверной информацией, требующей приостановления действия сертификата;

иным лицом, предусмотренным политикой применения сертификатов, в соответствии с которой выпущен сертификат.

Процедура рассмотрения Заявления на приостановление действия сертификата

Заявление на приостановление действия сертификата может быть подано в бумажной или электронной форме, либо с использованием любых средств связи, но в любом случае с аутентификацией согласно подразделу 3.4 настоящего Регламента.

Заявление на приостановление действия сертификата должно содержать следующую информацию:

серийный номер сертификата или иную информацию, позволяющую однозначно идентифицировать сертификат;

причину приостановления;

необходимые комментарии.

После получения Заявления на приостановление действия сертификата Оператор ЦР производит верификацию Заявления, и если таковая прошла успешно, то производит формирование запроса на приостановление действия сертификата и подписывает его своей ЭЦП. Уполномоченное лицо УЦ Комиссии на основании подписанного ЭЦП Оператора ЦР запроса на приостановление действия сертификата приостанавливает действие сертификата. После приостановления действия сертификата Владелец такового уведомляется об этом, а УЦ Комиссии публикует СОС, содержащий информацию о приостановлении действия сертификата.

Заявление на приостановление действия сертификата рассматривается в течение 1 рабочего дня с момента его подачи. Временем подачи Заявления считается:

при передаче по электронной почте время передачи сообщения на почтовый сервер УЦ;

при вручении лично или передачей иными способами время получения.

Ограничение на срок приостановления действия сертификата

Не устанавливается.

Обстоятельства возобновления действия сертификата

Действие сертификата может быть возобновлено:

по Заявлению Владельца сертификата;

по решению УЦ Комиссии.

Заявление на возобновление действия сертификата

Заявление на возобновление действия сертификата может быть подано:

Владельцем сертификата;

сотрудником УЦ Комиссии, если он располагает достоверной информацией, требующей возобновления действия сертификата, либо информацией об отсутствии причин для дальнейшего приостановления действия или отзыва сертификата.

Процедура рассмотрения Заявления на возобновление действия сертификата

Заявление на восстановление действия сертификата может быть подано в бумажной или электронной форме, либо с использованием любых средств связи, но в любом случае с аутентификацией согласно подразделу 3.4 настоящего Регламента.

В любом случае Заявление на возобновление действия сертификата должно содержать серийный номер сертификата или иную информацию, позволяющую однозначно идентифицировать сертификат.

После получения Заявления на возобновление действия сертификата Оператор ЦР производит верификацию запроса, и если таковая прошла успешно, то формирует Запрос на возобновление действия сертификата и подписывает его своей ЭЦП. Уполномоченное лицо УЦ Комиссии на основании подписанного ЭЦП Оператора ЦР Запроса на возобновление действия сертификата производит возобновление действия

сертификата. После возобновления действия сертификата Владелец такового уведомляется, а СОС, не содержащий информацию о приостановлении действия сертификата, публикуется.

Заявление на возобновление действия сертификата рассматривается в течение 1 рабочего дня с момента его подачи. Временем подачи Заявления на возобновление действия сертификата считается:

при передаче по электронной почте время отправки сообщения в адрес Оператора ЦР;

при вручении лично или передачей иными способами время получения Оператором ЦР Заявления.

Сервисы УЦ Комиссии по проверке статуса сертификатов

Эксплуатационные характеристики

Для проверки статуса сертификатов УЦ Комиссии предоставляет доступ к СОС в репозитории УЦ, а также предоставляет доступ к OCSP-службе.

Доступность сервисов

Комплексом организационно-технических мер обеспечивается доступность СОС и OCSP-службы в режиме 24x7.

СОС публикуются по следующим URL-адресам:

http://ca.eecommission.org/share/CAcrlXX.crl ,

https://ca.eecommission.org/share/CAcrlXX.crl ,

где XX версия сертификата ЦС.

Дополнительные возможности

Не предусмотрено.

Прекращение использования услуг

Владелец сертификата может отказаться от услуг УЦ Комиссии следующим образом:

отказавшись от обновления сертификата по истечению срока его действия;

подав Заявление на отзыв своего сертификата до истечения срока действия без выдачи нового.

Депонирование и возврат ключей

УЦ Комиссии не осуществляет депонирование и возврат ключей.

Методы и политика депонирования и возврат ключей

Не предусмотрено.

Методы и политика инкапсуляции и восстановления сессионного ключа

Не предусмотрено.

Организационные, эксплуатационные и физические меры обеспечения безопасности

В настоящем разделе описываются меры защиты информационных ресурсов УЦ Комиссии, порядок эксплуатации средств защиты, а также порядок действий обслуживающего персонала УЦ Комиссии.

Физические меры обеспечения безопасности

Физические меры обеспечения безопасности определяются договором аренды нежилых помещений, предусматривающим наличие поста охраны при входе в здание, в котором расположены арендуемые помещения.

Размещение и организация доступа к компонентам УЦ Комиссии

Все компоненты УЦ Комиссии находятся в специализированных помещениях с ограниченным доступом, оборудованных для предотвращения и определения неавторизованного доступа, использования или раскрытия конфиденциальной информации.

Физический доступ

Физический доступ к компонентам УЦ Комиссии защищен как минимум двумя уровнями доступа. На каждом уровне доступа осуществляется проверка разрешения на доступ.

Контроль доступа к программным компонентам УЦ Комиссии осуществляется с использованием двухфакторной аутентификации, включая использование аппаратных носителей ключевой информации.

Электропитание

Аппаратное обеспечение УЦ Комиссии обеспечено источниками бесперебойного электропитания, обеспечивающими их штатное функционирование.

Кондиционирование и влажность

Требования по кондиционированию и влажности в помещениях соответствуют техническим условиям эксплуатации аппаратного обеспечения.

Пожарная безопасность

Меры пожарной безопасности соответствуют требованиям руководящих документов по пожарной безопасности страны пребывания Комиссии.

Хранение носителей информации

Вся информация, подлежащая архивному хранению хранится в специально оборудованном архивохранилище, доступ к которому имеет ограниченный круг лиц.

Уничтожение информации

Все носители информации, содержащие важную информацию, после окончания срока хранения подлежат уничтожению путем физического уничтожения носителей информации.

Ключи ЭЦП уничтожаются в соответствии с порядком, указанным в эксплуатационной документации соответствующего СКЗИ.

Внешнее архивное хранение

Не предусмотрено.

Процессуальные меры обеспечения безопасности

Доверенные роли

Доверенные роли представлены как минимум следующими ролями:

оператор ЦР;

системный администратор;

администратор УЦ;

администратор аудита.

Количество сотрудников, требуемое для выполнения операций

Все операции, за исключением генерации ключей Уполномоченного лица УЦ Комиссии (ключи ЦС, OCSP-службы, TSP-службы), могут выполняться в индивидуальном порядке и не требуют коллегиальности, если иное не установлено политикой применения сертификатов, в соответствии с которой выпускается сертификат.

Для генерации ключей ЦС, OCSP-службы, TSP-службы необходимо участие как минимум двух сотрудников УЦ Комиссии.

Идентификация и аутентификация для каждой роли

Первичная аутентификация и идентификация сотрудника УЦ Комиссии осуществляется при приеме на работу с использованием общепринятых документов, удостоверяющих личность. Доступ к программно-аппаратному обеспечению УЦ Комиссии осуществляется в соответствии с полученной ролью. Последующая аутентификация и идентификация сотрудника УЦ Комиссии производится с использованием программно-аппаратных средств аутентификации и идентификации.

Роли, требующие разделения обязанностей

Роль Администратора аудита не может быть объединена ни с одной из ролей.

Управление персоналом

Требования к квалификации, опыту и допуску к секретным материалам

К персоналу, выполняющему доверенные роли, как минимум предъявляются следующие требования:

лояльность;

понимание и соблюдение политик безопасности;

необходимая подготовка для выполнения своих обязанностей.

Процедуры проверки на соответствие общим требованиям

При назначении сотруднику УЦ Комиссии доверенной роли он проходит процедуру проверки в соответствии требованиям раздела 5.3.1 настоящего Регламента.

Требования к профессиональной подготовке

Программа подготовки сотрудников УЦ Комиссии включает следующее:

концепция PKI, в объемах необходимых для выполнения служебных обязанностей;

должностные обязанности;

политики и процедуры безопасности и деятельности УЦ Комиссии;

использование и эксплуатация развернутого аппаратного и программного обеспечения УЦ Комиссии.

Требования и частота переподготовки

Переподготовка персонала УЦ Комиссии осуществляется в объемах и с частотой, необходимых для поддержания и совершенствования сотрудниками УЦ Комиссии их квалификации и успешного выполнения функциональных обязанностей.

Частота и последовательность кадровых перемещений

Нет условий.

Санкции за неправомочные действия

Любые неправомочные действия персонала УЦ Комиссии влекут за собой санкции в соответствии с действующим законодательством страны пребывания УЦ Комиссии.

Любые неправомочные действия Владельца сертификата могут наказываться немедленным расторжением Соглашения с УЦ Комиссии, в том числе отзывом сертификата, а также преследоваться в соответствии с законодательством страны пребывания УЦ Комиссии.

Требования для независимых подрядчиков

Ко всем лицам, выполняющим доверенные роли, но не являющимися сотрудниками УЦ Комиссии, предъявляются такие же требования, как и к сотрудникам УЦ Комиссии.

Обеспечение персонала документацией

УЦ Комиссии обеспечивает свой персонал необходимой документацией для успешного выполнения их должностных обязанностей.

Процедуры регистрации событий

Типы регистрируемых событий

Регистрации подлежат следующие типы событий:

события жизненного цикла ключей УЦ Комиссии, включая генерацию, резервное копирование, восстановление, архивирование и уничтожение;

события жизненного цикла сертификатов, включая:

подача Заявлений на выпуск, приостановление действия, возобновление действия, отзыв сертификатов, подача заявлений на обновление ключей; результаты обработки данных Заявлений;

выпуск сертификатов и СОС;

события, влияющие на безопасность:

все неудачные попытки выполнить какие-либо действия;

попытки доступа к компонентам УЦ Комиссии каким-либо образом;

действия, осуществляемые персоналом УЦ Комиссии;

аварии программно-аппаратного обеспечения УЦ Комиссии и другие аномалии;

изменение профилей доступа к компонентам УЦ Комиссии персонала УЦ Комиссии;

деятельность межсетевых экранов.

Запись о регистрации события должна содержать следующую информацию:

дата и время события;

автор записи;

тип события.

Частота обработки журналов регистрации событий

Файлы журналов регистрации событий проверяются и архивируются Администратором аудита не реже двух раз в неделю. Так же журналы регистрации событий просматриваются в случаях подозрительной или необычной активности, а также при возникновении критических ситуаций. Обработка журналов регистрации событий должна включать просмотр событий и верификацию того, что записи в журналах не были изменены или подделаны.

Срок хранения журналов регистрации событий

Минимальный срок хранения журналов регистрации событий составляет 15 лет.

Защита журналов регистрации событий

Доступ к журналам регистрации событий имеют:

Системный администратор;

Администратор УЦ;

Администратор аудита.

Журналы регистрации событий защищаются системой регистрации событий от неавторизованного доступа, модификации, изменения или удаления.

Процедуры резервного копирования журналов регистрации событий

Резервное копирование журналов регистрации событий осуществляется в соответствии с общими процедурами резервного копирования.

Система регистрации событий

Данные об автоматически регистрируемых событиях записываются приложениями и операционными системами. Данные о событиях, регистрируемых вручную, записываются персоналом УЦ Комиссии.

Оповещение субъекта, явившегося причиной события

Не производится.

Оценка уязвимости

Оценка уязвимости систем производится в ходе проведения обработки журналов регистрации событий.

Архивные записи

Состав архивируемой информации

Обязательному архивному хранению подлежит:

заявления на выпуск, отзыв, приостановление действия и возобновление действия сертификатов, сопутствующая информация;

заявления на изготовление ключей ЭЦП;

выпущенные сертификаты;

журналы регистрации событий;

реестр выпущенных СОС;

документация УЦ Комиссии;

внутренняя и внешняя корреспонденция УЦ Комиссии.

Срок хранения архивной информации

Указанная в подпункте 5.5.1 информация хранится в течение всего срока деятельности УЦ Комиссии, но не менее 15 лет. В случае прекращения деятельности УЦ Комиссии до истечения сроков хранения информации указанная информация передается на хранение в подразделение Комиссии, осуществляющее архивное хранение документов.

После окончания срока хранения информация уничтожается путем физического уничтожения носителей информации. Выделение архивных документов к уничтожению и уничтожение осуществляются постоянно действующей комиссией, формируемой из числа сотрудников УЦ Комиссии и назначаемой распоряжением руководителя УЦ Комиссии.

Защита архива

Архивные документы и информация на отчуждаемых носителях хранятся в специально оборудованном помещении – архивохранилище, обеспечивающим режим хранения архивных документов, устанавливаемый актами Комиссии. Защита от модификации, удаления и разглашения архивной информации осуществляется методами и средствами ограничения доступа.

Процедура резервного копирования архива

Нет условий.

Требования к штампу времени архивных записей

Не предусмотрено.

Система архивного хранения

Применяется внутренняя система архивного хранения Комиссии.

Процедура получения и верификации архивной информации

Доступ к архиву разрешен только сотрудникам УЦ Комиссии, обладающим доверенной ролью. Доступ иным субъектам разрешается только по решению руководителя УЦ Комиссии. При получении информации производится контроль ее целостности.

Замена ключей

УЦ Комиссии при плановом обновлении ключевых пар компонент УЦ Комиссии должен осуществить данную процедуру без нарушения работоспособности системы и прозрачно для Пользователей сертификатов и Владельцев сертификатов.

Восстановление при компрометации и аварии

Действия при компрометации и аварии

Все участники ИОК должны быть оповещены в случаях компрометации ключей электронной подписи компонент УЦ Комиссии (ЦС, OCSP-службы, TSP-службы) или происшествий, влияющих на штатное функционирование УЦ Комиссии.

В случае компрометации УЦ Комиссии в кратчайшие сроки приступает к функционированию с использованием новых ключевых пар.

В случае выхода из строя по каким-либо причинам каких-либо компонент УЦ Комиссии осуществляется их восстановление из резервных копий. Обязательному резервному копированию подлежит следующая информация:

заявления и сопутствующая информация;

реестр выпущенных сертификатов;

журналы регистрации событий.

Резервное копирование ключей УЦ Комиссии осуществляется согласно пункту 6.3.4 настоящего Регламента.

Повреждение компьютерных ресурсов, программного обеспечения и/или данных

В случае повреждения (подозрения в повреждении) компьютерных ресурсов, программного обеспечения и/или данных УЦ Комиссии восстанавливает работоспособность, используя резервные копии.

Все субъекты, на которых отражается произошедшая авария или сбой немедленно извещаются. По окончанию восстановления все субъекты, чьи интересы были затронуты аварией или сбоем оповещаются о восстановлении.

Процедура восстановления в случае компрометации ключа электронной подписи Уполномоченного лица УЦ Комиссии

В случае компрометации ключа электронной подписи Уполномоченного лица УЦ Комиссии осуществляется отзыв его сертификата, а также оповещение всех субъектов ИОК о компрометации доступными методами.

В случае компрометации ключей Владельцы сертификатов обязаны немедленно оповестить УЦ Комиссии о факте компрометации. УЦ Комиссии осуществляет отзыв таких сертификатов в соответствие с порядком, указанным в разделе 4.9.3 настоящего Регламента.

Возможность непрерывности функционирования после бедствий

Непрерывность функционирования после бедствий обеспечивается мерами, указанными в Регламенте восстановления работоспособности компонент УЦ Комиссии
.

Прекращение деятельности УЦ Комиссии

Деятельность УЦ Комиссии прекращается в соответствии с порядком, предусмотренным положением об удостоверяющим центром Комиссии. Кроме того, УЦ Комиссии оповещает всех Владельцев сертификатов и Пользователей сертификатов о прекращении своей деятельности.

Технические меры обеспечения безопасности

Требования к средствам ЭЦП

Владельцы сертификатов должны использовать средства ЭЦП, соответствующие требованиям к средствам ЭЦП, изложенным в Требованиях к созданию, развитию и функционированию трансграничного пространства доверия утверждаемых Советом Комиссии. Перед использованием указанных средств их соответствие установленным требованиям должно быть подтверждено уполномоченными органами страны пребывания Комиссии в порядке, установленным ее законодательством.

Генерация и инсталляция ключевых пар

Генерация ключевых пар

Генерация ключевых пар при выпуске сертификатов на имя члена Коллегии Комиссии, должностного лица или сотрудника Комиссии осуществляется на АРМ Оператора ЦР с применением СКЗИ VIPNet CSP 4.2 (вариант исполнения 3). Ключевые пары записываются на ключевые носители, требования к которым приведены в разделе 6.3.1 настоящего Регламента.

Генерация ключевых пар при выпуске сертификатов для автоматизированных систем Комиссии осуществляется в порядке, предусмотренном политикой применения сертификатов, в соответствии с которой выпускаются данные сертификаты.

Передача ключа ЭЦП Владельцу сертификата

В случае генерации ключевой пары на АРМ Оператора ЦР передача ключа ЭЦП осуществляется путем передачи ключевого носителя Владельцу сертификата. Ключевой носитель передается способом, гарантирующим конфиденциальность ключа ЭЦП.

Передача ключа проверки ЭЦП в УЦ Комиссии

Требований не предъявляется.

Передача ключа проверки ЭЦП Уполномоченного лица УЦ Комиссии

Ключ проверки ЭЦП Уполномоченного лица УЦ Комиссии содержится в сертификате ЦС. Сертификат ЦС опубликован в репозитории по URL-адресам:

http://ca.eecommission.org/share/CAcertXX.cer ,

https://ca.eecommission.org/share/CAcertXX.cer ,

где XX версия сертификата ЦС.

Размеры ключей

Длина ключей, используемых для формирования и проверки ЭЦП:

ключ ЭЦП 256 бит;

ключ проверки ЭЦП 512 бит (ГОСТ Р 34.102012);

Длина ключей, используемых для шифрования:

сессионный ключ для шифрования по ГОСТ 2814789 256 бит;

ключ ЭЦП 256 бит;

ключ проверки ЭЦП 512 бит (на базе ГОСТ Р 34.102012).

Генерация параметров ключа проверки ЭЦП и проверка качества

Не применяется.

Цели использования ключей

В соответствии с пунктом 7.1.2 настоящего Регламента.

Защита ключа ЭЦП и технический контроль криптографических модулей

Стандарты и контроль криптографических модулей

Формирование ключей ЭЦП производится на следующие типы носителей:

типы носителей, поддерживаемые СКЗИ VIPNet CSP 4.2 (формуляр ФРКЕ.0010603 30 01 ФО);

криптографический модуль Программно-аппаратный комплекс ViPNet HSM (формуляр ФРКЕ.0012701 30 01 ФО).

Создание копий ключей ЭЦП на компьютере при использовании отчуждаемого носителя для хранения ключей недопустимо.

Контроль ключа ЭЦП несколькими лицами

Контроль ключа ЭЦП несколькими лицами допустим только в случае хранения ключа ЭЦП в криптографическом модуле Программно-аппаратный комплекс ViPNet HSM.

Депонирование ключа ЭЦП

Депонирование ключа ЭЦП недопустимо.

Резервная копия ключа ЭЦП

Резервное копирование и хранение резервных копий ключей ЭЦП компонент УЦ Комиссии осуществляется с использованием методов и средств, обеспечивающих уровень защищенности не меньше уровня защищенности ключевого носителя.

Архивирование ключа ЭЦП

УЦ Комиссии не осуществляет архивное хранение ключей ЭЦП.

Перенос ключа ЭЦП из/в криптографический модуль

Генерация ключей ЭЦП Уполномоченного лица УЦ, используемых для подписания сертификатов, квитанций OCSP-службы происходит непосредственно в криптографическом модуле Программно-аппаратный комплекс ViPNet HSM (вариант исполнения 1). Перенос ключа ЭЦП Уполномоченного лица УЦ, используемого для подписания сертификатов, из криптографического модуля осуществляется в процессе резервного копирования ключа в порядке, предусмотренном эксплуатационной документацией на криптографический модуль. Процесс переноса ключей ЭЦП Уполномоченного лица должен контролироваться минимум двумя сотрудниками УЦ Комиссии.

Единоличное хранение резервной копии ключа ЭЦП Уполномоченного лица УЦ Комиссии не допускается. Хранение резервной копии ключа ЭЦП УЦ Комиссии осуществляется путем разделения ключа (секрета) по схеме два из трех. Ответственными за хранение отдельных частей резервной копии ключа ЭЦП УЦ Комиссии (секрета) являются:

системный администратор;

администратор УЦ;

администратор аудита.

Хранение ключей ЭЦП в криптографическом модуле

Ключи ЭЦП Уполномоченного лица УЦ Комиссии, используемые для подписания сертификатов и квитанций OCSP-службы, хранятся в криптографическом модуле в зашифрованном виде.

Метод активации ключа ЭЦП

Активация ключа ЭЦП может осуществляться только его владельцем.

Для активации ключа ЭЦП должны использоваться данные активации, удовлетворяющие требованиям подраздела 6.5 настоящего Регламента. Активация ключа ЭЦП должна производиться на ограниченный период времени.

Метод деактивации ключа ЭЦП

Деактивация ключа ЭЦП должна производиться либо автоматически, либо путем отключения ключевого носителя.

Метод уничтожения ключа ЭЦП

После окончания срока действия или архивного хранения, если таковое осуществляется, ЭЦП уничтожается методами, гарантирующими невозможность его восстановления.

Оценка криптографических модулей

См. раздел 6.2.1.

Другие аспекты управления ключевой парой

Архивирование ключа проверки ЭЦП

Ключ проверки ЭЦП архивируется в составе сертификата в соответствии с подразделом 5.5 настоящего Регламента.

Сроки действия сертификата и использования ключевой пары

Срок действия ключей ЭЦП составляет:

членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии не более 1 года;

ЦС не более 3 лет (из них 15 месяцев для подписания сертификатов остальное время только для подписания СОС);

OCSP-службы не более 6 месяцев;

TSP-службы не более 3 месяцев.

Срок действия сертификатов составляет:

членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии не более 15 лет;

ЦС не более 16 лет;

OCSP-службы не более 15 лет;

TSP-службы не более 15 лет.

Данные активации

Генерация и инсталляция данных активации

Данные активации используются для защиты ключевых носителей. Данные активации создаются перед генерацией ключевой пары. УЦ Комиссии может не осуществлять создание данных активации для Заявителей.

В качестве данных активации могут быть использованы:

пароль, PIN;

биометрическая информация;

системы строгой двухфакторной аутентификации.

Для всех политик применения сертификатов пароль (PIN) должен отвечать следующим минимальным требованиям:

известен только Владельцу сертификата;

длина не менее 8 символов;

мощность алфавита не менее 10 символов;

не должен содержать слов, словосочетаний, имен и т.п.

В политиках применения сертификатов могу устанавливаться дополнительные требования к данным активации.

Защита данных активации

Данные активации должны защищаться от потери, порчи, неавторизованного использования или раскрытия.

Другие аспекты, относящиеся к данным активации

Передача или уничтожение данных активации должны осуществляться методами, обеспечивающими невозможность потери, кражи, разглашения, порчи, модификации или неавторизованного использования.

Средства управления безопасностью вычислительной техники

Особые технические требования по безопасности вычислительной техники

Используемая вычислительная техника обеспечивает сохранность и защиту данных УЦ Комиссии и ключей ЭЦП от уничтожения, порчи, модификации, разглашения или неавторизованного использования.

Оценка безопасности вычислительной техники

Автоматизированная система УЦ Комиссии аттестована на соответствие требованиям защищенности информации от несанкционированного доступа

Технические средства управления жизненным циклом

Средства управления разработкой системы

Нет условий.

Средства управления организацией безопасности

УЦ комиссии использует механизмы проверки безопасной конфигурации и целостности используемых систем.

Средства управления безопасностью жизненного цикла

Нет условий.

Средства управления сетевой безопасностью

УЦ Комиссии использует средства сетевой безопасности, предотвращающие неавторизованный доступ к информации, и защищающие от атак.

Метки времени

Сертификаты и СОС содержат информацию о дате и времени. УЦ Комиссии синхронизирует все программные и технические средства по сигналам точного времени ГЛОНАСС.

Структура сертификатов, СОС, OCSP-ответов и TSP-ответов

Структура сертификата

Структура сертификатов соответствует требованиям к сертификатам ключей проверки электронной цифровой подписи, утверждаемым Комиссией.

Все издаваемые сертификаты содержат следующие базовые поля:

Serial Number уникальный серийный (регистрационный) номер сертификата в реестре сертификатов УЦ Комиссии;

Signature Algorithm объектный идентификатор алгоритма, используемого для подписи сертификата;

Issuer отличительное имя ЦС УЦ Комиссии;

Valid From дата начала действия сертификата;

Valid To дата окончания действия сертификата;

Subject идентификационные данные Владельца сертификата или автоматизированной системы Комиссии;

Subject Public Key ключ проверки ЭЦП Владельца сертификата или автоматизированной системы Комиссии;

Version версия структуры сертификата формата X.509;

Signature ЭЦП Уполномоченного лица УЦ Комиссии.

Номер версии

Версия издаваемых сертификатов не ниже 3.

Расширения сертификата

В издаваемых сертификатах могут использоваться только перечисленные в данном разделе расширения. В случае если значение какого-либо поля (флага) перечисленных расширений не определено настоящим Регламентом, УЦ Комиссии вправе определить значение данного поля для издаваемых сертификатов в соответствии с требованиями X .509 и RFC 5280.

Authority Key Identifier

Данное расширение обязательно для всех сертификатов, за исключением самоподписанных (сертификатов ЦС УЦ Комиссии), и является некритическим. Это

расширение должно обязательно содержать поле keyIdentifier, в котором содержится идентификатор ключа проверки ЭЦП ЦС УЦ Комиссии. Остальные поля не обязательны.

Subject Key Identifier

Данное расширение должно присутствовать во всех сертификатах, являться некритическим и содержит идентификатор ключа проверки ЭЦП Владельца сертификата или автоматизированной системы Комиссии.

KeyUsage

Данное расширение должно присутствовать во всех сертификатах и быть критическим.

Значение полей расширения KeyUsage:

Смещение битовой маски	Поле	Сертификат Уполномоченного лица УЦ	Сертификаты OCSP-службы и TSP-службы	Сертификаты членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии	Описание
0	digitalSignature	0	0/1	0/1	ЭЦП
1	nonRepudiation	0	0/1	0/1	Неотрекаемость от авторства
2	keyEncipherment	0	0/1	0/1	Шифрование ключей
3	dataEncipherment	0	0/1	0/1	Шифрование данных
4	keyAgreement	0	0/1	0/1	Согласование ключей
5	keyCertSign	1	0	0	Э Ц П сертификатов
6	CRLSign	1	0	0	ЭЦП СОС
7	encipherOnly	0	0/1	0/1	Зашифрование
8	decipherOnly	0	0/1	0/1	Расшифрование

Certificate Policies

Данное расширение должно присутствовать в каждом сертификате, выпущенном УЦ Комиссии, содержать объектный идентификатор политики применения сертификатов, в соответствии с которой данный сертификат выдан. Идентификаторы политик применения сертификатов используются в соответствии с разделами 7.1.6 и 7.1.7 настоящего Регламента. Расширение является некритическим.

Basic Constraints

Расширение должно содержится сертификате ЦС УЦ Комиссии и является критическим. Значение флага cA установлено в 1 (true). Расширение сертификата ЦС УЦ Комиссии так же содержит поле pathLenConstraint, значение которого установлено в 0 (ноль).

Name Constraints

Используется в соответствии с разделом 3.1 настоящего Регламента.

Policy Constraints

Используется в соответствии с разделом 7.1.7 настоящего Регламента.

CRL Distribution Points

Данное расширение должно содержаться во всех сертификатах членов Коллегии Комиссии, должностных лиц, сотрудников Комиссии и автоматизированных систем Комиссии, быть некритическим и содержать список точек распространения СОС. Список точек распространения СОС приведен в разделе 4.10.2 настоящего Регламента.

Authority Information Access

Расширение должно присутствовать во всех сертификатах, быть некритическим и содержать URL-адрес точки публикации сертификата ЦС УЦ Комиссии в соответствии с разделом 6.2.4 настоящего Регламента и URL-адрес OCSP-службы УЦ Комиссии в соответствии с разделом 4.9.9 настоящего Регламента.

Extended Key Usage

Данное расширение присутствует в сертификатах и является некритическим.

Расширение содержит объектные идентификаторы областей использования сертификатов, предусмотренных политикой применения сертификатов, в соответствии с которой выпущен сертификат.

Объектные идентификаторы криптографических алгоритмов

Все участники ИОК должны использовать в своей работе криптографические алгоритмы с объектными идентификаторами, соответствующими RFC 3279, RFC 7091.

Формы имен

В сертификате поля идентификационных данных Уполномоченного лица УЦ Комиссии и Владельца сертификата содержат атрибуты имени формата X.500.

Ограничения имен

Обязательными атрибутами поля идентификационных данных Уполномоченного лица УЦ являются:

Common Name – Псевдоним ЦС УЦ Комиссии;

Organization – Евразийская Экономическая Комиссия;

Organization Unit – УЦ Евразийской экономической комиссии;

Country – буквенный код страны пребывания Комиссии (например, RU)

Email – ca-info@eecommission.org

Обязательные атрибуты поля идентификационных данных Владельца сертификата устанавливаются политикой применения сертификатов, в соответствии с которой выпускается сертификат.

Объектные идентификаторы применяемых политик применения сертификатов

Объектные идентификаторы политик применения сертификатов перечислены в приложении № 2 настоящего Регламента. В сертификате Уполномоченного лица УЦ может использоваться OID 2.5.29.32.0, обозначающий любую политику применения сертификатов.

Использование расширения Policy Constraints

Нет условий.

Семантика и синтаксис квалификаторов политики

Нет условий.

Обработка семантики критического расширения Certificate Policies

Нет условий.

Структура списков отозванных сертификатов

Структура СОС должна соответствовать RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

СОС содержат следующие основные поля:

Version версия структуры СОС формата X.509;

Signature Algorithm объектный идентификатор алгоритма, используемого для подписи СОС;

Signature ЭЦП Уполномоченного лица УЦ Комиссии.

Issuer отличительное имя ЦС УЦ Комиссии;

This Update дата и время выпуска текущего СОС;

Next Update дата и время планового выпуска следующего СОС;

Next Publication дата и время следующей плановой публикации СОС;

Revoked Certificates список аннулированных (отозванных) сертификатов, включающий серийный номер сертификата и дату отзыва. Данное поле может отсутствовать, если нет отозванных сертификатов.

Номер версии

Все издаваемые СОС версии 2.

Расширения СОС и элементов СОС

Authority Key Identifier

Идентификатор ключа Уполномоченного лица УЦ, которым подписан данный СОС

.

CRL Number

Некритическое рекомендуемое расширение, содержащее порядковый номер СОС.

Reason Code

Некритическое рекомендуемое расширение элемента СОС, содержащее причину отзыва сертификата.

Invalidity Date

Не применяется.

Структура OCSP-ответа

Все ответы OCSP-службы (OCSP-ответы) содержат следующие поля:

Version версия структуры OCSP-ответа;

Status статус OCSP-ответа;

Signature algorithm объектный идентификатор алгоритма, используемого для подписи OCSP-ответа;

HasNonce указатель на наличие идентификатора OCSP-ответа;

id-pkix-ocsp-nonce идентификатор OCSP-ответа;

ProducedAt дата и время подписания OCSP-ответа OCSP-службой;

Extensions не применяется;

Certificate of signer of OCSP response идентификационные данные Владельца сертификата OCSP-службы (Уполномоченного лица УЦ Комиссии);

Verification of certificate of signer of OCSP response результат проверки сертификата OCSP-службы;

Verification of OCSP response результат проверки ЭЦП OCSP-службы.

Single responses количество проверяемых сертификатов в запросе, для каждого из которых:

Hash algorithm идентификатор алгоритма хеширования; o Serial number серийный номер сертификата;

Issuer key hash хеш идентификационных данных Уполномоченного лица УЦ;

Issuer name hash хеш ключа проверки ЭЦП Уполномоченного лица УЦ;

Certificate status результат проверки статуса сертификата;

RevTime дата и время отзыва сертификата;

RevReason причина отзыва сертификата;

ThisUpdate дата и время, на которые была осуществлена проверка сертификата;

NextUpdate дата и время, не позднее которых будет доступна более новая информация о Статусе сертификата (если дата и время не указаны, то информация доступна постоянно);

Archive cutoff не применяется;

Extensions не применяется;

Verification of single response результат проверки OCSP-ответа;

Certificates from OCSP response сертификат OCSP-службы.

Номер версии

Версия структуры OCSP-ответа 1.

Тип OCSP-ответа

OCSP-служба УЦ Комиссии формирует OCSP-ответы базового типа.

Сертификат OCSP-службы

В OCSP-службе для подписания OCSP-ответов применяется сертификат, расширение Extended Key Usage которого содержит идентификатор 1.3.6.1.5.5.7.3.9 (Подписание OCSP).

Структура штампа времени

Все ответы TSP-службы (штампы времени) содержат следующие поля:

Policy ID идентификатор политики, в соответствии с которой выпущен штамп времени;

Serial Number серийный номер (идентификатор) штампа времени;

Accuracy (microseconds) точность часов TSP-службы, мкс;

Ordering: 0

HasNonce: 1

TSA идентификационные данные TSP-службы;

Stamp time дата и время подписания штампа времени TSP-службой;

Hash algorithm идентификатор алгоритма хеширования;

Hash size размер хеша, байт;

Hash значение хеша;

Certificate of signer of time-stamp: идентификационные данные Владельца сертификата TSP-службы (Уполномоченного лица УЦ Комиссии);

Verification of time-stamp: результат проверки штампа времени.

Verification of certificate of signer of time-stamp: результат проверки сертификата оператора TSP-службы.

Certificates from time-stamp (1):

Common Name =TSP-служба УЦ Комиссии, OU=УЦ Евразийской экономической комиссии , O=Евразийская экономическая Комиссия, C=RU, E= info@eecommission.org

Номер версии

Версия структуры TSP-ответа 1.

Сертификат TSP-службы

В TSP-службе для подписания TSP-ответов применяется сертификат, расширение Extended Key Usage которого содержит идентификатор 1.3.6.1.5.5.7.3.8 (Установка отметки времени).

Аудит соответствия и другие оценки

Частота и условия оценки

Внутренний и внешний аудит УЦ Комиссии проводится по решению руководства УЦ Комиссии.

Идентификация и квалификация эксперта

Внутренний аудит проводится Администратором аудита УЦ Комиссии.

Внешний аудит проводится независимой организацией, соответствующей следующим требованиям:

имеет опыт эксплуатации информационных систем на основе технологий PKI и информационной безопасности, а также опыт в проведении аудита безопасности;

имеет не менее двух специалистов, имеющих высшее образование или прошедших переподготовку по специальности "Информационная безопасность".

Отношение эксперта к оцениваемому

Для проведения внешнего аудита привлекается организация организационно или юридически независимая от УЦ Комиссии.

Охватываемые аудитом области

Область вопросов, рассматриваемая при проведении аудита:

физическая безопасность УЦ Комиссии;

аутентификация и идентификация;

услуги УЦ Комиссии;

безопасность программного обеспечения и доступа к сети;

обеспечение персональной безопасности сотрудников УЦ Комиссии;

ведение журналов событий и мониторинга системы;

процедуры архивирования и резервного копирования.

Действия, предпринимаемые в случае обнаружения недостатков

В случае обнаружения недостатков руководство УЦ Комиссии организует работы по их устранению в кратчайшие сроки.

Сообщение результатов аудита

Отчеты о проведенных внешних аудиторских проверках направляются руководителю УЦ Комиссии.

Другие коммерческие и юридические вопросы

Оплата

Оплата выпуска или обновления сертификатов

УЦ Комиссии предоставляет свои услуги на безвозмездной основе.

Оплата доступа к реестру сертификатов

Оплата доступа к реестру сертификатов не предусмотрена.

Оплата доступа к сервисам получения информации об отзыве или статусе сертификатов

Оплата доступа к сервисам получения информации об отзыве или статусе сертификатов не предусмотрена.

Оплата других услуг

УЦ Комиссии предоставляет свои услуги на безвозмездной основе.

Условия возврата платежей

Нет условий.

Финансовая ответственность

Страховое обеспечение

Нет условий.

Иные активы

Нет условий.

Сфера действия страхования или гарантии для Владельцев сертификатов

Нет условий.

Конфиденциальность информации

Информация, являющаяся конфиденциальной

Конфиденциальной информацией считается:

ключи ЭЦП;

персональная и корпоративная информация Владельцев сертификатов, содержащаяся в УЦ Комиссии и не подлежащая непосредственной рассылке в качестве части сертификата или СОС;

информация, хранящаяся в журналах регистрации событий УЦ Комиссии;

отчетные материалы по выполненным проверкам деятельности УЦ Комиссии;

информация о способах и порядке защиты аппаратного и программного обеспечения УЦ Комиссии, способах администрирования и действий на случай непредвиденных ситуаций;

документы с грифом "для служебного пользования" или "конфиденциально".

Информация, не являющаяся конфиденциальной

Информация, не являющейся конфиденциальной информацией является открытой информацией. Открытая информация может публиковаться по решению УЦ Комиссии. Место, способ и время публикации также определяется решением УЦ Комиссии.

Информация, включаемая в сертификаты и СОС, издаваемые УЦ Комиссии, не считается конфиденциальной. Подразумевается, что Заявитель знает, какая информация будет содержаться в сертификате, и согласен с ее публикацией.

Вся информация, подлежащая публикации в соответствии с данным Регламентом УЦ Комиссии так же не считается конфиденциальной.

Обязательства по защите конфиденциальной информации

Все участники должны не раскрывать и всячески препятствовать раскрытию конфиденциальной информации, каким бы то ни было третьим лицам, за исключением случаев, требующих ее раскрытия в соответствии с действующим законодательством страны пребывания Комиссии или при наличии судебного постановления.

Защита персональных данных

Обеспечение защиты персональных данных

УЦ Комиссии осуществляет защиту персональных данных Владельцев сертификатов в соответствии с законодательством страны пребывания Комиссии.

Данные, рассматриваемые как персональные

Данные, определенные как таковые в соответствии с законодательством страны пребывания Комиссии, за исключением данных, которые должны публиковаться в соответствии с действующим законодательством страны пребывания Комиссии в области ЭЦП.

Данные не рассматриваемая как персональная

Все данные не являющиеся персональными.

Обязательство по защите персональных данных

УЦ Комиссии защищает персональные данные Владельцев сертификатов и всячески препятствует их раскрытию третьим лицам.

Предупреждение и согласие на использование персональных данных

Любое использование персональных данных возможно только с согласия их владельца. Заявление на выпуск сертификата считается согласием на использование указанных в заявлении персональных данных в сертификате.

Раскрытие в соответствии с судебным или административным процессом

Раскрытие персональных данных осуществляется в соответствии с текущим законодательством страны пребывания Комиссии.

Иные условия раскрытия информации

Нет условий.

Права на интеллектуальную собственность

Комиссия является собственником всех документов, программно-технических средств и информационных ресурсов, которые созданы за счет средств Комиссии, приобретены на законных основаниях, получены в порядке дарения или наследования.

Вся продукция, в том числе и интеллектуального характера, произведенная сотрудниками УЦ Комиссии при выполнении ими своих служебных обязанностей, является собственностью Комиссии, если отдельным договором не предусмотрен иной режим.

Комиссия является обладателем исключительных прав на все созданные им объекты интеллектуальной собственности, в соответствии с законодательством страны пребывания Комиссии.

Все торговые марки, лицензии, графические символы и прочее используемое УЦ Комиссии являются интеллектуальной собственностью их владельцев.

Заявления и гарантии

Заявления и гарантии УЦ Комиссии

УЦ Комиссии гарантирует:

что его деятельность соответствует требованиям, установленными законодательством страны пребывания Комиссии и актами Комиссии;

отсутствие каких-либо искажений или ошибок по вине сотрудников УЦ Комиссии в выпущенных сертификатах и СОС;

соответствие сертификата требованиям политик применения сертификатов, в соответствии с которыми он выпущен;

использование репозитория и услуг аннулирования (отзыва) в соответствии с настоящим Регламентом.

Заявления и гарантии ЦС

См. пункт 9.6.1 настоящего Регламента.

Заявления и гарантии Владельца сертификата

Владелец сертификата гарантирует, что:

вся информация, переданная им в заявлении на выпуск сертификата, является достоверной;

ключ ЭЦП хранится в тайне и неавторизованный доступ к нему невозможен;

Сертификат используется только по назначению и в соответствии с требованиями настоящего Регламента и политикой применения сертификатов, в соответствии с которой сертификат выпущен;

немедленно оповестит УЦ Комиссии при компрометации ключа ЭЦП.

Заявления и гарантии Пользователя сертификатов

Используя сертификаты, Пользователь сертификатов гарантирует, что:

использование сертификата осуществляется в соответствии с назначением, указанным в сертификате и требованиями настоящего Регламента;

использование сертификата осуществляется только после проведения проверки ЭЦП сертификата и его статуса, показавшей его действительность, и в соответствие с политикой применения сертификатов, идентификатор которой указан в сертификате.

Заявления и гарантии других участников

Нет условий.

Отказ от гарантий

Нет условий.

Ограничение ответственности

УЦ Комиссии не несет ответственность за неисполнение своих обязательств по независящим от него причинам.

УЦ Комиссии не несет ответственности в случае нарушения Владельцами сертификатов и Пользователями сертификатов требований настоящего Регламента и политик применения сертификатов.

Возмещение ущерба

Нет условий.

Период и прекращение действия регламента

Период действия

Настоящий Регламент и его изменения считаются действующими с момента публикации до момента прекращения его действия.

Прекращение действия

Настоящий Регламент периодически исправляется и дополняется, оставаясь действующим до публикации новой версии, уведомления о прекращении его действия или даты прекращения действия политик применения сертификатов в таком уведомлении.

Результат прекращения действия и долговечность

После завершения действия настоящего Регламента его требования продолжают действовать для всех участников, использующих сертификаты УЦ Комиссии,

выпущенные в период действия настоящего Регламента, в течение всего срока действия таких сертификатов.

Индивидуальные уведомления и связь между участниками

Участники ИОК могут использовать любые способы связи между собой, если каким-либо соглашением не определено иное.

Изменения

Процедура изменения

Изменения в настоящий Регламент могут быть внесены Руководителем УЦ Комиссии. Изменения могут быть оформлены в виде измененного документа либо в виде обновления. Изменения и обновления публикуются.

Срок и механизм оповещения

УЦ Комиссии оставляет за собой право вносить несущественные изменения в Регламент УЦ Комиссии и политики применения сертификатов без оповещения, в случае исправления опечаток, ошибок, URL или изменения контактной информации.

В случае если Руководитель УЦ Комиссии считает, что необходимо немедленное существенное изменение политик применения сертификатов для предотвращения или остановки нарушения безопасности ИОК или любой его части, он может сделать его и опубликовать, после чего оповестить участников.

За исключением вышеописанных случаев изменения и обновления Регламента УЦ Комиссии и политик применения сертификатов публикуются в репозитории УЦ Комиссии не позднее чем за 14 дней до даты ввода в действие данных изменений и дополнений.

Обстоятельства, при которых OID должен быть изменен

Если Руководитель УЦ Комиссии определяет, что необходима замена OID документа, новое обновление должно содержать новый OID.

Условия разрешения споров

При возникновении споров стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путем переговоров. Споры между сторонами, связанные с действием политик применения сертификатов и не урегулированные в процессе переговоров, должны рассматриваться в административном порядке.

Применяемое законодательство

Для определения законности, толкования, интерпретации и исполнения положений настоящего Регламента любой субъект права должен использовать законодательство страны пребывания Комиссии и акты органов Союза.

Соответствие применяемому законодательству

Все участники должны руководствоваться законодательством страны пребывания Комиссии, а так же руководящими документами контролирующих организаций в

области ЭЦП, шифрования и экспорта/импорта программно-аппаратных средств и технической информации страны пребывания Комиссии.

Разнообразные положения

Полнота соглашения

Нет условий.

Передача прав и обязанностей

Нет условий.

Делимость

В случае если по решению суда какие-либо положения данного документа будут признаны не имеющими юридической силы, оставшиеся положения все равно остаются действительными.

Правоприменение

Нет условий.

Форс-мажор

Стороны Регламента УЦ Комиссии освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение явилось следствием форс-мажорных обстоятельств, возникших после возникновения обязательств в соответствии с настоящим Регламентом.

Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон Регламента УЦ Комиссии) и непредотвратимые при данных условиях обстоятельства включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования аппаратно-программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов страны пребывания Комиссии, повлекшие невозможность исполнения Стороной/ Сторонами Регламента УЦ Комиссии своих обязательств по настоящему Регламенту.

В случае возникновения форс-мажорных обстоятельств, срок исполнения Сторонами Регламента УЦ Комиссии своих обязательств по настоящему Регламенту отодвигается соразмерно времени, в течение которого действуют такие обстоятельства.

Сторона Регламента УЦ Комиссии, для которой создалась невозможность исполнения своих обязательств по настоящему Регламенту, должна немедленно известить в письменной форме другую Сторону Регламента УЦ Комиссии о наступлении, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств, а также представить доказательства существования названных обстоятельств.

Не извещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

В случае, если невозможность полного или частичного исполнения Сторонами Регламента УЦ Комиссии какого-либо обязательства по настоящему Регламенту

обусловлена действием форс-мажорных обстоятельств и существует свыше одного месяца, то каждая из Сторон Регламента УЦ Комиссии вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства.

Другие положения

Нет условий.

ПРИЛОЖЕНИЕ № 1
к Регламенту
Удостоверяющего центра
Евразийской экономической комиссии

Порядок работы OCSP-службы и TSP-службы Удостоверяющего центра Евразийской экономической комиссии

УЦ Комиссии оказывает услуги по предоставлению актуальной информации о статусе сертификатов посредством OCSP-службы. OCSP-службы по запросам пользователей УЦ Комиссии формирует и предоставляет этим пользователям OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата ключа ЭЦП. OCSP-ответы представляются в форме электронного документа, подписанного ЭЦП с использованием сертификата ключа подписи Уполномоченного лица УЦ Комиссии. OCSP-ответ признается действительным при одновременном выполнении следующих условий:

Подтверждена подлинность ЭЦП OCSP-службы в OCSP-ответе;

Сертификат Уполномоченного лица УЦ Комиссии на момент подтверждения подлинности ЭЦП OCSP-ответа действителен;

ключ ЭЦП Уполномоченного лица УЦ Комиссии на момент формирования OCSP-ответа действителен;

Сертификат Уполномоченного лица УЦ Комиссии содержит в расширении Extended Key Usage (область использования – ЭЦП ответа OCSP- службы) OID 1.3.6.1.5.5.7.3.9.

адрес обращения к Службе статусов сертификатов Удостоверяющего центра – https: //ca-ocsp.eecommission.org:8877. Указанный адрес заносится в расширение Authority Information Access (AIA) издаваемых УЦ Комиссии сертификатов.

Удостоверяющий центр оказывает услуги по выдаче штампов времени посредством TSP-службы. Штамп времени, относящийся к электронному документу, признается действительным при одновременном выполнении следующих условий:

подтверждена подлинность ЭЦП Уполномоченного лица УЦ Комиссии в штампе времени;

Сертификат Уполномоченного лица УЦ Комиссии на момент подтверждения подлинности ЭП штампа времени действителен;

ключ ЭЦП Уполномоченного лица УЦ Комиссии на момент формирования штампа времени действителен;

Сертификат Уполномоченного лица УЦ Комиссии содержит в расширении Extended Key Usage (область использования – Установка штампа времени) OID= 1.3.6.1.5.5.7.3.8;

адрес обращения к TSP-службы:

https://ca-tsp.eecommission.org:8777

ПРИЛОЖЕНИЕ № 2
к Регламенту
Удостоверяющего центра
Евразийской экономической комиссии

Объектные идентификаторы политик применения сертификатов

Объектный идентификатор	Краткое наименование политики применения сертификатов	Полное наименование политики применения сертификатов
1.2.643.3.294.1.2.1	Базовая политика применения сертификатов	Удостоверяющий центр Евразийской экономической комиссии. Политика применения сертификатов ключей проверки электронной цифровой подписи членов Коллегии Комиссии, должностных лиц и сотрудников Комиссии.
1.2.643.3.294.1.2.2	Политика применения сертификатов OCSP-службы	Удостоверяющий центр Евразийской экономической комиссии. Политика применения сертификатов ключей проверки электронной цифровой подписи OCSP-службы УЦ Комиссии.
1.2.643.3.294.1.2.3	Политика применения сертификатов TSP-службы	Удостоверяющий центр Евразийской экономической комиссии. Политика применения сертификатов ключей проверки электронной цифровой подписи TSP-службы УЦ Комиссии.
1.2.643.3.294.1.2.4	Политика применения SSL сертификатов	Удостоверяющий центр Евразийской экономической комиссии. Политика применения сертификатов аутентификации серверов.
1.2.643.3.294.1.2.5	Политика применения сертификатов ДТС	Удостоверяющий центр Евразийской экономической комиссии. Политика применения сертификатов доверенной третьей стороны Комиссии.

ПРИЛОЖЕНИЕ № 3
к Регламенту
Удостоверяющего центра
Евразийской экономической комиссии

Шаблоны заявлений

Заявление на выпуск сертификата

Я, _____,

(должность, Ф.И.О.)

прошу выпустить сертификат ключа проверки ЭЦП с областью использования в: __

_____

(указать наименование подсистем Интеграционного сегмента Комиссии)

для выпуска сертификата сообщаю следующие данные:

Фамилия, имя, отчество

Подразделение

Должность

Адрес электронной почты (e-mail):

Ключевая фраза

Владелец сертификата _____ _____

(подпись) (фамилия, инициалы)

Подтверждаю, что указанная ключевая фраза является паролем для экстренной связи в случае компрометации ключа ЭЦП и обязуюсь обеспечивать сохранение конфиденциальности данного пароля.

С Регламентом Удостоверяющего центра Евразийской экономической комиссии ознакомлен. В случае выявления факта компрометации ключа ЭЦП, соответствующего выпускаемому на мое имя сертификату, обязуюсь немедленно проинформировать об этом событии Удостоверяющий центр Евразийской экономической комиссии.

Настоящим я,

_____,

(фамилия, имя, отчество владельца сертификата)

_____

(серия и номер паспорта, кем и когда выдан)

соглашаюсь с обработкой своих персональных данных Удостоверяющим центром Евразийской экономической комиссии и признаю, что персональные данные, заносимые в сертификаты ключей проверки ЭЦП, владельцем которых я являюсь, относятся к общедоступным персональным данным

Владелец сертификата _____ _____

(подпись) (фамилия, инициалы)

Руководитель подразделения _____ _____

(подпись) (фамилия, инициалы)

"____"_____ 20____ г.

Заявление
на аннулирование (отзыв) сертификата

Я, _____,

(должность, Ф.И.О.)

в связи с _____

_

(причина отзыва сертификата)

прошу аннулировать (отозвать) мой сертификат ключа проверки ЭЦП, содержащий следующие данные:

Серийный номер сертификата

Фамилия, имя, отчество

Подразделение

Должность

Адрес электронной почты (e-mail):

Владелец сертификата _____ _____

(подпись) (фамилия, инициалы)

"____" _____ 20____ г.

Заявление
на приостановление действия сертификата

Я, _____,

(должность, Ф.И.О.)

прошу приостановить действие моего сертификата ключа проверки ЭЦП, содержащего следующие данные:

Серийный номер сертификата

Фамилия, Имя, Отчество

Подразделение

Должность

Адрес электронной почты (e-mail):

Срок приостановления действия сертификата _____ дней.

(количество дней)

Владелец сертификата _____ _____

(подпись) (фамилия, инициалы)

"____" _____ 20____ г.

Заявление
на возобновление действия сертификата

Я, _____,

(должность, Ф.И.О.)

прошу возобновить действие моего сертификата ключ проверки ЭЦП, содержащего следующие данные:

Серийный номер сертификата

Фамилия, имя, отчество

Подразделение

Должность

Адрес электронной почты (e-mail):

Владелец сертификата _____ _____
(подпись) (фамилия, инициалы)

"____" _____ 20____ г.

Заявление
на создание ключа электронной цифровой подписи

Я,_____,
(должность, Ф.И.О.)

прошу создать ключ электронной цифровой подписи.

Данные ключевого носителя для хранения создаваемого ключа электронной цифровой подписи:

Тип ключевого носителя

Серийный номер ключевого носителя

_____ _____
(подпись) (фамилия, инициалы)

"____" _____ 20____ г.

ПРИЛОЖЕНИЕ № 4
к Регламенту
Удостоверяющего центра
Евразийской экономической комиссии

Порядок проведения работ по подтверждению действительности ЭЦП и штампов времени

УЦ Комиссии осуществляет проведение работ по подтверждению подлинности ЭЦП электронного документа, подтверждению действительности штампа времени или соответствия штампа времени электронному документу (далее Специальные работы), по заявлению пользователя сертификата.

Решение о подлинности ЭЦП электронного документа принимает УЦ Комиссии.

В заявлении на подтверждение подлинности ЭЦП в электронном документе указываются:

дата и время подачи заявления;

идентификационные данные Владельца сертификата, подлинность ЭЦП которого необходимо подтвердить в электронном документе;

наименование файла, содержащего электронный документ с ЭЦП, подлинность которой необходимо проверить;

дата и время формирования ЭЦП электронного документа;

дата и время, на момент наступления которых требуется установить подлинность ЭЦП.

Обязательным приложением к заявлению на подтверждение подлинности ЭЦП в электронном документе является отчуждаемый носитель информации CD/DVD-ROM, содержащий:

Сертификат, с использованием которого необходимо осуществить подтверждение подлинности ЭЦП в электронном документе;

электронный документ – в виде одного файла, содержащего данные и значение ЭЦП этих данных, либо двух файлов: один из которых содержит данные, а другой значение ЭЦП этих данных.

В заявлении на подтверждение действительности штампа времени и соответствии штампа времени электронному документу указываются:

дата и время подачи заявления;

наименование файла стандарта CMS, содержащего штамп времени, действительность которого необходимо подтвердить;

наименование файла, содержащего исходные данные, для которых был сформирован штамп времени;

дата и время, на момент наступления которых требуется подтвердить действительность штампа времени.

Обязательным приложением к заявлению на подтверждение действительности штампа времени и соответствии штампа времени электронному документу является отчуждаемый носитель информации CD/DVD-ROM, содержащий:

файл, содержащий штамп времени, действительность которого необходимо подтвердить;

файл, содержащий исходные данные, для которых был сформирован штамп времени.

Проведение Специальных работ осуществляет комиссия, сформированная из числа сотрудников УЦ Комиссии. Результатом проведения Специальных работ является заключение УЦ Комиссии. Заключение содержит:

состав комиссии, осуществлявшей проверку;

основание для проведения проверки;

результат проверки ЭЦП электронного документа или результат проверки штампа времени и его соответствия исходным данным;

данные, представленные комиссии для проведения проверки.

отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

время и место проведения проверки;

содержание и результаты проверки;

обоснование результатов проверки.

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

Срок проведения Специальных работ по одной ЭЦП или одному штампу времени и предоставлению пользователю заключения по выполненной проверке составляет десять рабочих дней с момента поступления заявления в УЦ Комиссии.