УТВЕРЖДЕНЫ

Решением Совета
Евразийской экономической комиссии
от 20 г. №

ТРЕБОВАНИЯ
к созданию, развитию и функционированию трансграничного пространства доверия

I. Общие положения

1. Настоящие Требования разработаны в соответствии с пунктом 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) и устанавливают требования к созданию, развитию и функционированию трансграничного пространства доверия в рамках Евразийского экономического союза (далее – Союз).

2. Целью настоящих Требований является обеспечение взаимоприемлемого уровня доверия при межгосударственном обмене данными и электронными документами органов государственной власти государств – членов Союза (далее – государства-члены) между собой и с Евразийской экономической комиссией (далее – Комиссия), а также защищенности и надежности функционирования трансграничного пространства доверия в результате применения субъектами электронного взаимодействия в рамках Союза данных требований.

3. Требования к элементам трансграничного пространства доверия устанавливают правовые, организационные и технические условия обеспечения доверия при межгосударственном обмене данными и

электронными документами, в том числе охватывают вопросы защиты информации.

4. Требования к элементам трансграничного пространства доверия определяются в соответствии с актуальными для таких элементов угрозами безопасности информации и действиями нарушителя.

5. Настоящие Требования не распространяются на какие-либо сервисы, элементы и компоненты, которые используются исключительно для целей внутригосударственного обмена данными и электронными документами.

6. Для целей настоящих Требований используются понятия, которые означают следующее:

«аккредитация» – комплекс организационно-технических мероприятий, в результате которых документально подтверждается соответствие заявителя (уполномоченного органа или организации) условиям аккредитации и официальное признание межгосударственной комиссией и уполномоченными органами его способности (компетентности) осуществлять функции и предоставлять услуги в рамках трансграничного пространства доверия в соответствии с настоящими Требованиями;

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

«межгосударственная комиссия» – комиссия, сформированная из представителей уполномоченных органов и Комиссии, выполняющая проверку компонентов общей инфраструктуры документирования

информации в электронном виде на соответствие настоящим Требованиям;

«общая инфраструктура документирования информации в электронном виде» – совокупность информационно-технологических и организационно-правовых мероприятий, правил и решений, реализуемых в целях придания юридической силы электронным документам, используемым в рамках Союза;

«операторы общей инфраструктуры документирования информации в электронном виде» – Комиссия и уполномоченные органы или определенные ими в соответствии с законодательством государств-членов организации, аккредитованные межгосударственной комиссией для предоставления услуг и осуществления функций в рамках трансграничного пространства доверия в соответствии с настоящими Требованиями;

«сертификат ключа проверки ЭЦП» – электронный документ, изданный удостоверяющим центром, подписанный ЭЦП удостоверяющего центра с использованием ключа ЭЦП и содержащий информацию, подтверждающую принадлежность указанного в сертификате ключа проверки ЭЦП определенному участнику обмена электронными документами, и иную информацию, предусмотренную соответствующими криптографическими стандартами и настоящими Требованиями;

«служба доверенной третьей стороны» – совокупность сервисов доверенной третьей стороны, функционирующих в составе интеграционного сегмента Комиссии и национальных сегментов интегрированной информационной системы Союза, обеспечивающих единое трансграничное пространство доверия ЭЦП при электронной

форме взаимодействия субъектов средствами интегрированной информационной системы Союза;

«средства доверенной третьей стороны» – программные и (или) аппаратные средства, используемые для реализации функций доверенной третьей стороны;

«средства удостоверяющего центра» – программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

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

«удостоверяющий центр» – уполномоченный орган или организация, обеспечивающие в соответствии с актами Комиссии или законодательством государства-члена предоставление услуг по созданию, распространению, хранению сертификатов ключей проверки ЭЦП и по проверке действительности этих сертификатов для использования в рамках трансграничного пространства доверия;

«уполномоченный орган» – орган государственной власти государства-члена или определенная им организация, наделенные полномочиями по реализации государственной политики в отдельных сферах;

«штамп времени» – электронный документ, используемый для доказательства факта существования какого-либо электронного документа в определенный момент времени, в котором заверенными ЭЦП являются значение хэш-функции от содержимого электронного документа и момент времени предоставления такого значения для заверения;

«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).

II. Создание, развитие и функционирование трансграничного пространства доверия

7. Создание, развитие и функционирование трансграничного пространства доверия обеспечивается Комиссией и уполномоченными органами в соответствии с Концепцией использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов, утвержденной Решением Совета Евразийской экономической комиссии от 18 сентября 2014 г. № 73, Стратегией развития трансграничного пространства доверия, утвержденной Решением Коллегии Евразийской экономической комиссии от 27 сентября 2016 г. № 105, Положением об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, утвержденным Решением Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125, а также с иными актами Комиссии по вопросам создания, развития и функционирования трансграничного пространства доверия.

8. Контроль за созданием, развитием и функционированием трансграничного пространства доверия осуществляется межгосударственной комиссией, в том числе путем проверки компонентов общей инфраструктуры документирования информации в электронном виде на соответствие настоящим Требованиям.

9. В целях обеспечения развития и контроля функционирования трансграничного пространства доверия в рамках национальных сегментов государств-членов интегрированной информационной системы Союза (далее – интегрированная система) государствами-членами определяются уполномоченные органы для осуществления контроля за соблюдением требований к правовым, организационным, техническим условиям обеспечения трансграничного пространства доверия, в том числе касающихся защиты информации государственных компонентов общей инфраструктуры документирования информации в электронном виде.

10. Общая инфраструктура документирования информации в электронном виде состоит из государственных компонентов и интеграционного компонента.

11. Оператором интеграционного компонента общей инфраструктуры документирования информации в электронном виде выступает Комиссия.

12. Операторами государственных компонентов общей инфраструктуры документирования информации в электронном виде выступают уполномоченные органы или определенные ими организации.

13. Субъектами электронного взаимодействия в рамках Союза являются государственные органы, физические или юридические лица,

взаимодействующие в рамках отношений, возникающих в процессе составления, отправления, передачи, получения, хранения и использования электронных документов и информации в электронном виде.

14. При электронном взаимодействии в рамках Союза доверие между субъектами электронного взаимодействия обеспечивается операторами общей инфраструктуры документирования информации в электронном виде и предоставляемыми ими доверенными сервисами, реализуемыми при помощи элементов трансграничного пространства доверия.

15. Элементы трансграничного пространства доверия, входящие в состав государственных компонентов и интеграционного компонента общей инфраструктуры документирования информации в электронном виде, должны соответствовать описанию согласно приложению № 1.

16. Элементы трансграничного пространства доверия эксплуатируются аккредитованными операторами общей инфраструктуры документирования информации в электронном виде для предоставления услуг и осуществления функций в рамках трансграничного пространства доверия в соответствии с настоящими Требованиями.

17. Оператор общей инфраструктуры документирования информации в электронном виде может обеспечивать эксплуатацию нескольких элементов трансграничного пространства доверия.

18. Операторы общей инфраструктуры документирования информации в электронном виде несут ответственность за ущерб, причиненный субъектам электронного взаимодействия в результате:

а) неисполнения или ненадлежащего исполнения обязанностей, предусмотренных настоящими Требованиями;

б) неисполнения или ненадлежащего исполнения обязанностей, предусмотренных законодательством государства-члена, в государственный компонент которого они входят.

19. Комиссия и государства-члены устанавливают согласованные требования к ответственности за нарушение настоящих Требований в части деятельности операторов общей инфраструктуры документирования информации в электронном виде.

20. Аккредитация операторов общей инфраструктуры документирования информации в электронном виде осуществляется в соответствии с Положением о комиссии по проверке компонентов общей инфраструктуры документирования информации в электронном виде на соответствие требованиям к созданию, развитию и функционированию трансграничного пространства доверия, утвержденным Решением Совета Евразийской экономической комиссии от № .

III. Общая инфраструктура документирования информации в электронном виде

1. Требования к удостоверяющему центру службы доверенной третьей стороны

21. Удостоверяющий центр службы доверенной третьей стороны осуществляет деятельность по созданию сертификатов ключей проверки ЭЦП, предназначенных для организации электронного взаимодействия доверенной третьей стороны, функционирующей в составе интеграционного сегмента Комиссии интегрированной системы

(далее – доверенная третья сторона Комиссии), и уполномоченных доверенных третьих сторон, функционирующих в национальных сегментах государств-членов интегрированной системы (далее – доверенные третьи стороны государств-членов).

22. Владельцами сертификатов ключей проверки ЭЦП, выдаваемых удостоверяющим центром службы доверенной третьей стороны, являются:

доверенная третья сторона Комиссии;

доверенные третьи стороны государств-членов.

23. Удостоверяющий центр службы доверенной третьей стороны должен функционировать в соответствии с международными рекомендациями по построению инфраструктуры открытых ключей (Public Key Infrastructure) и согласованными с уполномоченными органами требованиями.

24. Удостоверяющий центр службы доверенной третьей стороны для создания сертификатов ключей проверки ЭЦП должен использовать средства удостоверяющего центра, соответствующие требованиям согласно приложению № 2. Перед использованием указанных средств их соответствие указанным установленным требованиям должно быть подтверждено уполномоченными органами страны пребывания Комиссии в порядке, установленном ее законодательством. Перед использованием средств удостоверяющего центра, разработанных для удостоверяющего центра службы доверенной третьей стороны в рамках проекта по совместной разработке специализированных средств криптографической защиты информации Союза, их соответствие указанным установленным требованиям должно быть подтверждено

уполномоченными органами всех государств-членов в порядке, установленном их законодательством.

25. Требования к функционированию удостоверяющего центра службы доверенной третьей стороны устанавливаются с учетом утверждаемых Комиссией моделей угроз безопасности информации и действий нарушителя.

26. Удостоверяющий центр службы доверенной третьей стороны должен обеспечивать выполнение следующих основных функций:

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

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

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

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

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

е) прекращение действия и аннулирование сертификатов ключей проверки ЭЦП;

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

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

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

к) проверка уникальности ключей проверки ЭЦП в реестре сертификатов и отказ в создании сертификата ключа проверки ЭЦП в случае отрицательного результата проверки уникальности ключа

проверки ЭЦП, указанного в запросе доверенной третьей стороны Комиссии или доверенной третьей стороны государства-члена;

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

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

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

о) осуществление проверок ЭЦП по обращениям доверенной третьей стороны Комиссии или доверенных третьих сторон государств-членов, созданных с использованием выданных им сертификатов ключей проверки ЭЦП;

п) создание штампов времени на квитанциях доверенной третьей стороны Комиссии и квитанциях доверенных третьих сторон государств-членов, содержащих результаты проверки ЭЦП, которыми подписаны электронные документы, при обращении таких доверенных третьих сторон с целью подтверждения времени создания электронных документов и их подписания соответствующей ЭЦП;

р) осуществление иных, связанных с использованием ЭЦП, функций.

27. Для функционирования удостоверяющего центра службы доверенной третьей стороны Комиссия во взаимодействии с

уполномоченными органами разрабатывает и утверждает технические, технологические, методические и организационные документы, предусматривающие детализацию требований к удостоверяющему центру службы доверенной третьей стороны.

28. Настоящие Требования и требования, содержащиеся в актах, утверждаемых Комиссией для обеспечения функционирования удостоверяющего центра службы доверенной третьей стороны, применяются межгосударственной комиссией для проверки удостоверяющего центра службы доверенной третьей стороны в рамках проверки интеграционного компонента общей инфраструктуры документирования информации в электронном виде.

2. Требования к службе доверенной третьей стороны и входящим в ее состав доверенным третьим сторонам

29. Служба доверенной третьей стороны является функциональной частью интегрированной системы.

30. Служба доверенной третьей стороны должна включать в себя сервисы доверенной третьей стороны Комиссии и сервисы доверенных третьих сторон государств-членов.

31. Каждая из доверенных третьих сторон, сервисы которых входят в состав службы доверенной третьей стороны, в соответствии с пунктом 21 Протокола об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза должна выполнять следующие задачи:

а) осуществление легализации (подтверждение подлинности) электронных документов и ЭЦП субъектов информационного взаимодействия в фиксированный момент времени;

б) обеспечение гарантий доверия в межгосударственном (трансграничном) обмене данными и электронными документами;

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

32. Доверенная третья сторона Комиссии и доверенные третьи стороны государств-членов должны обеспечивать функционирование в своем составе следующей совокупности сервисов, реализуемых с использованием средств доверенной третьей стороны:

а) сервис подтверждения подлинности (проверка ЭЦП, действительности и соответствия сертификата ключа проверки ЭЦП установленным требованиям, получение результата от сервиса проверки полномочий и формирование квитанций с результатом проверки подлинности электронного документа);

б) сервис проверки полномочий (проверка полномочий субъекта электронного взаимодействия, сформировавшего и подписавшего электронный документ в национальном сегменте государства-члена или интеграционном сегменте Комиссии интегрированной системы);

в) сервис штампа времени (создание штампов времени для электронных документов, входящих в национальный сегмент государства-члена или интеграционный сегмент Комиссии интегрированной системы, и квитанций с результатом проверки подлинности электронного документа);

г) сервис хранения данных (документирование выполняемых доверенной третьей стороной операций);

д) сервис предоставления информации (об операциях доверенной третьей стороны по запросам уполномоченных органов и Комиссии).

33. Сервисы, реализуемые средствами доверенной третьей стороны Комиссии или средствами доверенных третьих сторон государств-членов, должны соответствовать настоящим Требованиям, Положению об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, а также актам Комиссии, касающимся вопросов функционирования доверенных третьих сторон.

34. Доверенная третья сторона Комиссии и доверенные третьи стороны государств-членов при выполнении своих функций должны обеспечить соблюдение в совокупности следующих основных условий:

а) обеспечение конфиденциальности ключа ЭЦП, ключ проверки которого содержится в выданном удостоверяющим центром службы доверенной третьей стороны сертификате ключа проверки ЭЦП;

б) уведомление удостоверяющего центра службы доверенной третьей стороны, доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов о нарушении конфиденциальности ключа ЭЦП, предназначенного для электронного взаимодействия в рамках Союза, в течение не более чем 12 часов с момента получения информации о таком нарушении;

в) прекращение использования ключа ЭЦП, предназначенного для электронного взаимодействия в рамках Союза, при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

г) использование ключа ЭЦП, предназначенного для электронного взаимодействия в рамках Союза, исключительно для подписания квитанций с результатами проверки ЭЦП электронного документа;

д) использование для создания и проверки ЭЦП, создания ключей ЭЦП и ключей проверки ЭЦП, предназначенных для электронного взаимодействия в рамках Союза, средств криптографической защиты информации, реализующих криптографические алгоритмы, определенные в соответствии с Решением Коллегии Евразийской экономической комиссии от 2 июня 2016 г. № 49 (ДСП), до реализации проекта по совместной разработке специализированных средств криптографической защиты информации Союза;

е) при проверке ЭЦП в электронных документах проверка соблюдения в совокупности следующих условий:

целостность данных, подписываемых ЭЦП, не нарушена;

ЭЦП выработана с использованием ключа ЭЦП, соответствующий сертификат ключа проверки ЭЦП имеется в распоряжении доверенной третьей стороны на момент начала проверки либо получен доверенной третьей стороной в процессе выполнения процедур проверки;

сертификат ключа проверки ЭЦП действителен на момент подписания электронного документа;

каждый сертификат ключа проверки ЭЦП из цепочки сертификатов ключей проверки ЭЦП удостоверяющих центров действителен на момент подписания;

ж) документирование и хранение в течение периода, установленного актами Комиссии или законодательством государств-членов, всей необходимой информации относительно всех проводимых проверок ЭЦП в электронных документах для обеспечения непрерывности оказания услуг и представления (в случае необходимости) доказательств в суде. Хранение указанной информации может осуществляться в электронном виде.

35. Доверенная третья сторона Комиссии должна использовать средства доверенной третьей стороны и средства ЭЦП в их составе, соответствующие требованиям согласно приложению № 3.

36. Комиссия для обеспечения функционирования доверенной третьей стороны Комиссии разрабатывает во взаимодействии с уполномоченными органами и утверждает технические, технологические, методические и организационные документы, предусматривающие детализацию компонентов и требований к доверенной третьей стороне интеграционного сегмента Комиссии интегрированной системы.

37. Требования к взаимодействию доверенной третьей стороны Комиссии и доверенных третьих сторон государств-членов между собой и с удостоверяющим центром службы доверенной третьей стороны устанавливаются с учетом соответствующих утверждаемых Комиссией моделей угроз безопасности информации и действий нарушителя.

38. Для обеспечения функционирования доверенных третьих сторон государств-членов уполномоченные органы разрабатывают и утверждают в соответствии с законодательством государств-членов и актами Комиссии технические, технологические, методические и организационные документы, предусматривающие детализацию компонентов и требований к доверенным третьим сторонам государств-членов.

39. Комиссия осуществляет передачу программных и аппаратных средств криптографической защиты информации, разработанных в рамках работ по созданию и развитию интегрированной системы и предназначенных для функционирования доверенных третьих сторон, уполномоченным органам заинтересованных государств-членов для

использования в составе национальных сегментов в порядке, утверждаемом Комиссией.

40. Настоящие Требования и требования, содержащиеся в документах, утверждаемых государствами-членами и Комиссией для обеспечения функционирования доверенных третьих сторон, используются межгосударственной комиссией для проверки службы доверенной третьей стороны и входящих в ее состав доверенных третьих сторон в рамках проверки компонентов общей инфраструктуры документирования информации в электронном виде.

3. Требования к удостоверяющему центру Комиссии и удостоверяющим центрам государств-членов, обеспечивающим субъектов электронного взаимодействия в рамках Союза сертификатами ключей проверки ЭЦП

41. Удостоверяющий центр Комиссии и удостоверяющие центры государств-членов, обеспечивающие субъектов электронного взаимодействия сертификатами ключей ЭЦП для электронного взаимодействия в рамках Союза, в соответствии со Стратегией развития трансграничного пространства доверия, являются элементами трансграничного пространства доверия и входят в состав компонентов общей инфраструктуры документирования информации в электронном виде.

42. Для электронного взаимодействия в рамках Союза допускаются только уполномоченные (аккредитованные) в соответствии с законодательством государств-членов или актами Комиссии удостоверяющие центры.

43. Удостоверяющий центр Комиссии и удостоверяющие центры государств-членов должны функционировать в соответствии с

международными рекомендациями по построению инфраструктуры открытых ключей (Public Key Infrastructure) и выполнять минимально необходимые требования, указанные в пункте 49 настоящих Требований.

44. Требования к деятельности удостоверяющих центров государств-членов, в том числе по защите информации, устанавливаются с учетом актуальных угроз безопасности информации и действий нарушителя в соответствии с законодательством государств-членов в сфере защиты информации.

45. Требования к деятельности удостоверяющего центра Комиссии устанавливаются с учетом утверждаемой Комиссией модели угроз безопасности информации и действий нарушителя в удостоверяющем центре Комиссии.

Удостоверяющий центр Комиссии для создания сертификатов ключей проверки ЭЦП должен использовать средства ЭЦП и средства удостоверяющего центра, соответствующие требованиям согласно приложению № 4. Перед использованием указанных средств их соответствие указанным требованиям должно быть подтверждено уполномоченными органами страны пребывания Комиссии в порядке, установленном ее законодательством.

46. Удостоверяющие центры государств-членов создают сертификаты ключей проверки ЭЦП в соответствии с законодательством соответствующего государства-члена.

47. Удостоверяющий центр Комиссии создает сертификаты ключей проверки ЭЦП в соответствии с настоящими Требованиями.

48. Для создания и проверки ЭЦП в государствах-членах должны использоваться сертифицированные (прошедшие проверку) в соответствии с их законодательством средства ЭЦП.

49. Для функционирования удостоверяющих центров в соответствии с законодательством государств-членов устанавливаются следующие минимально необходимые требования:

а) обеспечение проверки личности субъектов электронного взаимодействия при выдаче сертификатов ключей проверки ЭЦП. Проверка личности получателя сертификата осуществляется либо непосредственно удостоверяющим центром, либо с привлечением третьего лица (центра регистрации и т.п.), если это предусмотрено законодательством государств-членов;

б) подробное информирование получателя сертификата ключа проверки ЭЦП при выдаче такого сертификата об условиях пользования услугами удостоверяющего центра, включая любые ограничения по их использованию;

в) выдача субъектам электронного взаимодействия в соответствии с законодательством государств-членов или актами Комиссии сертификатов ключей проверки ЭЦП, соответствующих требованиям согласно приложению № 5;

г) ведение и своевременное обновление реестров сертификатов, с предоставлением всем субъектам электронного взаимодействия информации о статусе (актуальности) всех выданных сертификатов ключей проверки ЭЦП. Такая информация должна быть доступна в любое время, в том числе и после прекращения действия сертификата ключа проверки ЭЦП, и предоставляться автоматизированным способом;

д) оперативное (не позднее 60 минут с момента получения соответствующего запроса) внесение информации в реестр сертификатов и список отозванных сертификатов при отзыве сертификатов. Сертификат 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 в течение периода, установленного законодательством государств-членов или актами Комиссии, всей необходимой информации относительно выдачи, получения и изменения статусов (актуальности) сертификатов ключей проверки ЭЦП (в том числе после прекращения деятельности по обеспечению субъектов электронного взаимодействия в рамках Союза сертификатами ключей ЭЦП) для обеспечения непрерывности оказания услуг и представления (при необходимости) доказательств в суде. Хранение указанной информации может осуществляться в электронном виде;

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

з) информирование уполномоченных органов о любых изменениях в выполнении закрепленных за ними функций, а также о намерении прекратить деятельность по обеспечению субъектов электронного взаимодействия в рамках Союза сертификатами ключей ЭЦП или иных случаях прекращения деятельности.

50. Для функционирования удостоверяющих центров государств-членов уполномоченные органы разрабатывают и утверждают

технические, технологические, методические и организационные документы в соответствии с законодательством своих государств-членов.

51. Комиссия для обеспечения функционирования удостоверяющего центра Комиссии разрабатывает во взаимодействии с уполномоченными органами и утверждает технические, технологические, методические и организационные документы.

52. Настоящие Требования и требования, содержащиеся в документах, утверждаемых государствами-членами и Комиссией для обеспечения функционирования удостоверяющих центров, используются межгосударственной комиссией для проверки службы доверенной третьей стороны в рамках проверки компонентов общей инфраструктуры документирования информации в электронном виде.

4. Требования к инфраструктуре обеспечения взаимодействия информационных систем и ресурсов государств-членов и Комиссии при межгосударственном обмене данными и электронными документами

53. Инфраструктура обеспечения взаимодействия информационных систем и ресурсов государств-членов и Комиссии при межгосударственном обмене данными и электронными документами состоит из интеграционной платформы интегрированной системы и систем межведомственного информационного взаимодействия государств-членов.

54. Интеграционная платформа интегрированной системы состоит из интеграционных шлюзов, подсистемы синхронизации данных, транспортной подсистемы, подсистемы взаимодействия с внешними информационными системами и подсистемы сопряжения.

55. Интеграционная платформа интегрированной системы включает в себя интеграционные шлюзы государств-членов, функционирующие в составе национальных сегментов государств-членов интегрированной системы, и интеграционный шлюз Комиссии, функционирующий в составе интеграционного сегмента Комиссии интегрированной системы.

56. Интеграционная платформа интегрированной системы в рамках подсистемы синхронизации данных должна обеспечивать информационное взаимодействие подсистем интегрированной системы в рамках интеграционного сегмента Комиссии.

57. Интеграционная платформа интегрированной системы в рамках транспортной подсистемы должна обеспечивать гарантированную доставку электронных сообщений между компонентами интеграционной платформы с использованием очередей сообщений.

58. Интеграционная платформа интегрированной системы в рамках подсистемы взаимодействия с внешними информационными системами должна обеспечивать единую точку подключения к интеграционной платформе при организации информационного взаимодействия с информационными системами интеграционных объединений, международных организаций и государств, не являющихся членами Союза (далее – внешние информационные системы).

59. Интеграционная платформа интегрированной системы в рамках подсистемы сопряжения должна обеспечивать взаимодействие между интеграционным шлюзом интеграционной платформы и применяемыми в государствах-членах системами межведомственного

информационного взаимодействия (для интеграционных шлюзов национальных сегментов государств-членов, реализованных на основе типового интеграционного шлюза), а также между подсистемой взаимодействия с внешними информационными системами.

60. Обмен информацией между интеграционным шлюзом интеграционного сегмента Комиссии интегрированной системы и подсистемой синхронизации данных, а также обмен информацией между интеграционными шлюзами национальных сегментов государств-членов интегрированной системы, между интеграционным шлюзом интеграционного сегмента Комиссии интегрированной системы и интеграционными шлюзами национальных сегментов государств-членов интегрированной системы должен выполняться в соответствии с Правилами электронного обмена данными в интегрированной информационной системе внешней и взаимной торговли, утвержденными Решением Коллегии Евразийской экономической комиссии от 27 января 2015 г. № 5.

61. Вычислительные ресурсы интеграционных шлюзов национальных сегментов государств-членов и интеграционного шлюза Комиссии должны обеспечить уровень своей доступности 24 часа в сутки, 7 дней в неделю, 365 (366) дней в году, за исключением периодов технического обслуживания.

62. Интеграционная платформа интегрированной системы должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверным форматом или недопустимыми значениями входных данных. В указанных случаях интеграционная платформа интегрированной системы должна обеспечивать сохранение информации об аварийных ситуациях в соответствующих журналах, после чего возвращаться в

рабочее состояние, предшествовавшее поступлению некорректных входных данных.

63. Интеграционные шлюзы и системы межведомственного информационного взаимодействия государств-членов должны обеспечивать защиту передаваемых данных.

64. Операторы интеграционных шлюзов должны ограничить круг сотрудников, имеющих доступ к передаваемым данным, при этом доступ к данным должен предоставляться таким сотрудникам только для расследования нештатных (конфликтных) ситуаций.

65. Интеграционные шлюзы и системы межведомственного информационного взаимодействия государств-членов должны обеспечивать идентификацию и аутентификацию отправителей и получателей передаваемых данных.

66. Интеграционные шлюзы должны обеспечивать документирование информации относительно операций, проведенных с передаваемыми и получаемыми данными, в том числе с электронными документами, и ее хранение в течение периода, установленного законодательством государств-членов или актами Комиссии, в том числе для возможности представления доказательств в суде.

67. Сервисы интеграционных шлюзов, используемые для реализации обмена электронными документами при трансграничном взаимодействии органов государственной власти государств-членов между собой и с Комиссией, должны соответствовать настоящим Требованиям, требованиям Положения об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической

комиссией и иным актам Комиссии по вопросам функционирования интеграционных шлюзов.

5. Требования к инфраструктуре и системам обеспечения защиты информации

68. Для защиты интеграционного сегмента Комиссии интегрированной системы Комиссией используется подсистема информационной безопасности, предназначенная в соответствии с техническим заданием на создание интегрированной информационной системы Евразийского экономического союза, утвержденным Решением Коллегии Евразийской экономической комиссии от 12 октября 2015 г. № 137, обеспечивать конфиденциальность, целостность и доступность данных при их обработке и хранении в интеграционном сегменте Комиссии, а также при их передаче по каналам связи при взаимодействии с национальными сегментами государств-членов интегрированной системы.

69. Для защиты национальных сегментов государств-членов интегрированной системы уполномоченными органами должны обеспечиваться создание и внедрение в государствах-членах подсистем защиты информации национальных сегментов государств-членов, предназначенных в соответствии с техническим заданием на создание интегрированной системы обеспечивать конфиденциальность, целостность и доступность данных при их создании, обработке и хранении в национальном сегменте государства-члена, а также при их передаче по каналам связи при взаимодействии с интеграционным сегментом Комиссии и национальными сегментами других государств-членов интегрированной системы. Для обеспечения конфиденциальности, целостности, доступности и сохранности

информации в национальном сегменте государства-члена интегрированной системы принимается и реализуется комплекс правовых, организационных и техническим мер защиты информации в соответствии с законодательством соответствующего государства-члена.

70. Операторы государственных компонентов общей инфраструктуры документирования информации в электронном виде должны принимать технические и организационные меры, направленные на нейтрализацию угроз для выполняемых ими функций. Указанные меры должны реализовываться на основе определения угроз безопасности информации и действий нарушителя, отраженных в документах (заданиях по безопасности, моделях угроз и др.), разрабатываемых в соответствии с законодательством государств-членов.

71. Операторы государственных компонентов общей инфраструктуры документирования информации в электронном виде должны обеспечивать наличие у своих сотрудников необходимых знаний, надежности, лояльности, опыта и квалификации, а также прохождение ими достаточной подготовки в области защиты информации в соответствии с законодательством соответствующего государства-члена.

72. В случае выявления любых фактов нарушения конфиденциальности, целостности и доступности информации элементов трансграничного пространства доверия операторы государственных компонентов общей инфраструктуры документирования информации в электронном виде должны максимально оперативно уведомить об этом свой уполномоченный орган.

Если нарушение защиты информации затрагивает 2 или более государства-члена, получивший такое уведомление уполномоченный орган уведомляет об этом уполномоченные органы других государств-членов и межгосударственную комиссию.

73. Меры и способы обеспечения защиты информации, реализуемые операторами государственных компонентов общей инфраструктуры документирования информации в электронном виде в отношении элементов трансграничного пространства доверия и предоставляемых ими доверенных сервисов, должны соответствовать требованиям согласно приложению № 6.