О Правилах признания электронной цифровой подписи (электронной подписи) в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии юридических лиц (хозяйствующих субъектов) с уполномоченными органами государств – членов Евразийского экономического союза и Евразийской экономической комиссией с использованием службы доверенной третьей стороны

Решение Коллегии Евразийской экономической комиссии от 22 августа 2023 года № 120.

В соответствии с пунктами 11 и 30 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 пунктом 5.2.3 плана мероприятий по реализации Стратегических направлений развития евразийской экономической интеграции до 2025 года, утвержденного распоряжением Совета Евразийской экономической комиссии от 5 апреля 2021 г. № 4, Коллегия Евразийской экономической комиссии **решила:**

1. Утвердить прилагаемые Правила признания электронной цифровой подписи (электронной подписи) в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии юридических лиц (хозяйствующих субъектов) с уполномоченными органами государств – членов Евразийского экономического союза и Евразийской экономической комиссией с использованием службы доверенной третьей стороны.

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

Председатель Коллегии
Евразийской экономической комиссии *М. Мясникович*

УТВЕРЖДЕНЫ
Решением Коллегии
Евразийской экономической комиссии
от 22 августа 2023 г. № 120

ПРАВИЛА

признания электронной цифровой подписи (электронной подписи) в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии юридических лиц (хозяйствующих субъектов) с

уполномоченными органами государств – членов Евразийского экономического союза и Евразийской экономической комиссией с использованием службы доверенной третьей стороны

I. Общие положения

1. Настоящие Правила разработаны в соответствии со следующими международными договорами и актами, составляющими право Евразийского экономического союза (далее – Союз):

Протокол 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);

Решение Евразийского межправительственного совета от 9 августа 2019 г. № 7 "О Концепции трансграничного информационного взаимодействия";

Решение Совета Евразийской экономической комиссии от 5 декабря 2018 г. № 96 " О требованиях к созданию, развитию и функционированию трансграничного пространства доверия";

Решение Совета Евразийской экономической комиссии от 18 сентября 2014 г. № 73 "О Концепции использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов";

Решение Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125 "Об утверждении Положения об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией";

распоряжение Совета Евразийской экономической комиссии от 5 апреля 2021 г. № 4 "О плане мероприятий по реализации Стратегических направлений развития евразийской экономической интеграции до 2025 года".

2. Настоящие Правила определяют порядок признания электронной цифровой подписи (электронной подписи) в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии юридических лиц (хозяйствующих субъектов) с уполномоченными органами государств – членов Союза (далее – государства-члены) и Евразийской экономической комиссией (далее – Комиссия) с использованием службы доверенной третьей стороны.

3. Настоящие Правила применяются в сферах, предусмотренных перечнем, утвержденным распоряжением Коллегии Евразийской экономической комиссии от 25 января 2022 г. № 8.

Применение положений настоящих Правил допускается также в иных сферах, если для них Комиссией не утверждены особые правила признания электронной цифровой

подписи (электронной подписи) в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии.

4. Трансграничное информационное взаимодействие реализуется в соответствии с законодательством государств-членов и правом Союза.

5. Механизм признания электронной цифровой подписи (электронной подписи) (далее – ЭЦП) в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии основывается на реализации задачи легализации (подтверждения подлинности) электронных документов и ЭЦП юридических лиц (хозяйствующих субъектов), выполняемой с использованием службы доверенной третьей стороны в соответствии с настоящими Правилами.

6. В рамках выполнения задачи легализации (подтверждения подлинности) электронных документов и ЭЦП юридических лиц (хозяйствующих субъектов) в фиксированный момент времени доверенные третьи стороны, сервисы которых входят в состав службы доверенной третьей стороны интегрированной информационной системы Союза (далее – интегрированная система), во взаимодействии друг с другом осуществляют для уполномоченных органов государств-членов и Комиссии процедуру проверки ЭЦП юридических лиц (хозяйствующих субъектов) в электронных документах с формированием квитанции доверенной третьей стороны как результата такой проверки (далее – процедура подтверждения подлинности).

7. Электронный документ, подлинность которого подтверждена квитанцией доверенной третьей стороны с положительным результатом проверки, признается в юрисдикции уполномоченного органа государства-члена и Комиссии равнозначным электронному документу, подписанному ЭЦП юридического лица (хозяйствующего субъекта).

8. Обеспечение юридической силы электронного документа при трансграничном информационном взаимодействии доверенных третьих сторон, уполномоченных органов государств-членов и Комиссии с юридическими лицами (хозяйствующими субъектами), а также иных участников процедуры подтверждения подлинности, определенных в разделе II настоящих Правил, осуществляется посредством применения к этим участникам единых требований к созданию, развитию и функционированию трансграничного пространства доверия, утверждаемых Комиссией.

II. Участники процедуры подтверждения подлинности

9. Участниками процедуры подтверждения подлинности являются:

а) юридические лица (хозяйствующие субъекты), представляющие электронные документы уполномоченным органам государств-членов или Комиссии;

б) уполномоченные органы государств-членов и Комиссия, взаимодействующие с юридическими лицами (хозяйствующими субъектами) и заинтересованные в

подтверждении подлинности электронных документов и ЭЦП юридических лиц (хозяйствующих субъектов);

в) элементы трансграничного пространства доверия, входящие в состав государственных компонентов и интеграционного компонента общей инфраструктуры документирования информации в электронном виде, в соответствии с приложением № 1 к Требованиям к созданию, развитию и функционированию трансграничного пространства доверия, утвержденным Решением Совета Евразийской экономической комиссии от 5 декабря 2018 г. № 96 (далее – элементы трансграничного пространства доверия).

III. Общие подходы к реализации процедуры признания ЭЦП в электронном документе и обеспечению юридической силы электронных документов

10. Юридическое лицо (хозяйствующий субъект) (далее – отправитель) представляет уполномоченному органу государства-члена или Комиссии (далее – получатель) электронный документ, подписанный ЭЦП, которая сформирована вне юрисдикции расположения получателя.

11. Получатель формирует и передает запрос на подтверждение подлинности электронного документа в службу доверенной третьей стороны, обращаясь к доверенной третьей стороне, находящейся в том же сегменте интегрированной системы , что и получатель.

Запрос на подтверждение подлинности электронного документа представляет собой структуру данных, в состав которой включаются полученный от отправителя электронный документ, элементы данных, позволяющие идентифицировать отправителя, а также элементы данных, позволяющие доверенным третьим сторонам, входящим в состав службы доверенной третьей стороны, идентифицировать юрисдикцию расположения получателя. Требования к формату и структуре запроса на подтверждение подлинности электронного документа установлены согласно приложению № 1.

12. Доверенные третьи стороны, сервисы которых входят в состав службы доверенной третьей стороны, во взаимодействии друг с другом обеспечивают проверку ЭЦП электронного документа в соответствии с положениями раздела IV настоящих Правил. Результатом проверки ЭЦП является квитанция доверенной третьей стороны, передаваемая получателю доверенной третьей стороной, находящейся в той же юрисдикции, что и получатель. Требования к формату и структуре квитанции доверенной третьей стороны установлены в приложении № 1 к настоящим Правилам.

13. Получатель, руководствуясь сведениями, представленными в квитанции доверенной третьей стороны, передаваемой получателю доверенной третьей стороной, находящейся в той же юрисдикции, что и получатель, либо признает документ в качестве подлинного (если квитанция свидетельствует о положительном результате

проверки ЭЦП) и выполняет его дальнейшую обработку, либо (если квитанция свидетельствует об отрицательном результате проверки ЭЦП) не признает электронный документ подлинным и может прекратить его обработку.

В случае если получатель прекращает обработку электронного документа, он уведомляет об этом отправителя.

14. Требования к электронным документам, подлинность которых подтверждается в рамках осуществления процедуры подтверждения подлинности, установлены согласно приложению № 2.

15. Уполномоченные органы государств-членов информируют Комиссию об удостоверяющих центрах, сертификаты ключа проверки ЭЦП которых могут использоваться в соответствии с настоящими Правилами.

Полный перечень указанных удостоверяющих центров публикуется на информационном портале Союза.

16. При представлении отправителем электронного документа получателю используются механизмы, предусмотренные Концепцией трансграничного информационного взаимодействия, утвержденной Решением Евразийского межправительственного совета от 9 августа 2019 г. № 7.

17. Взаимодействие получателя с доверенной третьей стороной выполняется с использованием интеграционной платформы интегрированной системы 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 (далее – Правила электронного обмена данными). Требования к структуре сообщений, в соответствии с которыми выполняется обмен запросами и квитанциями, установлены согласно приложению № 3.

IV. Правила информационного взаимодействия и обработки данных доверенными третьими сторонами при проверке ЭЦП электронного документа

18. Информационное взаимодействие доверенных третьих сторон выполняется с использованием интеграционной платформы интегрированной системы в соответствии с Правилами электронного обмена данными.

Информационное взаимодействие доверенных третьих сторон выполняется без реализации какого-либо общего процесса в рамках Союза с использованием служебных сообщений интегрированной системы.

Для уведомления об ошибках используются технологические сообщения об ошибках, формируемые и направляемые в соответствии с Правилами электронного обмена данными и требованиями, указанными в приложении № 3 к настоящим Правилам.

19. Доверенная третья сторона, принявшая от получателя запрос на подтверждение подлинности электронного документа (далее – доверенная третья сторона получателя), выполняет его обработку, формирует и передает от своего имени запрос на подтверждение подлинности электронного документа к доверенной третьей стороне, находящейся в той же юрисдикции, что и отправитель (далее – доверенная третья сторона отправителя).

Требования к структуре запроса к доверенной третьей стороне отправителя установлены в приложении № 1 к настоящим Правилам. Требования к структуре сообщения, в соответствии с которыми выполняется передача запроса через интеграционную платформу интегрированной системы, установлены в приложении № 3 к настоящим Правилам.

20. Доверенная третья сторона отправителя, получившая запрос от доверенной третьей стороны получателя, осуществляет следующие действия:

а) выполняет проверку всех ЭЦП электронного документа, указанного в запросе;

б) формирует квитанцию доверенной третьей стороны отправителя, содержащую результаты проверки всех ЭЦП электронного документа, указанного в запросе;

в) передает сформированную квитанцию доверенной третьей стороны отправителя доверенной третьей стороне получателя.

21. Проверка ЭЦП заключается в проверке соблюдения следующих условий в совокупности:

целостность электронного документа, не нарушена, что проверяется путем сравнения хэш-значения электронного документа, вычисленного доверенной третьей стороной, с хэш-значением электронного документа;

ЭЦП сформирована с использованием ключа ЭЦП, соответствующий сертификат ключа проверки ЭЦП которого указан в составе электронного документа;

сертификат ключа проверки ЭЦП действителен на момент подписания электронного документа (срок действия сертификата ключа проверки ЭЦП не истек и этот сертификат не отозван);

каждый сертификат ключа проверки ЭЦП из цепочки сертификатов ключей проверки ЭЦП удостоверяющих центров действителен на момент подписания (срок действия сертификатов ключей проверки ЭЦП удостоверяющих центров не истек и эти сертификаты не отозваны);

сертификат ключа проверки ЭЦП предназначен для проверки ЭЦП электронного документа;

ЭЦП сформирована руководителем юридического лица (хозяйствующего субъекта);

подлинность штампа времени электронного документа (при наличии) проверена.

Доверенная третья сторона отправителя вправе дополнительно проверять ЭЦП отправителя в электронном документе, в том числе в соответствии с требованиями законодательства своего государства-члена.

Проверка каждой ЭЦП выполняется независимо от результатов проверки других ЭЦП электронного документа. Отрицательный результат проверки одной ЭЦП не означает прекращения проверок других ЭЦП электронного документа.

В случае если все указанные условия при проверке всех ЭЦП электронного документа выполняются, подлинность электронного документа считается подтвержденной (положительный результат проверки). Если хотя бы одно из условий для одной ЭЦП не выполняется, подлинность электронного документа считается неподтвержденной (отрицательный результат проверки).

При проверке ЭЦП все указанные проверки осуществляются на дату и время, указанные в штампе времени, при отсутствии штампа времени проверка осуществляется на текущую дату и время.

22. Квитанция доверенной третьей стороны отправителя подписывается ЭЦП, сформированной в соответствии с криптографическими стандартами службы доверенной третьей стороны.

23. Доверенная третья сторона отправителя передает квитанцию доверенной третьей стороне получателя с использованием интеграционной платформы интегрированной системы.

24. Доверенная третья сторона получателя после получения квитанции доверенной третьей стороны отправителя проверяет соблюдение следующих требований в совокупности:

а) хэш-значение электронного документа, вложенного в квитанцию доверенной третьей стороны отправителя, совпадает с хэш-значением электронного документа, отправленного доверенной третьей стороне отправителя доверенной третьей стороной получателя в составе запроса на подтверждение подлинности электронного документа;

б) квитанция подписана ЭЦП доверенной третьей стороны отправителя, сформированной с использованием ключа ЭЦП доверенной третьей стороны отправителя, соответствующий сертификат ключа проверки ЭЦП которого указан в составе этой ЭЦП;

в) сертификат ключа проверки ЭЦП доверенной третьей стороны отправителя издан удостоверяющим центром службы доверенной третьей стороны и действителен на момент подписания квитанции;

г) сертификат ключа проверки ЭЦП удостоверяющего центра службы доверенной третьей стороны действителен на момент подписания квитанции;

д) время формирования квитанции доверенной третьей стороны отправителя, указанное в составе квитанции, отличается от времени получения этой квитанции доверенной третьей стороной получателя не более чем на 4 часа;

е) наименование доверенной третьей стороны получателя, включенное в состав квитанции доверенной третьей стороны отправителя, не отличается от наименования, включенного в состав исходного запроса к доверенной третьей стороне отправителя.

25. По результатам выполненной проверки квитанции доверенной третьей стороны отправителя доверенной третьей стороной получателя формируется квитанция, которая подписывается ЭЦП в соответствии с криптографическим стандартом юрисдикции доверенной третьей стороны получателя. Требования к структуре квитанции доверенной третьей стороны установлены в приложении № 1 к настоящим Правилам.

26. Доверенная третья сторона получателя передает получателю квитанцию с использованием интеграционной платформы интегрированной системы. Требования к структуре сообщения, посредством которого выполняется передача квитанции, установлены в приложении № 3 к настоящим Правилам.

V. Разрешение нештатных ситуаций

27. Нештатной признается ситуация, при которой обработка данных по причине технических сбоев, несоответствия структуры электронных документов, квитанций доверенной третьей стороны или сообщений установленным правилам либо по другим основаниям не может быть произведена согласно положениям настоящих Правил.

28. Разрешением нештатных ситуаций занимаются технические подразделения операторов элементов трансграничного пространства доверия.

29. Для обеспечения оперативного взаимодействия технические подразделения операторов элементов трансграничного пространства доверия должны определить перечень ответственных лиц, участвующих в разрешении нештатных ситуаций.

30. В целях разрешения нештатных ситуаций каждой доверенной третьей стороной ведется журнал аудита, содержащий информацию о приеме, обработке, отправке сообщений и электронных документов, а также о формировании квитанций доверенной третьей стороны.

31. Доверенная третья сторона формирует технологическое сообщение об ошибке в том случае, если при обработке входящего сообщения (запроса на подтверждение подлинности электронного документа или сообщения, содержащего квитанцию доверенной третьей стороны) возникла любая из следующих ошибок:

а) несоответствие формата или структуры сообщения требованиям, установленным в приложении № 3 к настоящим Правилам;

б) несоответствие формата или структуры запроса на подтверждение подлинности электронного документа либо несоответствие квитанции доверенной третьей стороны требованиям, установленным в приложении № 1 к настоящим Правилам;

в) несоответствие формата и структуры электронного документа, вложенного в запрос на подтверждение подлинности, требованиям, установленным в приложении № 2 к настоящим Правилам;

г) невозможность передачи запроса на подтверждение подлинности электронного документа доверенной третьей стороне отправителя в связи с невозможностью определить юрисдикцию доверенной третьей стороны отправителя;

д) время ожидания квитанции доверенной третьей стороны отправителя доверенной третьей стороной получателя превышает 4 часа с момента отправки запроса на подтверждение подлинности электронного документа;

е) иные ошибки, приводящие к невозможности формирования и отправки квитанции доверенной третьей стороны.

32. Формирование технологических сообщений об ошибке осуществляется в соответствии с приложением № 3 к настоящим Правилам.

33. Технологическое сообщение об ошибке с использованием интеграционной платформы интегрированной системы направляется:

а) доверенной третьей стороной получателя – в адрес получателя;

б) доверенной третьей стороной отправителя – в адрес доверенной третьей стороны получателя.

34. Для уведомления получателя о невозможности формирования доверенной третьей стороной отправителя соответствующей квитанции осуществляется передача (ретранслирование) доверенной третьей стороной получателя в адрес получателя технологического сообщения об ошибке, полученного от доверенной третьей стороны отправителя.

35. В случае получения получателем от доверенной третьей стороны получателя технологического сообщения об ошибке, свидетельствующего о превышении времени ожидания квитанции доверенной третьей стороны отправителя, получатель может при необходимости выполнить повторную отправку запроса на подтверждение подлинности электронного документа.

36. Операторами элементов трансграничного пространства доверия должны быть проанализированы все возникшие нештатные ситуации, сформированы выводы о причинах их возникновения и приняты все меры для их устранения и недопущения в дальнейшем.

ПРИЛОЖЕНИЕ № 1
к Правилам признания
электронной цифровой
подписи (электронной
подписи) в электронном документе
и обеспечения юридической
силы электронных
документов при
трансграничном
информационном взаимодействии
юридических лиц
(хозяйствующих субъектов)
с уполномоченными органами
государств – членов
Евразийского экономического
союза и Евразийской

экономической комиссией
с использованием службы
доверенной третьей стороны

ТРЕБОВАНИЯ

к формату и структуре запроса к доверенной третьей стороне и формированию квитанции доверенной третьей стороны

1. Настоящий документ устанавливает требования к формату и структуре данных, которые передаются доверенной третьей стороне в качестве запроса с целью подтверждения подлинности электронных цифровых подписей (электронных подписей) и электронных документов при трансграничном взаимодействии юридических лиц (хозяйствующих субъектов) с уполномоченными органами государств – членов Евразийского экономического союза и Евразийской экономической комиссией (далее – запрос), а также требования к формированию квитанции доверенной третьей стороны.

2. Доверенная третья сторона при приеме запроса должна проверять его соответствие требованиям настоящего документа. В случае нарушения требований настоящего документа обработка запроса должна быть прекращена и участник процедуры подтверждения подлинности, сформировавший запрос, должен быть уведомлен об этом доверенной третьей стороной.

3. Запрос должен передаваться в виде структуры DVCSRequest, определенной стандартом RFC 3029 (Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols, https://datatracker.ietf.org/doc/html/rfc3029).

4. Поля структуры DVCSRequest должны заполняться в соответствии с требованиями стандарта RFC 3029 для реализации сервиса "Validation of Digitally Signed Document (vsd)" с уточнениями, указанными в таблице 1.

Таблица 1

Требования к заполнению полей структуры DVCSRequest

Поле	Требование
requestInformation.version	поле не заполняется
requestInformation.service	заполняется значением "vsd(2)"
requestInformation.nonce	поле не заполняется
requestInformation.requestTime	поле не заполняется
requestInformation.requester	поле заполняется наименованием (идентификатором) органа (организации), сформировавшей запрос уполномоченный орган: требования к заполнению поля определяются на национальном уровне; Комиссия: используется элемент dNSName, который заполняется фиксированным значением "EEC";

	доверенная третья сторона (ДТС) получателя: используется элемент dNSName, который заполняется идентификатором государства – члена Евразийского экономического союза (далее – государство-член) получателя, инициировавшего запрос, в соответствии со стандартом ISO 3166-1 alpha-2
requestInformation.requestPolicy	поле не заполняется
requestInformation.dvcs	используется элемент dNSName, который заполняется идентификатором государства-члена отправителя в соответствии со стандартом ISO 3166 -1 alpha-2; поле используется ДТС получателя для определения того, в какое из государств-членов необходимо перенаправить запрос
requestInformation.dataLocations	поле не заполняется
requestInformation.extensions	поле не заполняется
data	используется элемент message, содержимое которого заполняется CMS-объектом SignedData содержащем электронный документ
transactionIdentifier	поле не заполняется

5. Квитанция должна формироваться в виде структуры DVCSResponse, упакованной и подписанной с использованием объекта SignedData в соответствии со стандартом RFC 3029 (Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols, https://datatracker.ietf.org/doc/html/rfc3029).

6. В состав структуры DVCSResponse, содержащей положительный либо отрицательный результат проверки ЭЦП, должен включаться блок dvCertInfo, поля которого должны заполняться в соответствии с требованиями стандарта RFC 3029 для реализации сервиса "Validation of Digitally Signed Document (vsd)" с уточнениями, указанными в таблице 2.

Таблица 2

Требования к заполнению полей блока dvCertInfo

Поле	Требования по заполнению
version	поле не заполняется
dvReqInfo	блок копируется из запроса DVCSRequest без изменений
serialNumber	поле заполняется уникальным номером квитанции, требования к которому определяются на национальном уровне
messageImprint.digestAlgorithm	заполняется OID-идентификатором алгоритма вычисления хэш-значения согласно приложению № 8 к Положению об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между

	собой и с Евразийской экономической комиссией, утвержденному Решением Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125 (далее – Положение об обмене электронными документами)
messageImprint.digest	поле заполняется значением хэш-значения электронного документа по правилам, определенным стандартом RFC 3029; используемый алгоритм вычисления хэш-суммы должен соответствовать сведениям, указанным в поле dvCertInfo.messageImprint.digestAlgorithm
responseTime	указывается время формирования квитанции; заполняется штампом времени, оформленным согласно стандарту RFC 3161 при формировании штампа времени идентификаторы криптографических стандартов должны указываться в соответствии с приложением № 8 к Положению об обмене электронными документами
policy	требования к заполнению поля определяются на национальном уровне
reqSignature	поле не заполняется

7. В случае критических ошибок, не позволяющих доверенной третьей стороне обработать запрос, а также в случае, если одна из проверок, предусмотренных пунктом 24 Правил признания электронной цифровой подписи (электронной подписи) в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии юридических лиц (хозяйствующих субъектов) с уполномоченными органами государств – членов Евразийского экономического союза и Евразийской экономической комиссией с использованием службы доверенной третьей стороны, утвержденных Решением Коллегии Евразийской экономической комиссии от 22 августа 2023 г. № 120 , закончилась неудачей, в состав структуры DVCSResponse должен включаться блок dvErrorNote, поля которого должны заполняться в соответствии с требованиями стандарта RFC 3029 с уточнениями, указанными в таблице 3.

Таблица 3

Требования к заполнению полей блока dvErrorNote

Поле	Требования по заполнению
transactionStatus.status	поле должно быть заполнено значением "2", что соответствует статусу "Отклонено" ("REJECTED")
transactionStatus.statusString	поле должно содержать человекочитаемое описание уведомления об ошибке
transactionStatus.failInfo	поле заполняется согласно требованиям RFC 3029; на национальном уровне при необходимости могут быть введены дополнительные коды статусов

transactionIdentifier	поле не заполняется

ПРИЛОЖЕНИЕ № 2
к Правилам признания
электронной цифровой
подписи (электронной
подписи) в электронном документе
и обеспечения юридической
силы электронных
документов при
трансграничном
информационном взаимодействии
юридических лиц
(хозяйствующих субъектов)
с уполномоченными органами
государств – членов
Евразийского экономического
союза и Евразийской
экономической комиссией
с использованием службы
доверенной третьей стороны

ТРЕБОВАНИЯ

к электронным документам

1. Настоящий документ устанавливает требования к электронным документам, подтверждение подлинности которых может быть выполнено с использованием службы доверенной третьей стороны в соответствии с Правилами признания электронной цифровой подписи (электронной подписи) в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии юридических лиц (хозяйствующих субъектов) с уполномоченными органами государств – членов Евразийского экономического союза и Евразийской экономической комиссией с использованием службы доверенной третьей стороны, утвержденными Решением Коллегии Евразийской экономической комиссии от 22 августа 2023 г. № 120.

2. К электронному документу предъявляются следующие требования:

а) размер файла с содержимым электронного документа должен соответствовать требованиям, установленным Правилами электронного обмена данными в интегрированной информационной системе внешней и взаимной торговли, утвержденными Решением Коллегии Евразийской экономической комиссии от 27 января 2015 г. № 5;

б) структура электронной цифровой подписи (электронной подписи) (далее – ЭЦП) электронного документа должна соответствовать стандарту RFC 5652 (Cryptographic Message Syntax (CMS) https://datatracker.ietf.org/doc/html/rfc5652) либо стандарту RFC 5126 (CMS Advanced Electronic Signature (CAdES) https://datatracker.ietf.org/doc/rfc5126)

, также допускается использование национальных стандартов государств – членов Евразийского экономического союза, основанных либо адаптированных на базе CMS или CAdES;

в) алгоритмы формирования ЭЦП, а также алгоритмы вычисления хэш-значений, используемых при формировании ЭЦП, определяются согласно приложению № 8 к Положению об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, утвержденному Решением Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125;

г) в состав ЭЦП должен включаться сертификат ключа проверки ЭЦП.

3. Основным форматом подписания электронных документов ЭЦП является CMS. Наравне с основным форматом могут использоваться такие стандарты, как CAdES, PAdES, XAdES, XMLDSIG.

ПРИЛОЖЕНИЕ № 3
к Правилам признания
электронной цифровой
подписи (электронной
подписи) в электронном документе
и обеспечения юридической
силы электронных
документов при
трансграничном
информационном взаимодействии
юридических лиц
(хозяйствующих субъектов)
с уполномоченными органами
государств – членов
Евразийского экономического
союза и Евразийской
экономической комиссией
с использованием службы
доверенной третьей стороны

ТРЕБОВАНИЯ

к структуре и формату сообщений, используемых при взаимодействии с доверенной третьей стороной

1. Настоящий документ содержит требования к структуре и формату сообщений, обмен которыми выполняется в соответствии с Правилами признания электронной цифровой подписи (электронной подписи) в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии юридических лиц (хозяйствующих субъектов) с уполномоченными органами государств – членов Евразийского экономического союза и Евразийской

экономической комиссией с использованием службы доверенной третьей стороны, утвержденными Решением Коллегии Евразийской экономической комиссии от 22 августа 2023 г. № 120 (далее – Правила признания ЭЦП).

2. Сообщения должны формироваться 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 (далее – Правила электронного обмена данными).

Все сообщения относятся к классу служебных сообщений.

3. При описании сообщений используются пространства имен согласно таблице 1.

Таблица 1

Перечень пространств имен документа

Префикс	Идентификатор пространства имен
vsd	urn:EEC:TTP:VSD:v1.0
soap	В соответствии с Правилами электронного обмена данными
wsa	В соответствии с Правилами электронного обмена данными

4. К сообщениям, содержащим запрос к доверенной третьей стороне на подтверждение подлинности электронного документа (далее – входящие сообщения), предъявляются следующие общие требования:

а) элемент заголовка wsa:To должен содержать логический адрес сервиса доверенной третьей стороны, обеспечивающего выполнение процедур, предусмотренных Правилами признания ЭЦП. Для идентификации такого сервиса должен использоваться логический адрес следующего формата:

EAEU://< идентификатор сегмента >/CA/TTP/VSD,

где "<идентификатор сегмента>" – идентификатор сегмента интегрированной информационной системы Евразийского экономического союза, формируемый согласно Правилам электронного обмена данными;

б) элемент заголовка wsa:ReplyTo/wsa:Address должен содержать логический адрес инициатора запроса (уполномоченного органа государства – члена Евразийского экономического союза или доверенной третьей стороны получателя), обеспечивающего обработку ответных сообщений, содержащих квитанцию доверенной третьей стороны;

в) элемент заголовка wsa:Action должен содержать следующее значение: int://SR/TTP/VSD/ForeignSignature/Check;

г) в тело (soap:Body) включается структура запроса к доверенной третьей стороне согласно таблице 2.

Таблица 2

Реквизитный состав структуры запроса к доверенной третьей стороне

Имя реквизита		Описание реквизита	Тип данных	Мн.
1. Запрос (vsd:Request)		оборачивающий элемент запроса	xs:base64Binary	1
	1.1. Содержимое запроса	содержимое запроса в двоичном формате		1

5. В целях оптимизации процесса передачи запроса в двоичном формате содержимое запроса должно передаваться в виде MIME-части, оформленной согласно Правилам электронного обмена данными.

6. В зависимости от результатов обработки входящего сообщения доверенная третья сторона направляет в ответ:

а) ответное сообщение, в котором в тело (soap:Body) включена квитанция доверенной третьей стороны, – в случае штатного выполнения процедур подтверждения подлинности;

б) технологическое сообщение об ошибке – в случае возникновения ошибки обработки сообщения и (или) содержимого запроса.

7. К ответному сообщению предъявляются следующие требования:

а) элемент заголовка wsa:To должен содержать значение элемента wsa:ReplyTo/wsa: Address входящего сообщения;

б) элемент заголовка wsa:From/wsa:Address должен содержать логический адрес сервиса доверенной третьей стороны, обеспечивающего выполнение процедур, предусмотренных Правилами признания ЭЦП; формат адреса приведен в подпункте "а" пункта 4 настоящего документа;

в) элемент заголовка wsa:RelatesTo должен содержать значение элемента wsa: MessageId входящего сообщения;

г) элемент заголовка wsa:Action должен содержать следующее значение: int://SR/ TTP/VSD/Receipt;

д) в тело (soap:Body) включается структура, содержащая квитанцию доверенной третьей стороны, согласно таблице 3.

Таблица 3

Реквизитный состав структуры, содержащей квитанцию доверенной третьей стороны

Имя реквизита		Описание реквизита	Тип данных	Мн.
1. Квитанция (vsd:Receipt)		оборачивающий элемент квитанции	xs:base64Binary	1
	1.1. Содержимое квитанции	содержимое квитанции в двоичном формате		1

8. В целях оптимизации процесса передачи квитанции доверенной третьей стороны в двоичном формате содержимое квитанции должно передаваться в виде MIME-части, оформленной согласно Правилам электронного обмена данными.

9. К технологическому сообщению об ошибке предъявляются следующие требования:

а) элемент заголовка wsa:To должен содержать значение элемента wsa:ReplyTo/wsa:Address входящего сообщения;

б) элемент заголовка wsa:From/wsa:Address должен содержать логический адрес сервиса доверенной третьей стороны, обеспечивающего выполнение процедур, предусмотренных Правилами признания ЭЦП; формат адреса приведен в подпункте "а" пункта 4 настоящего документа;

в) элемент soap:Code/soap:Subcode/soap:Value должен содержать код одной из типовых ошибок, предусмотренных Правилами электронного обмена данными, либо одно из значений, указанных в таблице 4.

Таблица 4

Коды ошибок

Класс ошибки	Код ошибки	Описание и особенности применения
soap:Sender	ttp:InvalidSOAPRequest	структура тела входящего SOAP-сообщения не соответствует установленным требованиям
soap:Sender	ttp: InvalidDVCSRequest	структура запроса DVCSRequest не соответствует установленным требованиям
soap:Sender	ttp: InvalidDocument	структура электронного документа не соответствует установленным требованиям
soap:Sender	ttp:TTPNotFound	доверенная третья сторона не смогла определить юрисдикцию, в которую необходимо отправить запрос
soap:Sender	ttp:Timeout	доверенная третья сторона получателя не получила от доверенной третьей стороны отправителя квитанцию доверенной третьей стороны отправителя в течение времени, установленного Правилами признания ЭЦП;

г) элемент тела сообщения soap:Fault/soap:Detail должен содержать SOAP-конверт вместе с содержимым тела и заголовками входящего сообщения, оформленный в соответствии с Правилами электронного обмена данными.