УТВЕРЖДЕНЫ

Решением Совета
Евразийской экономической комиссии
от 20 г. №

ПРАВИЛА
взаимного признания электронной цифровой подписи (электронной подписи), изготовленной в соответствии с законодательством одного государства – члена Евразийского экономического союза, другим государством-членом для целей государственных (муниципальных) закупок

I. Общие положения

1. Настоящие Правила разработаны в целях обеспечения беспрепятственного доступа поставщиков, зарегистрированных на территории одного государства – члена Евразийского экономического союза (далее – государство-член), принимающих участие в государственных (муниципальных) закупках, проводимых в электронном формате в другом государстве-члене, а также потенциальных поставщиков, принимающих участие в таких закупках (далее – поставщики), путем взаимного признания электронной цифровой подписи (электронной подписи) (далее – ЭЦП), изготовленной в соответствии с законодательством одного государства-члена, другим государством-членом.

2. Для целей настоящих Правил используются понятия, которые означают следующее:

«доверенная третья сторона» – организация, наделенная в соответствии с законодательством государств-членов правом осуществлять деятельность по проверке электронной цифровой подписи (электронной подписи) в электронных документах в фиксированный

момент времени в отношении лица, подписавшего электронный документ;

«закупки на межгосударственном (трансграничном) уровне» – участие потенциальных поставщиков и поставщиков в закупках заказчиков, зарегистрированных в другом государстве-члене;

«квитанция доверенной третьей стороны» – электронный документ, формируемый доверенной третьей стороной и подписанный электронной цифровой подписью (электронной подписью) доверенной третьей стороны, служащий для подтверждения результата проверки подлинности электронного документа и электронной цифровой подписи (электронной подписи) в электронном документе;

«криптографический стандарт» – совокупность технических спецификаций, устанавливающих правила формирования и проверки электронных цифровых подписей (электронных подписей);

«оператор веб-портала» – орган государственной власти, юридическое лицо или осуществляющее предпринимательскую деятельность физическое лицо, которые в соответствии с законодательством государства-члена владеют веб-порталом, необходимыми для его функционирования программно-аппаратными средствами и (или) обеспечивают его функционирование;

«сервис доверенной третьей стороны» – компонент доверенной третьей стороны, реализующий определенную задачу (функцию) доверенной третьей стороны;

«сертификат ключа проверки ЭЦП» – электронный документ, изданный удостоверяющим центром, подписанный закрытым (личным) ключом удостоверяющего центра и содержащий информацию, подтверждающую принадлежность указанного в сертификате открытого ключа определенному участнику обмена электронными документами, и

иную информацию, предусмотренную соответствующими криптографическими стандартами;

«субъекты электронного взаимодействия» – государственные органы, физические или юридические лица, взаимодействующие в рамках отношений, возникающих в процессе составления, отправления, передачи, получения, хранения и использования электронных документов, а также информации в электронном виде;

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

«хэш-значение» – контрольное значение, являющееся автоматизированным результатом применения функции преобразования массива данных в единую бинарную строку, и гарантирующая, что при любом изменении массива данных хэш-значение будет иным, нежели для первоначального массива данных;

«штамп времени» – реквизит электронного документа, удостоверяющий дату и время создания электронного документа;

«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);

«электронный документ» – документ в электронном виде, заверенный электронной цифровой подписью (электронной подписью) и отвечающий требованиям общей инфраструктуры документирования информации в электронном виде.

Иные понятия, используемые в настоящих Правилах, применяются в значениях, определенных международными договорами и актами, составляющими право Евразийского экономического Союза, регулирующими вопросы осуществления закупок.

3. Механизм признания ЭЦП электронного документа в процессе осуществления закупок на межгосударственном (трансграничном) уровне основывается на использовании сервисов доверенных третьих сторон государств-членов, обеспечивающих осуществление легализации (подтверждение подлинности) электронных документов и ЭЦП субъектов электронного взаимодействия и фиксированный момент времени.

4. В рамках осуществления легализации (подтверждение подлинности) электронных документов и ЭЦП субъектов электронного взаимодействия и фиксированный момент времени, доверенные третьи стороны в координации друг с другом осуществляют проверку ЭЦП электронных документов с формированием квитанции доверенной третьей стороны как результата такой проверки (далее – процедура подтверждения подлинности).

5. Электронные документы субъектов электронного взаимодействия, участвующих в процедурах закупок на межгосударственном (трансграничном) уровне, подлинность ЭЦП которых подтверждена квитанцией доверенной третьей стороны с положительным результатом проверки, признаются на территории государства-члена равным по юридической силе аналогичном

документам на бумажном носителе, заверенным подписью либо подписью и печатью, субъекта электронного взаимодействия, участвующего в процедурах закупок на межгосударственном (трансграничном) уровне.

6. В выполнении процедур подтверждения подлинности участвуют доверенные третьи стороны, наделенные в соответствии с законодательством государства-члена правом на осуществление деятельности по проверке ЭЦП электронных документов и соответствующие требованиям законодательства государств-членов в сфере защиты информации и настоящим Правилам.

II. Участники процедуры подтверждения подлинности

7. Участниками процедуры подтверждения подлинности являются:

а) заказчики;

б) поставщики, зарегистрированные на территории одного государства-члена и принимающие участие в закупках, проводимых в другом государстве-члене;

в) операторы веб-порталов;

г) операторы электронных торговых площадок (электронных площадок);

д) удостоверяющие центры;

е) удостоверяющий центр службы доверенной третьей стороны, обеспечивающий предоставление сертификатов ключей проверки ЭЦП доверенным третьим сторонам, уполномоченным на проверку ЭЦП, в том числе в процессах осуществления закупок (далее – удостоверяющий центр службы доверенной третьей стороны);

ж) доверенные третьи стороны;

з) иные субъекты электронного взаимодействия, наделенные

в соответствии с законодательством государства-члена полномочиями на участие в закупках на межгосударственном (трансграничном) уровне, которым необходимо осуществлять проверку ЭЦП электронных документов (далее – иные субъекты электронного взаимодействия).

III. Процедура подтверждения подлинности

8. В процессе осуществления закупок на межгосударственном (трансграничном) уровне заказчики, поставщики, операторы электронных торговых площадок (электронных площадок) и (или) операторы веб-порталов, а также иные субъекты электронного взаимодействия взаимодействуют друг с другом в том числе путем обмена электронными документами, подписанными ЭЦП.

При конкурсных процедурах закупок на межгосударственном (трансграничном) уровне, проводимых на электронной торговой площадке (электронной площадке) или на веб-портале, должны быть обеспечены равные условия применения ЭЦП между потенциальными поставщиками и поставщиками государства-члена, на территории которого находится электронная торговая площадка (электронная площадка) или веб-портал. Для этого применение ЭЦП должно быть ограничено идентификацией и аутентификацией поставщика при его входе на электронную торговую площадку (электронную площадку) или веб-портал при помощи сертификата открытого ключа (сертификата ключа проверки ЭЦП) и подписанием электронных документов, не зависящих от времени их подписания и не ставящих поставщиков в неравные условия, с учетом необходимости подтверждения подлинности ЭЦП при помощи доверенной третьей стороны.

При направлении поставщиком нескольких ценовых предложений в том числе без применения ЭЦП, оператором электронной торговой

площадкой (электронной площадкой) или оператором веб-портала должен фиксироваться факт и время подачи ценового предложения от поставщика в момент его получения электронной торговой площадкой (электронной площадкой) или веб-порталом.

9. Подписание электронных документов поставщиком или иными субъектами электронного взаимодействия осуществляется при помощи средств ЭЦП, соответствующих требованиям национального законодательства поставщика или иных субъектов электронного взаимодействия, при этом порядок подписания электронных документов определяет оператор электронных торговых площадок (электронных площадок) и (или) оператор веб-порталов.

10. В случае представления поставщиком или иными субъектами электронного взаимодействия электронного документа, подписанного ЭЦП, изготовленной с использованием криптографических стандартов и в соответствии с требованиями государства-члена места регистрации поставщика или иных субъектов электронного взаимодействия, оператор электронной торговой площадки (электронной площадки) формирует и передает запрос на проверку ЭЦП электронного документа (далее – инициатор запроса) доверенной третьей стороне своего государства-члена.

~~10.~~ Инициатор запроса направляет запрос на проверку ЭЦП электронного документа доверенной третьей стороне своего государства-члена ~~не позднее 24 часов~~ начиная с момента получения электронного документа, подписанного поставщиком или иными субъектами электронного взаимодействия.

В случаях, предусмотренных законодательством государств-членов, инициатором запроса~~ов~~ к доверенной третьей стороне может выступать оператор веб-портала этого государства-члена.

11. Запрос на проверку ЭЦП электронного документа представляет собой структуру данных, в состав которой включаются электронный документ, ЭЦП для проверки (отдельно или в составе электронного документа), сведения для определения места регистрации субъекта, сформировавшего ЭЦП электронного документа, и идентификации инициатора запроса.

Дополнительно в состав запроса на проверку ЭЦП может быть включено хэш-значение электронного документа, вычисленное в соответствии с законодательством государства-члена места регистрации электронной торговой площадки (электронной площадки).

12. Доверенные третьи стороны во взаимодействии друг с другом обеспечивают проверку ЭЦП электронного документа в соответствии с положениями раздела IV настоящих Правил. Документом, определяющим результат проверки ЭЦП, является квитанция доверенной третьей стороны, передаваемая инициатору запроса доверенной третьей стороной, которой был направлен запрос на проверку ЭЦП электронного документа.

13. Инициатор запроса, руководствуясь сведениями, представленными в квитанции доверенной третьей стороны, признает электронный документ в качестве подлинного (если квитанция доверенной третьей стороны свидетельствует о положительном результате проверки ЭЦП и ее ЭЦП действительна) и выполняет его дальнейшую обработку или не признает электронный документ подлинным (если квитанция доверенной третьей стороны свидетельствует об отрицательном результате проверки ЭЦП и (или) ее ЭЦП недействительна), прекращает его обработку и уведомляет об этом поставщика.

14. Требования к формату и структуре запроса на проверку

ЭЦП, а также требования к формату и структуре квитанции доверенной третьей стороны установлены в приложении № 1.

Формат и структура запроса на проверку ЭЦП, а также формат и структура квитанции доверенной третьей стороны, представленные в приложении № 2, должны быть использованы в случае необходимости альтернативной реализации информационного обмена.

Используемыей для взаимодействия между доверенными третьими сторонами стандарты, определяющиими формат и структуру запроса на проверку ЭЦП электронного документа, передаваемого доверенной третьей стороне, и квитанции доверенной третьей стороны, формируемой доверенной третьей стороной в ответ на запрос на проверку ЭЦП электронного документа, с учетом требований настоящих Правил указывается в соглашении, заключаемом между доверенными третьими сторонами.

15. Требования к формату и структуре электронного документа, подлинность которого подтверждается в рамках осуществления процедуры подтверждения подлинности, установлены в приложении № 3.

16. ~~Правила»~~ Порядок информационного взаимодействия между инициатором запроса и доверенной третьей стороной государства-члена инициатора запроса устанавливаются на национальном уровне.

В целях унификации процесса информационного взаимодействия используются общие требования к структуре, формату и организации обмена сообщениями, установленные приложением № 4.

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

электронного документа

17. Взаимодействие между доверенными третьими сторонами должно осуществляться с использованием защищенных каналов передачи данных, в соответствии с требованиями законодательства государств-членов в сфере защиты информации и заключенными соглашениями между доверенными третьими сторонами.

18. Доверенная третья сторона, принявшая запрос на проверку ЭЦП электронного документа от инициатора запроса (далее – доверенная третья сторона инициатора запроса), выполняет его обработку, в том числе расчет хэш-значения электронного документа с использованием криптографического стандарта функции хэширования ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» (далее – трансграничный алгоритм хэширования), формирует и направляет от своего имени запрос на проверку ЭЦП электронного документа к доверенной третьей стороне государства-члена места регистрации субъекта, сформировавшего ЭЦП электронного документа, подлежащую проверке (далее – доверенная третья сторона проверяемого участника).

19. Доверенная третья сторона проверяемого участника, получившая запрос на проверку ЭЦП электронного документа от доверенной третьей стороны инициатора запроса, осуществляет следующие действия:

а) выполняет проверку ЭЦП электронного документа, переданного в запросе на проверку ЭЦП электронного документа;

б) формирует квитанцию, содержащую результаты проверки ЭЦП электронного документа, переданного в запросе на проверку ЭЦП электронного документа;

в) передает сформированную квитанцию доверенной третьей

стороне инициатора запроса.

20. Проверка ЭЦП электронного документа 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 проверяемого участника, с хэш-значением электронного документа, переданным доверенной третьей стороной инициатора запроса;

ЭЦП сформирована с использованием закрытого (личного) ключа (ключа ЭЦП), соответствующий открытый ключ которого (сертификат ключа проверки ЭЦП) указан в составе этой ЭЦП;

сертификат ключа проверки ЭЦП действителен на момент проверки электронного документа или его подписания при наличии штампа времени;

каждый сертификат ключа проверки ЭЦП из цепочки сертификатов ключей проверки ЭЦП удостоверяющих центров действителен на момент подписания электронного документа при наличии штампа времени или на момент проверки;

сертификат ключа проверки ЭЦП предназначен для проверки ЭЦП электронного документа;

подтверждена действительность штампа времени электронного документа (при наличии).

Доверенная третья сторона проверяемого участника вправе дополнительно осуществлять проверку ЭЦП проверяемого участника государственных (муниципальных) закупок на межгосударственном (трансграничном) уровне в электронном документе, в том числе в соответствии с требованиями законодательства своего государства-члена.

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

Все указанные проверки осуществляются на текущие дату и время проверки ЭЦП электронного документа или на дату и время, указанные в штампе времени при его наличии.

~~Максимальный с~~Срок на проверку~~и~~ ЭЦП электронного документа и подготовки квитанции доверенной третьей стороны ~~не должен превышать 60 секунд с момента отправки запроса на проверку ЭЦПсрок, установленный в заключенных~~устанавливается в соглашениях между доверенными третьими сторонами.

21. Квитанция доверенной третьей стороны проверяемого участника подписывается ЭЦП, сформированной в соответствии со следующими криптографическими стандартами:

а) трансграничный алгоритм хэширования;

б) ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

22. Доверенная третья сторона инициатора запроса после получения квитанции доверенной третьей стороны проверяемого участника проверяет соблюдение следующих требований в совокупности:

а) хэш-значение электронного документа, вычисленное с применением трансграничного алгоритма хэширования, вложенного

в квитанцию доверенной третьей стороны проверяемого участника, совпадает с вычисленным хэш-значением электронного документа, полученного от инициатора запроса в составе запроса на проверку ЭЦП электронного документа;

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

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

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

д) время формирования квитанции доверенной третьей стороны проверяемого участника, указанное в составе квитанции, отличается от времени получения этой квитанции доверенной третьей стороной инициатора запроса не более чем на значение, согласованное между операторами доверенной третьей стороны инициатора и доверенной третьей стороны проверяемого участника;

е) идентификатор запроса на проверку ЭЦП электронного документа, включенный в состав квитанции доверенной третьей стороны проверяемого участника, не отличается от идентификатора исходного запроса к доверенной третьей стороне проверяемого участника на проверку ЭЦП электронного документа.

23. В целях унификации процесса обмена сообщениями между

инициатором запроса, доверенной третьей стороной инициатора запроса, доверенной третьей стороной проверяемого участника, для сообщения, в состав которого включается запрос на проверку ЭЦП электронного документа к доверенной третьей стороне проверяемого участника, и сообщения, в состав которого включается квитанция доверенной третьей стороны проверяемого участника, используются структура и формат, указанные в приложении № 4 к настоящим Правилам.

24. По результатам выполненной проверки квитанции доверенной третьей стороны поверяемого участника доверенной третьей стороной инициатора запроса формируется и передается инициатору запроса квитанция, которая подписывается ЭЦП в соответствии с криптографическим стандартом государства-члена доверенной третьей стороны инициатора запроса.

V. Разрешение нештатных ситуаций

25. Нештатной признается ситуация, при которой обработка данных по причине технических сбоев, несоответствия структур данных, которыми обмениваются участники процедуры подтверждения подлинности.

26. Разрешением нештатных ситуаций занимаются доверенные третьи стороны, операторы электронных торговых площадок (электронных площадок) и (или) операторы веб-порталов, удостоверяющие центры, включая удостоверяющие центры службы доверенной третьей стороны, а также иные субъекты электронного взаимодействия.

27. Для обеспечения оперативного взаимодействия доверенные третьи стороны, операторы электронных торговых площадок (электронных площадок) и (или) операторы

веб-порталов, а также операторы доверенных третьих сторон должны определить перечень ответственных лиц, участвующих в разрешении нештатных ситуаций, а также каналы взаимодействия указанных ответственных лиц.

28. 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 стороной.

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

а) несоответствие формата или структуры сообщений, используемых для передачи запросов на проверку ЭЦП и квитанций доверенной третьей стороны (в случае использования таких сообщений);

б) несоответствие формата или структуры запроса на проверку ЭЦП либо несоответствие квитанции доверенной третьей стороны требованиям, установленным в приложении № 1 (приложении № 2 в случае альтернативной реализации информационного обмена) к настоящим Правилам;

в) невозможность передачи запроса на подтверждение подлинности электронного документа доверенной третьей стороне проверяемого участника в связи с невозможностью определить, какой именно доверенной третьей стороне должен быть передан запрос;

г) время ожидания квитанции доверенной третьей стороны проверяемого участника доверенной третьей стороной инициатора запроса превышает срок, установленный в заключенных соглашениях

между доверенными третьими сторонами~~60 секунд с момента отправки запроса~~

~~на проверку ЭЦП электронного документа~~;

д) иные технологические ошибки, приводящие к невозможности обработки запроса на проверку ЭЦП электронного документа либо формирования и отправки квитанции доверенной третьей стороны.

30. Формирование технологических сообщений об ошибках выполняется в соответствии с приложением № 4 к настоящим Правилам.

31. Технологическое сообщение об ошибке направляется:

а) доверенной третьей стороной инициатора запроса – в адрес инициатора запроса;

б) доверенной третьей стороной проверяемого участника – в адрес доверенной третьей стороны инициатора запроса.

32. При получении доверенной третьей стороной инициатора запроса технологического сообщения об ошибке от доверенной третьей стороны проверяемого участника доверенная третья сторона инициатора запроса должна уведомить инициатора запроса о невозможности получения им квитанции доверенной третьей стороны. В указанном уведомлении указывается причина возникшей нештатной ситуации.

33. Операторами электронных торговых площадок (электронных площадок) и (или) операторами веб-порталов, доверенными третьими сторонами должны быть проанализированы все возникшие нештатные ситуации, сформированы выводы о причинах их возникновения и приняты необходимые меры для их устранения и недопущения в дальнейшем.

ПРИЛОЖЕНИЕ № 1

к Правилам взаимного признания
электронной цифровой подписи
(электронной подписи), изготовленной
в соответствии с законодательством
одного государства – члена Евразийского
экономического союза, другим
государством-членом для целей
государственных (муниципальных)
закупок

ТРЕБОВАНИЯ

к формату и структуре запроса на проверку электронной цифровой подписи (электронной подписи) электронного документа, формату и структуре квитанции доверенной третьей стороны в соответствии со стандартом RFC 3029

1. Настоящие требования устанавливают единые требования к формату и структуре запроса на проверку электронной цифровой подписи (электронной подписи) (далее – ЭЦП) электронного документа, передаваемого доверенной третьей стороне, а также единые требования к формату и структуре квитанции доверенной третьей стороны, формируемой доверенной третьей стороной в ответ на запрос на проверку ЭЦП электронного документа.

2. Запрос на проверку ЭЦП электронного документа 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).

3. 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. Элементы DVCSRequest в соответствии со стандартом RFC 3029, не указанные в таблице 1, не должны заполняться

при формировании запроса на проверку ЭЦП электронного документа к доверенной третьей стороне.

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	сведения, идентифицирующие инициатора запроса на проверку ЭЦП электронного документа: требования к заполнению поля определяются на национальном уровне
requestInformation.requestPolicy	поле заполняется идентификатором urn:EEC:TTP:VSD:ETP:1.0
requestInformation.dvcs	код страны в соответствии с ISO 3166-1 alpha-2, в которой были выпущены ЭЦП для проверки поле используется доверенной третьей стороной инициатора запроса для определения того, в какое из государств-членов необходимо перенаправить запрос
requestInformation.dataLocations	поле не заполняется
requestInformation.extensions.MimeType	тип документа в соответствии со стандартом Multipurpose Internet Mail Extensions (https://datatracker.ietf.org/doc/html/rfc5322) поле заполняется следующими значениями в соответствии с типом документа: – для XML - "application/xml" – для бинарных документов - "application/octet-stream"
requestInformation.extensions.XPathDS	XPath-путь в передаваемом XML-документе, по которому расположена ЭЦП Не заполняется в случае прикрепленной в передаваемом электронном документе ЭЦП в двоичном формате
requestInformation.extensions.DocumentHash	необязательный блок для передачи хэш-значения электронного документа, вычисленного

	в соответствии с законодательством государства-члена инициатора запроса
requestInformation.extensions.DocumentHash.Transforms	необязательный блок, состоящий из последовательности Transform (1.. unbounded) блок для передачи перечня преобразований, которые были применены к XML-документу, переданному для проверки ЭЦП, до формирования хэш-значения Не заполняется в случае расчета хэш-значения для докумнета в двоичном формате
requestInformation.extensions.DocumentHash.Transforms.Transform	оборачивающий блок трансформации
requestInformation.extensions.DocumentHash.Transforms.Transform.Algorithm	поле для указания идентификатора алгоритма преобразования XML-документа
requestInformation.extensions.DocumentHash.Transforms.Transform.XPath	необязательное поле для указания XPath выражения преобразования XML-документа
requestInformation.extensions.DocumentHash.Algorithm	заполняется OID-идентификатором алгоритма вычисления хэш-значения электронного документа
requestInformation.extensions.DocumentHash.DigestValue	заполняется хэш-значением электронного документа, вычисленным в соответствии с законодательством государства-члена инициатора запроса
data	используется элемент message, содержимое которого заполняется: – CMS-объектом SignedData, содержащим электронный документ в двоичном формате; – электронным документов в формате языка разметки eXtensible Markup Language (XML), закодированный в виде base64.
transactionIdentifier	статистически уникальный 128-битный идентификатор запроса на проверку ЭЦП электронного документа (GUID)

4. В запросе на проверку ЭЦП электронного документа может быть передан только 1 электронный документ.

5. Не допускается передача запроса на проверку ЭЦП электронного документа, подписанного с использованием криптографических

стандартов разных государств-членов Евразийского экономического союза (далее – государства-члены).

В случае проверки электронного документа, имеющего в своем составе 2 и более ЭЦП, сформированные с использованием криптографических стандартов разных государств-членов, необходимо сформировать отдельные запросы на проверку ЭЦП электронного документа для каждой ЭЦП.

6. В запросе на проверку ЭЦП электронного документа DVCSRequest в блоке data может быть передан либо электронный документ в формате XML, закодированный в виде base64, либо CMS-объект SignedData, содержащий электронный документ в двоичном формате.

– для передачи электронного документа в формате XML дополнительно заполняется поле XPath блока requestInformation.extensions;

7. Передаваемая в запросе на проверку ЭЦП электронного документа в блоке data должна формироваться с учетом требований Правил взаимного признания электронной цифровой подписи (электронной подписи), изготовленной в соответствии с законодательством одного государства – члена Евразийского экономического союза, другим государством-членом для целей государственных (муниципальных) закупок, утверждаемых Решением Совета Евразийской экономической комиссии (далее соответственно – закупки, Правила).

8. 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.

9. 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

Структура квитанции доверенной третьей стороны

Поле	Требования по заполнению
version	поле не заполняется
dvReqInfo	блок копируется из запроса DVCSRequest без изменений
serialNumber	статистически уникальный 128-битный идентификатор (GUID), указанный в запросе на проверку ЭЦП электронного документа
messageImprint.digestAlgorithm	заполняется OID-идентификатором алгоритма вычисления хэш-значения электронного документа
messageImprint.digest	поле заполняется хэш-значением электронного документа, переданного для проверки ЭЦП при передаче в запросе объекта SignedData проверка должна быть выполнена по правилам, определенным стандартом RFC 3029; используемый алгоритм вычисления хэш-значения 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 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)
policy	поле заполняется идентификатором urn:EEC:TTP:VSD:ETP:1.0
reqSignature	поле не заполняется

10. В квитанции доверенной третьей стороны в блоке messageImprint.digest передается хэш-значение электронного документа, переданного для проверки ЭЦП.

При формировании квитанции доверенной третьей стороны для инициатора запроса хэш-значение вычисляется с использованием криптографического стандарта государства-члена инициатора запроса.

При формировании квитанции доверенной третьей стороны для доверенной третьей стороны хэш-значение электронного документа вычисляется с использованием трансграничного алгоритма хэширования в соответствии с приложением № 8 к Положению об обмене электронными документами.

Идентификатор алгоритма хэширования, используемого для вычисления хэш-значения электронного документа, передается в поле messageImprint.digestAlgorithm.

11. Формирование штампа времени (поле responseTime) для квитанции доверенной третьей стороны проверяемого участника выполняется с использованием сервиса штампа времени удостоверяющего центра службы доверенной третьей стороны.

Формирование штампа времени для квитанции доверенной третьей стороны инициатора запроса выполняется с использованием сервиса штампа времени государства-члена.

В случае недоступности сервиса штампа времени удостоверяющего центра службы доверенной третьей стороны должен использоваться автономный сервис штампа времени доверенной третьей стороны проверяемого участника с формированием штампа времени при помощи криптографических стандартов ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» и ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

12. В случае критических ошибок, не позволяющих доверенной третьей стороне обработать запрос, а также в случае, если одна из проверок, предусмотренных пунктом 19 Правил 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	статистически уникальный 128-битный

идентификатор (GUID), указанный в запросе на проверку ЭЦП электронного документа

ПРИЛОЖЕНИЕ № 2

к Правилам взаимного признания электронной цифровой подписи (электронной подписи), изготовленной в соответствии с законодательством одного государства – члена Евразийского экономического союза, другим государством-членом для целей государственных (муниципальных) закупок

ТРЕБОВАНИЯ
к формату и структуре запроса на проверку электронной цифровой подписи (электронной подписи) электронного документа, формату и структуре квитанции доверенной третьей стороны в соответствии со стандартом OASIS DSS

1. Настоящее приложение устанавливает единые требования к формату и структуре запроса на проверку электронной цифровой подписи (электронной подписи) (далее – ЭЦП) электронного документа, передаваемого доверенной третьей стороне, а также единые требования к формату и структуре квитанции доверенной третьей стороны, формируемой доверенной третьей стороной в ответ на запрос на проверку ЭЦП электронного документа.

2. Запрос на проверку ЭЦП электронного документа должен передаваться в виде структуры VerifyRequest, определенной стандартом OASIS DSS (OASIS Digital Signature Service Version 1.0 http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html). Поля структуры VerifyRequest должны заполняться в соответствии с требованиями стандарта OASIS DSS для реализации протокола проверки ЭЦП (verifying protocol) с уточнениями, указанными в таблице 1. Элементы VerifyRequest в соответствии со стандартом OASIS DSS, не указанные

в таблице 1, не должны заполняться при формировании запроса на проверку ЭЦП электронного документа к доверенной третьей стороне.

Таблица 1

Структура запроса на проверку ЭЦП электронного документа

Элемент	Тип данных	Описание	Кратность
VerifyRequest	xs:extension base=”dss:RequestBaseType”	оборачивающий элемент запроса на проверку ЭЦП электронного документа	1
@RequestID	xs:string	статистически уникальный 128-битный идентификатор запроса на проверку ЭЦП электронного документа (GUID)	1
@Profile	xs:anyURI	идентификатор профиля DSS: urn:EEC:TTP:DSS:1.0:verify:1.0	1
dss:OptionalInputs	dss:AnyType	блок дополнительных данных запроса на проверку ЭЦП электронного документа	1
ttp:CountryName	xs:string	элемент, указывающий код страны в соответствии с ISO 3166-1 alpha-2, в которой были выпущены ЭЦП для проверки	1
ttp:Requester	xs:string	сведения, идентифицирующие инициатора запроса на проверку ЭЦП электронного документа: требования к заполнению поля определяются на национальном уровне	1
dss:DocumentHash	xs:extension base="dss:DocumentBaseType"	хэш-значение электронного документа, переданного для проверки ЭЦП, вычисленная в соответствии с законодательством государства-члена инициатора запроса	0..1
ds:Transforms	ds:TransformType	перечень преобразований, которые доверенная третья	0..1

Элемент	Тип данных	Описание	Кратность
		сторона применила к электронному документу, переданного для проверки ЭЦП, до формирования хэш-значения	
ds:DigestMethod	ds:DigestMethodType	описание алгоритма хэширования	1
@Algorithm	anyURI	URI алгоритма хэширования в соответствии с законодательством государства-члена инициатора запроса	1
ds:DigestValue	ds:DigestValueType	хэш-значение электронного документа, переданного для проверки ЭЦП	1
dss:InputDocuments	-	электронный документ, передаваемый в запросе, для проверки ЭЦП. В запросе на проверку ЭЦП электронного документа передается только один электронный документ для проверки ЭЦП	1
dss:Document	dss:DocumentType	элемент содержит электронный документ, а также сведения, необходимые для выполнения проверок ЭЦП	1
@ID	xs:ID	уникальный в рамках запроса на проверку ЭЦП электронного документа идентификатор электронного документа. Указывается в случае, если передаваемый в запросе документ содержит в своем составе ЭЦП	0..1
-	составной тип (xs:choice)		
Base64XML	xs:base64Binary	электронный документ в формате языка разметки eXtensible Markup Language (XML), закодированный в виде base64	1

Элемент	Тип данных	Описание	Кратность
dss:Base64Data	xs:extension base=”xs:base64Binary”	электронный документ в двоичном формате, закодированный в виде base64	1
@MimeType	xs:string	описание типа документа в двоичном формате в соответствии со стандартом Multipurpose Internet Mail Extensions (https://datatracker.ietf.org/doc/html/rfc5322)	0..1
-	xs:base64Binary	данные, закодированные base64	1
dss:SignatureObject	ds:SignatureMethodType	оборачивающий элемент ЭЦП	1
-	составной тип (xs:choice)		
ds:Signature	ds:SignatureType	ЭЦП и сертификат ключа проверки ЭЦП	1
dss:Base64Signature	xs:extension base="xs:base64Binary"	элемент для передачи открепленной ЭЦП в двоичном формате	1
@Type	xs:anyURI	идентификатор типа ЭЦП в двоичном формате в соответствии с таблицей 3	1
-	xs:base64Binary	данные, закодированные в формате base64	1
dss:SignaturePtr		блок для указания ЭЦП для проверки Заполняется, если ЭЦП для проверки вложена в электронный документ, передаваемый в запросе на проверку ЭЦП электронного документа	1
@WhichDocument	xs:IDREF	идентификатор электронного документа, в который вложена ЭЦП для проверки, соответствующий атрибуту //dss:Document@ID запроса на проверку ЭЦП электронного документа	1
@XPath	xs:string	XPath-путь в передаваемом XML-документе, по которому расположена ЭЦП	0..1

Элемент	Тип данных	Описание	Кратность
		Не заполняется в случае прикрепленной в передаваемом электронном документе ЭЦП в двоичном формате	

3. При формировании запроса на проверку ЭЦП электронного документа и квитанции доверенной третьей стороны используются пространства имен, перечень которых приведен в таблице 2.

Таблица 2

Перечень пространств имен документа

Префикс	Адрес
dss	urn:oasis:names:tc:dss:1.0:core:schema
ds	http://www.w3.org/2000/09/xmldsig#
xades	http://uri.etsi.org/01903/v1.3.2#
xs	http://www.w3.org/2001/XMLSchema
ttp	urn:EEC:TTP:DSS:1.0

4. В запросе на проверку ЭЦП электронного документа может быть передан только 1 электронный документ.

5. Не допускается передача запроса на проверку ЭЦП электронного документа, подписанного с использованием криптографических стандартов разных государств-членов Евразийского экономического союза (далее – государства-члены).

В случае проверки электронного документа, имеющего в своем составе 2 и более ЭЦП, сформированные с использованием криптографических стандартов разных государств-членов, необходимо

сформировать отдельные запросы на проверку ЭЦП электронного документа для каждой ЭЦП.

Таблица 3

Идентификаторы типа ЭЦП в двоичном формате

Наименование	URI
CMS-подпись	urn:ietf:rfc:5652
CAdES-подпись	urn:ietf:rfc:5126

6. В запросе на проверку ЭЦП электронного документа в блоке VerifyRequest/dss:Document/dss:InputDocuments/ может быть передан либо электронный документ в формате XML, либо электронный документ в двоичном формате.

– для передачи электронного документа в формате XML заполняется элемент VerifyRequest/dss:Document/dss: InputDocuments/ Base64XML;

– для передачи электронного документа в двоичном формате заполняется блок VerifyRequest/dss:Document/ dss:InputDocuments/dss: Base64Data.

7. Передаваемые в запросе на проверку ЭЦП электронного документа в блоках VerifyRequest/dss:SignatureObject/ds:Signature и VerifyRequest/dss:SignatureObject/dss:Base64Signature ЭЦП должны формироваться с учетом требований Правил взаимного признания электронной цифровой подписи (электронной подписи), изготовленной в соответствии с законодательством одного государства – члена Евразийского экономического союза, другим государством-членом для целей государственных (муниципальных) закупок, утверждаемых

Решением Совета Евразийской экономической комиссии (далее соответственно – закупки, Правила).

8. Квитанция доверенной третьей стороны представляет собой электронный XML-документ в формате OASIS DSS (структура VerifyResponse) с уточнениями, указанными в таблице 4. Элементы структуры VerifyResponse в соответствии со стандартом OASIS DSS, не указанные в таблице 4, не должны заполняться при формировании квитанции доверенной третьей стороны.

Таблица 4

Структура квитанции доверенной третьей стороны

Элемент	Тип данных	Описание	Кратность
VerifyResponse	dss:ResponseBaseType	оборачивающий элемент квитанции доверенной третьей стороны	1
@RequestID	xs:string	статистически уникальный 128-битный идентификатор (GUID), указанный в запросе на проверку ЭЦП электронного документа	1
@Profile	xs:anyURI	идентификатор профиля DSS: urn:EEC:TTP:DSS:1.0:verify:1.0	1
dss:Result	-	элемент содержащий сведения о результатах проверки ЭЦП	1
ResultMajor	xs:anyURI	элемент с основными сведениями о проведенных проверках в соответствии с таблицей 6	1
ResultMinor	xs:anyURI	элемент с дополнительными сведениями о проведенных проверках в	1

Элемент	Тип данных	Описание	Кратность
		соответствии с таблицей 7	
ResultMessage	dss:InternationalStringType	элемент, содержащий дополнительное текстовое описание о произведенных проверках или возникших ошибках. Случаи, когда данный элемент должен быть заполнен, приведены в таблице 7. Дополнительно должен заполняться при передаче сведений при тестировании, испытаниях, а также в иных случаях по решению участников	0..1
dss:OptionalOutputs	dss:AnyType		
ds:X509Data	ds:X509DataType	сертификат открытого ключа проверки ЭЦП электронного документа, переданного для проверки ЭЦП Не заполняется в случае формирования квитанции с отрицательным результатом проверки ЭЦП если сертификат открытого ключа отсутствовал в запросе	0..1
dss:DocumentHash	xs:extension base="dss:DocumentBaseType"	хэш-значение электронного документа, переданного для проверки ЭЦП Не заполняется в случае формирования квитанции с отрицательным результатом проверки ЭЦП, если	0..1

Элемент	Тип данных	Описание	Кратность
		электронный документ отсутствовал в запросе	
ds:Transforms	ds:TransformType	перечень преобразований, которые доверенная третья сторона применила к электронному документу, переданного для проверки ЭЦП, до формирования хэш-значения Заполняется в случае формирования квитанции доверенной третьей стороны для электронного документа в формате языка разметки XML	0..1
ds:DigestMethod	ds:DigestMethodType	описание алгоритма хэширования	1
@Algorithm	anyURI	URI алгоритма хэширования: Указывается 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	1

Элемент	Тип данных	Описание	Кратность
		обмене электронными документами)	
ds:DigestValue	ds:DigestValueType	хэш-значение электронного документа, переданного для проверки ЭЦП	1
ttp:SignatureTTP	dss:InlineXMLType	блок для передачи квитанции доверенной третьей стороны проверяемого участника, заполняется только при формировании квитанции доверенной третьей стороной для инициатора запроса	0..1
ttp:ValidationTimeStamp	xades:EncapsulatedPKIDataType	штамп времени поверки ЭЦП, оформленный согласно стандарту протокола штампов времени RFC 3161 При формировании квитанции доверенной третьей стороны используется штамп времени, полученный от сервиса проверки ЭЦП При формировании квитанции доверенной третьей стороны для инициатора запроса используется штамп времени, переданный в квитанции доверенной третьей стороны проверяемого участника	0..1
ttp:Responder	xs:string	сведения, идентифицирующие доверенную третью сторону: требования к заполнению поля	1

Элемент	Тип данных	Описание	Кратность
		определяются на национальном уровне	
ds:Signature	ds:SignatureType	оборачивающий элемент блока ЭЦП квитанции	1
ds:SignedInfo	ds:SignedInfoType	оборачивающий элемент блока подписанных данных	1
ds:CanonicalizationMethod	ds:CanonicalizationMethodType	оборачивающий элемент алгоритма каноникализации XML	1
@Algorithm	xs:anyURI	указывается идентификатор алгоритма каноникализации XML http://www.w3.org/2001/10/xml-exc-c14n#	1
ds:SignatureMethod	ds:SignatureMethodType	оборачивающий элемент алгоритма формирования ЭЦП	1
@Algorithm	xs:anyURI	атрибут-идентификатор алгоритма формирования ЭЦП. Указывается согласно приложению № 8 к Положению об обмене электронными документами	1
ds:Reference	ds:ReferenceType	оборачивающий элемент для ссылки на подписываемый блок основных реквизитов квитанции	1
@URI	xs:anyURI	атрибут, идентифицирующий блок ds:Reference в качестве ссылки на блок основных реквизитов квитанции. Заполняется значением «urn:EEC:TTP:v1.0:verify:response»	1
ds:Transforms	ds:TransformsType	оборачивающий элемент перечня трансформаций	1

Элемент	Тип данных	Описание	Кратность
ds:Transform	ds:TransformType	оборачивающий элемент трансформации	1
@Algorithm	xs:anyURI	указывается идентификатор алгоритма каноникализации XML http://www.w3.org/2001/10/xml-exc-c14n#	1
ds:Transform	ds:TransformType	оборачивающий элемент трансформации	1
@Algorithm	xs:anyURI	указывается идентификатор алгоритма исключения блока подписи из квитанции http://www.w3.org/2000/09/xmldsig#enveloped-signature	1
ds:DigestMethod	ds:DigestMethodType	оборачивающий элемент алгоритма хэширования	1
@Algorithm	xs:anyURI	При формировании квитанции доверенной третьей стороны для инициатора запроса указывается URI алгоритма хэширования государства-члена инициатора запроса При формировании квитанции доверенной третьей стороной для доверенной третьей стороны указывается URI алгоритма хэширования в соответствии с приложениемN 8 к Положению об обмене электронными документами	1
ds:DigestValue	ds:DigestValueType	хэш-значение блока основных реквизитов квитанции после	1

Элемент	Тип данных	Описание	Кратность
		проведения каноникализации XML	
ds:Reference	ds:ReferenceType	оборачивающий элемент ссылки на блок дополнительных реквизитов квитанции в формате XAdES	1
@URI	xs:anyURI	атрибут-ссылка на XML-элемент блока дополнительных реквизитов квитанции в формате XAdES, приведенных в таблице 5, заполняется значением «http://uri.etsi.org/01903#SignedProperties»	1
ds:Transforms	ds:TransformsType	оборачивающий элемент перечня трансформаций	1
ds:Transform	ds:TransformType	оборачивающий элемент трансформации	1
@Algorithm	xs:anyURI	указывается идентификатор алгоритма каноникализации XML http://www.w3.org/2001/10/xml-exc-c14n#	1
ds:DigestMethod	ds:DigestMethodType	оборачивающий элемент алгоритма хэширования	1
@Algorithm	xs:anyURI	При формировании квитанции доверенной третьей стороны для инициатора запроса указывается URI алгоритма хэширования государства-члена инициатора запроса При формировании квитанции доверенной третьей стороной для доверенной третьей стороны указывается URI алгоритма хэширования в	1

Элемент	Тип данных	Описание	Кратность
		соответствии с приложениемN 8 к Положению об обмене электронными документами	
ds:DigestValue	ds:DigestValueType	хэш-значение блока дополнительных реквизитов квитанции в формате XAdES после проведения каноникализации XML	1
ds:SignatureValue	ds:SignatureValueType	значение ЭЦП, рассчитанное для элемента ds:SignedInfo квитанции после проведения каноникализации XML	1
ds:KeyInfo	ds:KeyInfoType	оборачивающий элемент ключевой информации, использованной при формировании ЭЦП	1
ds:X509Data	ds:X509DataType	оборачивающий элемент сертификата ключа проверки ЭЦП доверенной третьей стороны	1
ds:X509Certificate	xs:base64Binary	сертификат ключа проверки ЭЦП доверенной третьей стороны	1
ds:Object	ds:ObjectType	оборачивающий элемент дополнительных блоков данных	1
xades:QualifyingProperties	xades:QualifyingPropertiesType	блок дополнительных реквизитов квитанции в формате XAdES. Описание блока приведено в таблице 5	1

Таблица 5

Структура блока дополнительных реквизитов квитанции в формате XAdES

Элемент	Тип данных	Описание	Кратность
xades:QualifyingProperties	xades:QualifyingPropertiesType	оборачивающий элемент блока дополнительных реквизитов квитанции в формате XAdES	1
xades:SignedProperties	xades:SignedPropertiesType	блок подписываемых свойств квитанции	1
xades:SignedSignaturePropertiesType	xades:SignedSignaturePropertiesType	оборачивающий элемент	1
xades: SigningTime	xsd:dateTime	элемент указания времени формирования ЭЦП, не должен значительно отличаться от времени в блоке xades:SignatureTimeStamp	1
xades:SigningCertificate	xades:CertIDListType	оборачивающий элемент сведений об использованном сертификате открытого ключа проверки ЭЦП доверенной третьей стороны	1
xades:Cert	xades:CertIDType	оборачивающий элемент сведений об используемом сертификате ключа проверки ЭЦП доверенной третьей стороны	1
xades:CertDigest	xades:DigestAlgAndValueType	оборачивающий элемент хэш-значения использованного сертификата ключа проверки ЭЦП доверенной третьей стороны	1
ds:DigestMethod	ds:DigestMethodType	оборачивающий элемент алгоритма хэширования	1
@Algorithm	xs:anyURI	URI алгоритма хэширования:	1

Элемент	Тип данных	Описание	Кратность
		При формировании квитанции для инициатора запроса, указывается URI алгоритма хэширования государства-члена инициатора запроса При формировании квитанции доверенной третьей стороны для ДТС указывается URI алгоритма хэширования согласно приложению № 8 к Положению об обмене электронными документами	
ds:DigestValue	ds:DigestValueType	хэш-значение сертификата ключа проверки ЭЦП доверенной третьей стороны	1
ds:IssuerSerial	ds:X509IssuerSerialType	оборачивающий элемент	1
ds:X509IssuerName	xs:string	наименование удостоверяющего центра, выпустившего сертификат открытого ключа проверки ЭЦП доверенной третьей стороны (поле Issuer заполняется согласно стандарту X.509)	1
ds:X509SerialNumber	xs:integer	серийный номер сертификата открытого ключа проверки ЭЦП доверенной третьей стороны, SerialNumber заполняется согласно стандарту X.509	1
xades:UnsignedProperties	xades:UnsignedPropertiesType	блок неподписываемых свойств квитанции, содержащий штамп времени	1
xades:UnsignedSignatureProperties	xades:UnsignedSignaturePropertiesType	блок неподписываемых свойств ЭЦП, содержащий штамп времени	1

Элемент	Тип данных	Описание	Кратность
xades:SignatureTimeStamp	xades:XAdESTimeStampType	оборачивающий элемент для штампа времени	1
ds:CanonicalizationMethod	ds:CanonicalizationMethodType	указывается идентификатор алгоритма каноникализации XML http://www.w3.org/2001/10/xml-exc-c14n#	1
xades:EncapsulatedTimeStamp	xades:EncapsulatedPKIDataType	штамп времени, оформленный согласно стандарту протокола штампов времени RFC 3161. Правила формирования штампа времени приведены в пункте 11 настоящих требований.	1

9. В квитанции доверенной третьей стороны в блоке VerifyResponse/dss:OptionalOutputs/dss:DocumentHash/ds:DigestValue передается хэш-значение электронного документа, переданного для проверки ЭЦП.

При формировании квитанции доверенной третьей стороны для инициатора запроса хэш-значение вычисляется с использованием криптографического стандарта государства-члена инициатора запроса.

При формировании квитанции доверенной третьей стороны для доверенной третьей стороны хэш-значение электронного документа вычисляется с использованием трансграничного алгоритма хэширования в соответствии с приложением № 8 к Положению об обмене электронными документами.

Идентификатор алгоритма хэширования, используемого для вычисления хэш-значения электронного документа, передается

в атрибуте VerifyResponse/dss:OptionalOutputs/dss:DocumentHash/ds:DigestMethod@Algorithm.

10. Идентификаторы алгоритмов формирования ЭЦП и вычисления хэш-значений, используемые при формировании запроса на проверку ЭЦП электронного документа, а также квитанции доверенной третьей стороны, определяются согласно приложению № 8 к Положению об обмене электронными документами.

11. Формирование штампа времени (элемент xades:EncapsulatedTimeStamp) для квитанции доверенной третьей стороны проверяемого участника выполняется с использованием сервиса штампа времени удостоверяющего центра службы доверенной третьей стороны.

Формирование штампа времени для квитанции доверенной третьей стороны инициатора запроса выполняется с использованием сервиса штампа времени государства-члена.

В случае недоступности сервиса штампа времени удостоверяющего центра службы доверенной третьей стороны должен использоваться автономный сервис штампа времени доверенной третьей стороны проверяемого участника с формированием штампа времени при помощи криптографических стандартов ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» и ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

12. Порядок проверки ЭЦП квитанции доверенной третьей стороны должен осуществляться в соответствии со стандартом Signature Syntax and Processing (XMLDsig, https://www.w3.org/TR/xmldsig-core1) с учетом следующих особенностей:

– подлинность ЭЦП квитанции доверенной третьей стороны подтверждается в соответствии с порядком, указанным в разделе 3.2 «Core Validation» стандарта XMLDsig, на основании значения блока .//ds:Signature/SignatureValue и расчётного значения для блока .//ds:Signature/ds:SignedInfo, с использованием сертификата ключа проверки ЭЦП, передаваемого в блоке .//ds:Signature/ds:SignedInfo/ds:KeyInfo/ds:X509Data/ds:X509Certificate;

– сертификат ключа проверки ЭЦП доверенной третьей стороны проверяемого участника, передаваемый в блоке .//ds:Signature/ds:SignedInfo/ds:KeyInfo/ds:X509Data/ds:X509Certificate, должен быть издан удостоверяющим центром службы доверенной третьей стороны и действителен на момент подписания квитанции доверенной третьей стороны проверяемого участника;

– сертификат ключа проверки ЭЦП доверенной третьей стороны инициатора запроса, передаваемый в блоке .//ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate, должен быть издан уполномоченным удостоверяющим центром государства-члена и действителен на момент подписания квитанции доверенной третьей стороны инициатора запроса;

– блок .//ds:Signature/ds:Objectxades:QualifyingProperties/xades:SignedProperties, соответствующий формату XAdES и заполняемый в соответствии с Таблицей 5, должен учитываться при выполнении проверки ЭЦП квитанции доверенной третьей стороны;

13. Порядок проверки блока .//ds:Signature/ds:Objectxades:QualifyingProperties/xades:SignedProperties дополнительной информации ЭЦП квитанции доверенной третьей стороны в формате XAdES должен осуществляться в соответствии с положениями стандарта XML Advanced Electronic Signatures (https://www.w3.org/TR/XAdES) с учетом следующих особенностей:

– штамп времени квитанции доверенной третьей стороны, передаваемый в блоке .//ds:Signature/ds:Objectxades:QualifyingProperties/ xades:UnsignedProperties/xades:SignatureTimeStamp/xades:EncapsulatedTi meStamp (далее – штамп времени квитанции доверенной третьей стороны), должен быть сформирован в соответствии со стандартом протокола штампов времени Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP, RFC 3161, https://www.ietf.org/rfc/rfc3161.txt);

– поле «messageImprint» штампа времени квитанции доверенной третьей стороны проверяемого участника формируется использованием трансграничного алгоритма хэширования в соответствии с приложением № 8 к Положению об обмене электронными документами;

– время подписания квитанции доверенной третьей стороны, указанное в блоке xades: SigningTime, не должно значительно отличаться от времени генерации в поле «genTime» штампа времени квитанции доверенной третьей стороны;

– хэш-значение сертификата ключа доверенной третьей стороны, указанная в блоке .//xades:SignedSignatureProperties/xades:SigningCertific ate/xades:Cert/xades:CertDigest/ds:DigestValue должна совпадать с хэш-значением, рассчитанным для сертификата ключа, передаваемого в ЭЦП квитанции доверенной третьей стороны в блоке.//ds: Signature /ds:SignedInfo/ds:KeyInfo/ds:X509Data/ds:X509Certificate, по алгоритму.//xades:SignedSignatureProperties/xades:SigningCertificate/xade s:Cert/xades:CertDigest/ds:DigestMethod[@Attribute='Algorithm'];

– наименование удостоверяющего центра, выпустившего сертификат ключа проверки ЭЦП доверенной третьей стороны и серийный номер сертификата ключа доверенной третьей стороны, передаваемые в блоках .//xades:SignedSignatureProperties/xades:Signing Certificate/xades:Cert/ds:IssuerSerial/ds:X509IssuerName и .//xades:Signed

SignatureProperties/xades:SigningCertificate/xades:Cert/ds:IssuerSerial/ds: X509SerialNumber, должны совпадать со значениями соответствующих полей сертификата ключа проверки ЭЦП доверенной третьей стороны проверяемого участника, передаваемый в блоке .//ds:Signature/ds: SignedInfo/ds:KeyInfo/ds:X509Data/ds:X509Certificate;

– подлинность штампа времени квитанции доверенной третьей стороны подтверждена на основании переданного в штампе времени значения ЭЦП и рассчитанного хэш-значения для квитанции доверенной третьей стороны на основании порядка, определенного стандартом Cryptographic Message Syntax (CMS, RFC 5652, https://datatracker.ietf. org/doc/html/rfc5652).

Таблица 6

Основные сведения о проведенной проверке

Статус проверки	URI
Процедура проверки ЭЦП выполнена	urn:oasis:names:tc:dss:1.0:resultmajor:Success
Процедура проверки ЭЦП не выполнена в связи с ошибкой в запросе на проверку ЭЦП электронного документа	urn:oasis:names:tc:dss:1.0:resultmajor:RequesterError
Процедура проверки ЭЦП не выполнена в связи с ошибкой на стороне ДТС	urn:oasis:names:tc:dss:1.0:resultmajor:ResponderError
Процедура проверки ЭЦП не выполнена в связи с отсутствием данных от сторонних источников	urn:oasis:names:tc:dss:1.0:resultmajor:InsufficientInformation

Таблица 7

Дополнительные сведения о проведенной проверке

Основной ответ	Статус проверки	URI
Процедура подтверждения подлинности ЭЦП выполнена (Success)	Подлинность ЭЦП и штамп времени (при наличии) подтверждена	urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:OnAllDocuments
	Подлинность ЭЦП не подтверждена	urn:oasis:names:tc:dss:1.0:resultminor:invalid:IncorrectSignature
	Подлинность ЭЦП подтверждена, но не подтверждена подлинность штампа времени ЭЦП	urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:InvalidSignatureTimestamp
Процедура подтверждения подлинности ЭЦП не выполнена в связи с ошибкой в запросе на проверку ЭЦП электронного документа (RequesterError)	Электронный документ, указанный в ds:Reference блока ds:Signature, отсутствует в запросе на проверку ЭЦП электронного документа	urn:oasis:names:tc:dss:1.0:resultminor:ReferencedDocumentNotPresent
	Сведения о сертификате проверки ЭЦП, ожидаемые сервером, отсутствуют в запросе на проверку ЭЦП электронного документа	urn:oasis:names:tc:dss:1.0:resultminor:KeyInfoNotProvided
	Сервер не смог обработать передаваемый электронный документ	urn:oasis:names:tc:dss:1.0:resultminor:NotParseableXMLDocument
	Сервер не смог обработать запрос, так как составе передаваемого	urn:oasis:names:tc:dss:1.0:resultminor:NotSupported

Основной ответ	Статус проверки	URI
	электронного документа не найдена ЭЦП	
	ЭЦП или ее содержимое не соответствуют криптографическому стандарту (стандартам) используемым ДТС, указанному в запросе на проверку ЭЦП электронного документа	urn:oasis:names:tc:dss:1.0:result minor:Inappropriate:signature
Процедура подтверждения подлинности ЭЦП не выполнена в связи с ошибкой на стороне ДТС (ResponderError)	Обработка запроса не удалась из-за ошибки, не указанной в существующих кодах ошибок. Более подробные сведения должны быть указаны в элементе dss:ResultMessage	urn:oasis:names:tc:dss:1.0:result minor:GeneralError
	Не удалось найти данные по сертификату проверки ЭЦП на стороне ДТС	urn:oasis:names:tc:dss:1.0:result minor:invalid:KeyLookupFailed
Процедура подтверждения подлинности ЭЦП не выполнена в связи с отсутствием данных от сторонних источников (InsufficientInformation)	Список отозванных сертификатов был недоступен для проверки	urn:oasis:names:tc:dss:1.0:result minor:CrlNotAvailiable
	Сведения об отзыве сертификата проверки ЭЦП были недоступны через протокол Online Certificate Status Protocol	urn:oasis:names:tc:dss:1.0:result minor:OcspNotAvailiable
	Не удалось установить цепочку доверия, связывающую сертификат проверки ЭЦП с доверенным корневым центром сертификации через потенциальные промежуточные центры сертификации.	urn:oasis:names:tc:dss:1.0:result minor:CertificateChainNotComplete

ПРИЛОЖЕНИЕ № 3

к Правилам взаимного признания
электронной цифровой подписи
(электронной подписи), изготовленной
в соответствии с законодательством
одного государства-члена Евразийского
экономического союза, другим
государством-членом для целей
государственных (муниципальных)
закупок

ТРЕБОВАНИЯ
к формату и структуре электронного документа

1. Настоящие требования устанавливают унифицированные требования к формату и структуре электронного документа, проверка электронной цифровой подписи (электронной подписи) (далее – ЭЦП) которого может быть выполнена с использованием доверенной третьей стороны согласно Правилам взаимного признания электронной цифровой подписи (электронной подписи), изготовленной в соответствии с законодательством одного государства – члена Евразийского экономического союза, другим государством-членом для целей государственных (муниципальных) закупок, утверждаемым Решением Совета Евразийской экономической комиссии № .

2. Электронный документ должен быть сформирован в следующих форматах:

а) формате языка разметки eXtensible Markup Language (XML) версии 1.0;

б) двоичном формате.

3. Требования к структуре и наполнению содержимого электронных документов определяются в соответствии с правом Евразийского

экономического союза, законодательством государств – членов Евразийского экономического союза.

4. Формат ЭЦП электронного документа, ее атрибуты и элементы должны соответствовать одному из перечисленных стандартов в зависимости от типа ЭЦП:

ЭЦП в формате XML: Signature Syntax and Processing (XMLDsig, https://www.w3.org/TR/xmldsig-core1), XML Advanced Electronic Signatures (XAdES, XAdES-T, https://www.w3.org/TR/XAdES);

ЭЦП в двоичном формате: Cryptographic Message Syntax (CMS, RFC 5652, https://datatracker.ietf.org/doc/html/rfc5652), CMS Advanced Electronic Signatures (CADES-BES, CADES-EPES, CADES-T, RFC 5126, https://datatracker.ietf.org/doc/html/rfc5126).

Применение расширений указанных стандартов при формировании ЭЦП не допускается.

5. К XML-подписи электронного документа предъявляются следующие требования:

а) в составе электронного документа может присутствовать несколько блоков Signature в случае подписания электронного документа более одной ЭЦП;

б) в состав элемента ds:Signature должен включаться атрибут ds:Signature/@Id, содержащий идентификатор ЭЦП, значение которого уникально в пределах электронного документа;

в) ЭЦП, передаваемые в блоках Signature, должны подписывать только данные, содержащиеся в электронном документе. Для элементов ds:Reference допускаются только ссылки типа «same-document reference» стандарта XMLDsig (раздел 4.3.3.3 стандарта). Ссылки на внешние по отношению к электронному документу данные не допускаются;

г) ссылки на блоки данных, для которых формируются хэш-значения, в составе ЭЦП должны формироваться по правилам стандарта XML Path Language (XML Path Language (XPath) Version 1.0. W3C Recommendation 16 November 1999 http://www.w3.org/TR/xpath);

д) в составе ds:Signature не допускается формирование следующих элементов: ds:Manifest, CounterSignature, CompleteCertificateRefs, CompleteRevocationRefs, SigAndRefsTimeStamp, RefsOnlyTimeStamp, CertificatesValues, RevocationValues;

е) в состав элемента ds:Signature должен включаться сертификат открытого ключа проверки ЭЦП в соответствии с требованиями стандарта XMLDsig.

6. К ЭЦП в двоичном формате электронного документа предъявляются следующие требования:

а) допускается использование как отсоединенной («detached signature» («external signature»)), так и присоединенной («attached signature») ЭЦП;

б) в случае формирования CMS-контейнера присоединенной ЭЦП значение ЭЦП и содержимое электронного документа должны находиться в одном контейнере. Не допускается исключение компонента eContent из элемента EncapsulatedContentInfo CMS-контейнера;

в) в состав CMS-контейнера должен включаться сертификат открытого ключа проверки ЭЦП в соответствии с требованиями стандарта RFC 3852;

г) в составе блока unsignedAttrs не допускается формирование элементов: Countersignature, complete-Icertificate-references, complete-revocation-references;

д) в составе блока signedAttrs не допускается формирование элементов: content-reference, content-identifier.

ПРИЛОЖЕНИЕ № 4

к Правилам взаимного признания электронной цифровой подписи (электронной подписи), изготовленной в соответствии с законодательством одного государства-члена Евразийского экономического союза, другим государством-членом для целей государственных (муниципальных) закупок

УНИФИЦИРОВАННЫЕ ТРЕБОВАНИЯ
к структуре, формату и организации обмена сообщениями при взаимодействии с доверенной третьей стороной

1. Настоящий документ содержит требования к структуре, формату и организации обмена сообщениями при взаимодействии с доверенной третьей стороной.

2. Для целей подтверждения права инициатора запроса на получение услуги по проверке электронной цифровой подписи (электронной подписи) электронного документа, а также для недопущения передачи персональных и конфиденциальных данных третьим лицам и исключения потенциальных угроз информационной безопасности участникам информационного взаимодействия выполнятся взаимная аутентификация на транспортном уровне перед осуществлением обмена сообщениями при помощи протокола защиты транспортного уровня (The Transport Layer Security, TLS, https://datatracker.ietf.org/doc/html/rfc5246).

Требования по выбору криптографических стандартов, применяемых при аутентификации инициатора запроса и доверенной третьей стороны, определяются на уровне государства-члена.

При реализации информационного взаимодействия между доверенными третьими сторонами государств-членов применяется трансграничный алгоритм хэширования и трансграничный алгоритм ЭЦП.

3. Для обеспечения доставки данных от одного участника информационного взаимодействия до другого, на транспортном уровне применяется протокол HyperText Transfer Protocol Secure (HTTPS, https://datatracker.ietf.org/doc/html/rfc2818) с учетом рекомендаций стандарта RFC 3029 (Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols, https://datatracker.ietf.org/doc/html/rfc3029), а также стандарта OASIS DSS (OASIS Digital Signature Service Version 1.0, http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html, если стандарт OASIS DSS выбран в качестве альтернативной реализации информационного обмена в дополнение к RFC 3029. ~~указаний раздела 6.1 стандарта OASIS DSS (OASIS Digital Signature Service Version 1.0, http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html#_Toc159076096).~~

4. Электронный обмен данными между участниками на технологическом уровне организовывается посредством сообщений в формате SOAP 1.2 (Simple Object Access Protocol, http://www.w3.org/TR/soap12-part1) с учетом ~~указаний~~ рекомендаций стандарта RFC 3029 (Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols, https://datatracker.ietf.org/doc/html/rfc3029), а также стандарта OASIS DSS (OASIS Digital Signature Service Version 1.0, http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html, –если стандарт OASIS

DSS выбран в качестве альтернативной реализации информационного обмена в дополнение к RFC 3029.

~~раздела 6.2 стандарта OASIS DSS (OASIS Digital Signature Service Version 1.0, http://does.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html#_Toc159076096).~~

5. Технологическое сообщение об ошибке оформляется в виде SOAP-сообщения Fault.

6. Коды типовых ошибок к использованию при формировании технологического сообщения об ошибке, указаны в таблице 8.

Таблица 8

Коды типовых ошибок

Класс ошибки	Код ошибки*	Описание и особенности применения
Sender	ttp:NotImplemented	сервер не поддерживает возможностей, необходимых для обработки запроса. Ошибка возвращается, при получении запроса в соответствии со стандартом, отличным от указанного в соглашении между участниками информационного обмена
Sender	ttp:InvalidSOAP	структура тела принятого SOAP-сообщения не соответствует установленным требованиям
Sender	ttp:InvalidRequest	структура запроса на проверку ЭЦП не соответствует установленным требованиям, вследствие чего запрос не может быть обработан
Sender, Receiver	ttp:InvalidReceipt	структура квитанции доверенной третьей стороны не соответствует установленным требованиям, вследствие чего квитанция не может быть обработана
Sender	ttp:TTPNotFound	запрос на подтверждение подлинности электронного документа доверенной третьей стороне проверяемого участника не передан в связи с невозможностью определить – какой именно доверенной третьей стороне должен быть передан запрос

Класс ошибки	Код ошибки*	Описание и особенности применения
Receiver	ttp:Timeout	время ожидания квитанции доверенной третьей стороны проверяемого участника доверенной третьей стороной инициатора запроса превысило установленное время
Receiver	ttp:GeneralError	иная технологическая ошибка, приводящая к невозможности обработки запроса на проверку ЭЦП либо формирования и отправки квитанции доверенной третьей стороны; указанный код используется в случае, если ошибка не описана в спецификации SOAP или настоящей таблице

* преффиксу «ttp» соответствует пространство имен:
– «urn:EEC:TTP:VSD:ETP:1.0» при осуществлении обмена по стандарту DVCS;
– «urn:EEC:TTP:DSS:1.0» при осуществлении обмена по стандарту OASIS DSS.