УТВЕРЖДЕНЫ

Решением Совета
Евразийской экономической комиссии
от 20 г. №

П Р А В И Л А
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:

«закупки на межгосударственном (трансграничном) уровне» – закупки, осуществляемые заказчиками, зарегистрированными в одном государстве-члене, с участием поставщиков (поставщика), зарегистрированных в других государствах-членах;

«оператор веб-портала» – орган государственной власти, юридическое лицо, которые в соответствии с законодательством государства-члена обеспечивают функционирование веб-портала;

«сервис доверенной третьей стороны» – компоненты доверенной третьей стороны, обеспечивающие выполнение определенной задачи (функции) доверенной третьей стороны;

«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;

«электронный документ» – документ в электронном виде, подписанный ЭЦП.

Иные понятия, используемые в настоящих Правилах, применяются в значениях, определенных международными договорами и актами, составляющими право Евразийского экономического союза.

3. Механизм признания ЭЦП при осуществлении закупок на межгосударственном (трансграничном) уровне основывается на использовании сервисов доверенных третьих сторон государств-членов, обеспечивающих легализацию (подтверждение подлинности (действительности)) ЭЦП субъектов электронного взаимодействия в фиксированный момент времени.

4. В рамках осуществления легализации (подтверждения подлинности (действительности)) ЭЦП доверенные третьи стороны во взаимодействии друг с другом осуществляют проверку ЭЦП с формированием квитанции доверенной третьей стороны как результата такой проверки (далее – процедура подтверждения подлинности (действительности)).

5. ЭЦП, которыми подписаны электронные документы для целей закупок на межгосударственном (трансграничном) уровне, взаимно признаются в государствах-членах, если подлинность (действительность) ЭЦП подтверждена квитанцией доверенной третьей стороны с положительным результатом проверки, а также соответственно взаимно признаются такие электронные документы.

6. Участниками процедуры подтверждения подлинности (действительности) являются:

а) заказчики;

б) поставщики;

в) операторы веб-порталов;

г) операторы электронных торговых площадок (электронных площадок) (далее – электронные торговые площадки);

д) удостоверяющие центры;

е) доверенные третьи стороны, наделенные в соответствии с законодательством государств-членов правом на осуществление деятельности по проверке ЭЦП и соответствующие требованиям законодательства государств-членов и настоящих Правил;

ж) удостоверяющий центр службы доверенной третьей стороны, обеспечивающий предоставление сертификатов ключей проверки ЭЦП и сервисов для проверки актуальности выданных сертификатов доверенным третьим сторонам, уполномоченным на проверку ЭЦП, в том числе в процессе осуществления закупок (далее – удостоверяющий центр службы доверенной третьей стороны);

з) гарант (в соответствии с Соглашением о взаимном признании банковских гарантий при осуществлении государственных (муниципальных) закупок от 29 августа 2023 года);

и) орган (организация) государства-члена, уполномоченный на ведение реестра банковских гарантий в порядке, установленном государством-членом.

II. Процедура подтверждения подлинности (действительности)

7. При осуществлении закупок на межгосударственном (трансграничном) уровне, проводимых на электронной торговой площадке или веб-портале одного государства-члена, потенциальные поставщики и (или) поставщики другого государства-члена формируют электронные документы на такой электронной торговой площадке или веб-портале и подписывают их ЭЦП.

Сканированные копии иных документов, предоставляемые потенциальными поставщиками и (или) поставщиками и являющиеся составной частью сформированного и подписанного ими на электронной торговой площадке или веб-портале электронного документа, предоставляются посредством функционала электронной торговой площадки или веб-портала.

8. При осуществлении закупок на межгосударственном (трансграничном) уровне, проводимых на электронной торговой площадке или веб-портале, поставщикам должны быть обеспечены равные условия применения ЭЦП. Для этого применение ЭЦП должно быть ограничено идентификацией и аутентификацией поставщика при его входе на электронную торговую 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 (действительности) ЭЦП при помощи доверенной третьей стороны.

В случае направления потенциальным поставщиком нескольких предложений о цене договора (контракта), в том числе без применения ЭЦП, оператором электронной торговой площадки или оператором веб-портала должны фиксироваться факт и время подачи каждого такого предложения в момент его получения.

9. В случае представления поставщиком электронного документа, подписанного ЭЦП, изготовленной с использованием криптографических стандартов и в соответствии с требованиями законодательства государства места регистрации поставщика, оператор электронной торговой площадки формирует и передает запрос на проверку ЭЦП (далее – инициатор запроса) доверенной третьей стороне своего государства-члена в момент получения такого электронного документа.

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

10. Запрос на проверку ЭЦП 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, и идентификации инициатора запроса.

Дополнительно в состав запроса на проверку ЭЦП может быть включен хэш электронного документа, вычисленный в соответствии с законодательством государства места регистрации электронной торговой площадки.

11. Доверенные третьи стороны во взаимодействии друг с другом обеспечивают проверку ЭЦП в соответствии с положениями раздела III 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.

12. Инициатор запроса, руководствуясь сведениями, представленными в квитанции доверенной третьей стороны, признает электронный документ в качестве подлинного (действительного) (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 (действительным) (если квитанция доверенной третьей стороны свидетельствует об отрицательном результате проверки ЭЦП и (или) ее ЭЦП недействительна), прекращает его обработку и уведомляет об этом участников процедуры подтверждения подлинности (действительности), указанных в подпунктах «а», «б» и «и» пункта 6 настоящих Правил.

13. Электронное взаимодействие между доверенными третьими сторонами осуществляется в соответствии с требованиями к формату и структуре запроса на проверку ЭЦП, а также с требованиями к формату и структуре квитанции доверенной третьей стороны, определенными согласно приложению № 1 (основной вариант) или приложению № 2 (рекомендательный вариант).

При взаимодействии доверенных третьих сторон между собой применяются требования к структуре, формату и организации обмена сообщениями согласно приложению № 3.

Используемые для взаимодействия между доверенными третьими сторонами стандарты, определяющие формат и структуру запроса на проверку ЭЦП, передаваемого доверенной третьей стороне, и квитанции доверенной третьей стороны, формируемой доверенной

третьей стороной в ответ на запрос на проверку ЭЦП, с учетом требований настоящих Правил указываются в соглашении, заключаемом между доверенными третьими сторонами.

14. Порядок электронного взаимодействия между инициатором запроса и доверенной третьей стороной государства инициатора запроса устанавливается на национальном уровне.

III. Правила электронного взаимодействия и обработки данных доверенными третьими сторонами при проверке ЭЦП

15. 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.

16. Доверенная третья сторона, получившая запрос на проверку ЭЦП от инициатора запроса (далее – доверенная третья сторона инициатора запроса), выполняет его обработку, в том числе вычисление хэша электронного документа с использованием криптографического стандарта функции хэширования, указанного в пункте 2 приложения № 1 (пункте 8 приложения № 2 в случае реализации рекомендательного варианта электронного взаимодействия) к настоящим Правилам, формирует и направляет от своего имени запрос на проверку ЭЦП к доверенной третьей стороне государства места регистрации субъекта, сформировавшего ЭЦП, подлежащую проверке (далее – доверенная третья сторона проверяемого участника).

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

а) выполняет проверку ЭЦП в электронном документе, переданном в запросе на проверку ЭЦП;

б) формирует квитанцию, содержащую результаты проверки ЭЦП в электронном документе, переданном в запросе на проверку ЭЦП;

в) передает сформированную квитанцию доверенной третьей стороне инициатора запроса.

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

целостность электронного документа не нарушена, что проверяется путем сравнения хэша электронного документа, вычисленного доверенной третьей стороной проверяемого участника, с хэшем электронного документа, переданного доверенной третьей стороной инициатора запроса;

ЭЦП сформирована с использованием ключа ЭЦП, соответствующий ключ проверки ЭЦП указан в сертификате ключа проверки ЭЦП, входящем в состав 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;

подтверждена действительность штампа времени электронного документа (при наличии).

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

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

Срок проверки ЭЦП и подготовки квитанции доверенной третьей стороны не должен превышать 60 секунд.

19. Квитанция доверенной третьей стороны проверяемого участника подписывается ЭЦП, сформированной в соответствии с криптографическими стандартами, указанными в пункте 2 приложения № 1 (пункте 8 приложения № 2 в случае реализации рекомендательного варианта электронного взаимодействия) к настоящим Правилам.

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

а) хэш электронного документа, вычисленный с применением криптографического стандарта функции хэширования, указанного в пункте 2 приложения № 1 (пункте 8 приложения № 2 в случае реализации рекомендательного варианта электронного взаимодействия) к настоящим Правилам, вложенного в квитанцию доверенной третьей стороны проверяемого участника, совпадает

с вычисленным хэшем электронного документа, полученного от инициатора запроса в составе запроса на проверку ЭЦП;

б) квитанция доверенной третьей стороны проверяемого участника подписана ЭЦП, сформированной с использованием закрытого (личного) 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 оператором доверенной третьей стороны инициатора запроса и оператором доверенной третьей стороны проверяемого участника;

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

21. В целях унификации процесса электронного взаимодействия для сообщения, в состав которого включается запрос на проверку ЭЦП или квитанция доверенной третьей стороны

проверяемого участника, используются структура и формат, указанные в приложении № 3 к настоящим Правилам.

22. По результатам 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 доверенной третьей стороны инициатора запроса.

IV. Разрешение нештатных ситуаций

23. Нештатной признается ситуация, при которой обработка данных, которыми обмениваются участники процедуры подтверждения подлинности (действительности), не может быть произведена согласно положениям настоящих Правил по причине технических сбоев или несоответствия структур данных.

24. Разрешением нештатных ситуаций занимаются доверенные третьи стороны, операторы электронных торговых площадок и (или) операторы веб-порталов, удостоверяющие центры, включая удостоверяющий центр службы доверенной третьей стороны.

25. Для обеспечения оперативного взаимодействия доверенные третьи стороны, операторы электронных торговых площадок и (или) операторы веб-порталов, а также операторы доверенных третьих сторон должны определить ответственных лиц, участвующих в разрешении нештатных ситуаций, и каналы взаимодействия указанных ответственных лиц.

26. Каждой доверенной третьей стороной ведется журнал аудита, содержащий следующую информацию о приеме, обработке, отправке

запросов, ответов и электронных документов, а также о формировании квитанций доверенной третьей стороной:

а) идентификатор сессии связи;

б) идентификатор запроса (ответа);

в) данные о пользователе или системе, инициировавшей передачу запроса или ответа;

г) дата и время приемки, обработки запроса и передачи ответа;

д) статус обработки запроса (ответа);

е) хэш электронного документа, переданного в запросе (ответе);

ж) код ошибки при получении или обработке запроса (ответа);

з) иные сведения в соответствии с соглашением между доверенными третьими сторонами.

27. Доверенная третья сторона формирует технологическое сообщение об ошибке в 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, определенным приложением № 1 (приложением № 2 – в случае реализации рекомендательного варианта электронного взаимодействия) 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 соглашениях между доверенными третьими сторонами;

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

28. Формирование технологических сообщений об ошибках выполняется в соответствии с приложением № 3 к настоящим Правилам.

29. 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.

30. Доверенная третья сторона инициатора запроса при получении технологического сообщения об ошибке от доверенной третьей стороны проверяемого участника должна уведомить инициатора запроса о невозможности получения им квитанции доверенной третьей стороны с указанием причины возникшей ошибки.

31. Субъект электронного взаимодействия при получении технологического сообщения об ошибке, связанной с нештатной ситуацией:

а) информирует инициатора запроса о поступлении технологического сообщения об ошибке;

б) при необходимости запрашивает у субъекта электронного взаимодействия, направившего технологическое сообщение об ошибке, дополнительную информацию об ошибке;

в) принимает необходимые действия для устранения ошибки на своей стороне, а также для предотвращения возникновения ошибок в будущем;

г) устранив ошибку, направляет повторно сообщение-запрос или сообщение-ответ.

_____

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

Т Р Е Б О В А Н И Я
к формату и структуре запроса на проверку электронной цифровой подписи (электронной подписи) в электронном документе, 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) в электронном документе, направляемого в доверенную третью сторону, а также единые требования к формату и структуре квитанции доверенной третьей стороны, формируемой доверенной третьей стороной в ответ на запрос на проверку ЭЦП в электронном документе.

2. Вычисление хэша электронного документа доверенной третьей стороной проверяемого участника и формирование ЭЦП, которой подписывается квитанция доверенной третьей стороны проверяемого участника, осуществляются в соответствии со следующими криптографическими стандартами:

а) ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

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

3. Запрос на проверку ЭЦП в электронном документе 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. Элементы DVCSRequest в соответствии со стандартом RFC 3029, не указанные в таблице 1, не должны заполняться при формировании запроса на проверку ЭЦП в электронном документе 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 в электронном документе: 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

Поле	Требование
	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 хэша электронного документа, вычисленного в соответствии с законодательством государства 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 в нем ЭЦП, до вычисления хэша. Не заполняется в случае вычисления хэша для документа 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 криптографического стандарта функции хэширования, применяемого для вычисления хэша электронного документа

Поле	Требование
requestInformation.extensions.DocumentHash.DigestValue	в поле указывается хэш электронного документа, вычисленный в соответствии с законодательством государства 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 в электронном документе (GUID)

5. В запросе на проверку ЭЦП в электронном документе может быть передан только 1 электронный документ.

6. В запросе на проверку ЭЦП в электронном документе 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. 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.

8. В состав структуры DVCSResponse, содержащей положительный либо отрицательный результат проверки ЭЦП в электронном документе,

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 в электронном документе
messageImprint.digestAlgorithm	заполняется OID-идентификатором криптографического стандарта функции хэширования, применяемого для вычисления хэша электронного документа
messageImprint.digest	в поле указывается хэш электронного документа, переданного для проверки в нем ЭЦП, при передаче в запросе объекта SignedData проверка должна быть выполнена по правилам, определенным стандартом RFC 3029; используемый криптографический стандарт функции хэширования должен соответствовать сведениям, указанным в поле dvCertInfo.messageImprint.digestAlgorithm
responseTime	указывается время формирования квитанции; при формировании квитанции доверенной третьей стороны проверяемого участника заполняется поле genTime; при формировании квитанции доверенной третьей стороны инициатора запроса заполняется поле timeStampToken с использованием штампа времени, оформленного согласно стандарту RFC 3161
dvStatus	поле не заполняется

Поле	Требования по заполнению
policy	поле заполняется идентификатором urn:EEC:TTP:VSD:ETP:1.0
reqSignature	поле не заполняется

9. В квитанции доверенной третьей стороны в блоке messageImprint.digest передается хэш электронного документа, переданного для проверки в нем ЭЦП.

При формировании квитанции доверенной третьей стороны инициатора запроса хэш электронного документа вычисляется с использованием криптографического стандарта функции хэширования государства инициатора запроса.

При формировании квитанции доверенной третьей стороны проверяемого участника хэш электронного документа вычисляется с использованием криптографического стандарта функции хэширования в соответствии с пунктом 2 настоящих Требований.

Идентификатор криптографического стандарта функции хэширования, применяемого для вычисления хэша электронного документа, передается в поле messageImprint.digestAlgorithm.

10. Формирование штампа времени (поле responseTime) для квитанции доверенной третьей стороны инициатора запроса выполняется с использованием сервиса штампа времени государства-члена инициатора запроса.

11. В случае критических ошибок, не позволяющих доверенной третьей стороне обработать запрос на проверку ЭЦП в электронном документе, а также в случае, если одна из проверок, предусмотренных пунктом 18 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 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 в электронном документе.

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

Т Р Е Б О В А Н И Я
к формату и структуре запроса на проверку электронной цифровой подписи (электронной подписи) в электронном документе, формату и структуре квитанции доверенной третьей стороны в соответствии со стандартом OASIS DSS

1. Настоящие Требования устанавливают единые требования к формату и структуре запроса на проверку электронной цифровой подписи (электронной подписи) (далее – ЭЦП) в электронном документе, направляемого в доверенную третью сторону, а также единые требования к формату и структуре квитанции доверенной третьей стороны, формируемой доверенной третьей стороной в ответ на запрос на проверку ЭЦП в электронном документе.

2. Запрос на проверку ЭЦП в электронном документе 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 в электронном документе (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 в электронном документе к доверенной третьей стороне.

Таблица 1

Структура запроса на проверку ЭЦП в электронном документе

Элемент	Тип данных	Описание	Кратность
VerifyRequest	xs:extension base=”dss:RequestBaseType”	оборачивающий элемент запроса на проверку ЭЦП в электронном документе	1
@RequestID	xs:string	статистически уникальный 128-битный идентификатор запроса на проверку ЭЦП в электронном документе (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 в электронном документе	1
ttp:CountryName	xs:string	элемент, указывающий код страны в соответствии с ISO 3166-1 alpha-2, в которой были выпущены ЭЦП в электронном документе для проверки	1
ttp:Requester	xs:string	сведения, идентифицирующие инициатора запроса на проверку ЭЦП в электронном документе: требования к заполнению поля определяются на национальном уровне	1
dss:DocumentHash	xs:extension base="dss:DocumentBaseType"	оборачивающий элемент для указания хэша электронного документа, переданного для проверки в нем ЭЦП, вычисленного в соответствии с законодательством	0..1

Элемент	Тип данных	Описание	Кратность
		государства-члена инициатора запроса	
ds:Transforms	ds:TransformType	перечень преобразований, которые доверенная третья сторона применила к электронному документу, переданного для проверки в нем ЭЦП, до формирования хэша электронного документа	0..1
ds:DigestMethod	ds:DigestMethodType	оборачивающий элемент криптографического стандарта функции хэширования	1
@Algorithm	anyURI	URI криптографического стандарта функции хэширования в соответствии с законодательством государства-члена инициатора запроса	1
ds:DigestValue	ds:DigestValueType	хэш электронного документа, переданного для проверки в нем ЭЦП	1
dss:InputDocuments	-	электронный документ, передаваемый в запросе, для проверки в нем ЭЦП. В запросе на проверку ЭЦП в электронном документе передается только один электронный документ для проверки в нем 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 в электронном документе идентификатор электронного документа. Указывается в случае, если передаваемый в запросе документ содержит в своем составе ЭЦП	0..1
-	составной тип (xs:choice)		

Элемент	Тип данных	Описание	Кратность
Base64XML	xs:base64Binary	электронный документ в формате языка разметки eXtensible Markup Language (XML), закодированный в виде base64	1
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 в нем ЭЦП	1
@WhichDocument	xs:IDREF	идентификатор электронного документа, в который вложена ЭЦП для проверки, соответствующий атрибуту //dss:Document@ID запроса на проверку ЭЦП в электронном документе	1

Элемент	Тип данных	Описание	Кратность
@XPath	xs:string	XPath-путь в передаваемом XML-документе, по которому расположена ЭЦП. Не заполняется в случае прикрепленной в передаваемом электронном документе ЭЦП в двоичном формате	0..1

3. При формировании запроса на проверку ЭЦП в электронном документе и квитанции доверенной третьей стороны используются пространства имен, перечень которых указан 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 в электронном документе может быть передан только 1 электронный документ.

Таблица 3

Идентификаторы типа ЭЦП в двоичном формате

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

5. В запросе на проверку ЭЦП в электронном документе 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:Base 64Data.

6. Передаваемые в запросе на проверку ЭЦП в электронном документе 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.

7. 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.

8. Вычисление хэша электронного документа доверенной третьей стороной проверяемого участника и формирование ЭЦП, которой подписывается квитанция доверенной третьей стороны проверяемого

участника, осуществляются в соответствии со следующими криптографическими стандартами:

а) ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

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

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 в электронном документе	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

Элемент	Тип данных	Описание	Кратность
ResultMinor	xs:anyURI	элемент с дополнительными сведениями о проведенных проверках в соответствии с таблицей 7	1
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 в электронном документе, переданного для проверки ЭЦП. Не заполняется в случае формирования квитанции с отрицательным результатом	0..1

Элемент	Тип данных	Описание	Крат-ность
		проверки ЭЦП если сертификат открытого ключа отсутствовал в запросе	
dss:DocumentHash	xs:extension base="dss:DocumentBaseType"	оборачивающий элемент для указания хэша электронного документа, переданного для проверки ЭЦП. Не заполняется в случае формирования квитанции с отрицательным результатом проверки ЭЦП, если электронный документ отсутствовал в запросе на проверку ЭЦП в электронном документе	0..1
ds:Transforms	ds:TransformType	перечень преобразований, которые доверенная третья сторона применила к электронному документу, переданному для проверки в нем ЭЦП, до вычисления хэша электронного документа. Заполняется в случае формирования квитанции доверенной третьей стороны для электронного документа в	0..1

Элемент	Тип данных	Описание	Кратность
		формате языка разметки XML	
ds:DigestMethod	ds:DigestMethodType	описание криптографического стандарта функции хэширования	1
@Algorithm	anyURI	URI криптографического стандарта функции хэширования, указывается согласно пункту 10 настоящих Требований	1
ds:DigestValue	ds:DigestValueType	хэш электронного документа, переданного для проверки в нем ЭЦП	1
ttp:SignatureTTP	dss:InlineXMLType	блок для передачи квитанции доверенной третьей стороны проверяемого участника, заполняется только при формировании квитанции доверенной третьей стороны проверяемого участника	0..1
ttp:ValidationTimeStamp	xades:EncapsulatedPKIDa Type	штамп времени поверки ЭЦП, оформленный согласно стандарту протокола штампов времени RFC 3161. Заполняется при формировании квитанции доверенной	0..1

Элемент	Тип данных	Описание	Крат-ность
		третьей стороны проверяемого участника. Правила формирования штампа времени приведены в пункте 10 настоящих Требований.	
ttp:Responder	xs:string	сведения, идентифицирующие доверенную третью сторону: требования к заполнению поля определяются на национальном уровне	1
ds:Signature	ds:SignatureType	оборачивающий элемент блока ЭЦП квитанции	1
@Id	ds:ID	Идентификатор подписи квитанции доверенной третьей стороны. Заполняется значением: “TTPResponseSignature”	
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.or	1

Элемент	Тип данных	Описание	Кратность
		g/2001/10/xml-exc-c14n#)	
ds:SignatureMethod	ds:SignatureMethodType	оборачивающий элемент алгоритма формирования ЭЦП	1
@Algorithm	xs:anyURI	при формировании квитанции доверенной третьей стороны инициатора запроса указываться идентификатор криптографического стандарта формирования ЭЦП государства-члена инициатора запроса при формировании квитанции доверенной третьей стороны проверяемого участника указывается идентификатор криптографического стандарта формирования ЭЦП в соответствии с пунктом 8 настоящих Требований	1
ds:Reference	ds:ReferenceType	оборачивающий элемент для ссылки на подписываемый блок основных реквизитов квитанции	1
@URI	xs:anyURI	атрибут, идентифицирующий блок	1

Элемент	Тип данных	Описание	Кратность
		ds:Reference в качестве ссылки на блок основных реквизитов квитанции. Заполняется значением: ""	
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: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) Таким образом, подпись охватывает все блоки квитанции	1
ds:DigestMethod	ds:DigestMethodType	оборачивающий элемент криптографического стандарта функции хэширования	1
@Algorithm	xs:anyURI	При формировании квитанции доверенной	1

Элемент	Тип данных	Описание	Крат-ность
		третьей стороны инициатора запроса указывается URI криптографического стандарта функции хэширования государства-члена инициатора запроса. При формировании квитанции доверенной третьей стороны проверяемого участника указывается URI криптографического стандарта функции хэширования в соответствии с пунктом 8 настоящих Требований	
ds:DigestValue	ds:DigestValueType	хэш, вычисленный для блока основных реквизитов квитанции после проведения каноникализации XML	1
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	1

Элемент	Тип данных	Описание	Кратность
		формате XAdES, приведенных в таблице 5, заполняется значением «#SignedProperties»	
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 криптографического стандарта функции хэширования	1
@Algorithm	xs:anyURI	При формировании квитанции доверенной третьей стороны инициатора запроса указывается URI криптографического стандарта функции хэширования государства-члена инициатора запроса. При формировании квитанции доверенной третьей стороны проверяемого	1

Элемент	Тип данных	Описание	Крат-ность
		участника указывается URI криптографическ ого стандарта функции хэширования в соответствии с пунктом 8 настоящих Требований	
ds:DigestValue	ds:DigestValueType	хэш, вычисленный для блока дополнительных реквизитов квитанции в формате XAdES после проведения каноникализации XML	1
ds:SignatureValue	ds:SignatureValueType	значение ЭЦП, вычисленное 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

Элемент	Тип данных	Описание	Кратность
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
@Target	ds:anyURI	Атрибут-ссылка на подпись квитанции доверенной третьей стороны. Заполняется значением "#TTPResponseSignature"	1
@Id	ds:ID	Атрибут-идентификатор для ссылки из блока Reference. Заполняется значением "SignedProperties"	1
xades:SignedSignatureProperties	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

Элемент	Тип данных	Описание	Кратность
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 хэша, вычисленного для сертификата ключа проверки ЭЦП доверенной третьей стороны	1
ds:DigestMethod	ds:DigestMethodType	оборачивающий элемент криптографического стандарта функции хэширования	1
@Algorithm	xs:anyURI	При формировании квитанции доверенной третьей стороны инициатора запроса, указывается URI криптографического стандарта функции хэширования государства-члена инициатора запроса. При формировании квитанции доверенной третьей проверяемого участника указывается URI криптографического стандарта функции хэширования согласно пункту 9 настоящих Требований	1
ds:DigestValue	ds:DigestValueType	хэш, вычисленный для сертификата ключа проверки ЭЦП	1

Элемент	Тип данных	Описание	Кратность
		доверенной третьей стороны	
ds:IssuerSerial	ds:X509IssuerSerialType	оборачивающий элемент	1
ds:X509IssuerName	xs:string	наименование удостоверяющего центра выпустившего сертифика 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. Не заполняется при формировании квитанции доверенной третьей стороны проверяемого участника	0..1
xades:UnsignedSignatureProperties	xades:UnsignedSignaturePropertiesType	блок неподписываемых свойств ЭЦП, содержащий штамп времени	1
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	1

Элемент	Тип данных	Описание	Кратность
		приведены в пункте 10 настоящих Требований.	

9. В квитанции доверенной третьей стороны блок VerifyResponse/dss:OptionalOutputs/dss:DocumentHash/ds:DigestValue заполняется хэшем электронного документа, переданного для проверки в нем ЭЦП.

При формировании квитанции доверенной третьей стороны инициатора запроса хэш электронного документа вычисляется с применением криптографического стандарта функции хэширования государства-члена инициатора запроса.

При формировании квитанции доверенной третьей стороны проверяемого участника хэш электронного документа вычисляется с применением криптографического стандарта функции хэширования в соответствии с пунктом 8 настоящих Требований.

10. Формирование штампа времени(необязательный элемент ttp:ValidationTimeStamp) для фиксации времени проверки ЭЦП в электронном документе для квитанции доверенной третьей стороны проверяемого участника выполняется с использованием сервиса штампа времени доверенной третьей стороны или сервиса штампа времени государства проверяемого участника (при наличии таких сервисов).

Формирование штампа времени (элемент xades:EncapsulatedTimeStamp) для квитанции доверенной третьей стороны инициатора запроса выполняется с использованием сервиса штампа времени государства инициатора запроса.

11. Порядок проверки ЭЦП в 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 (действительность) 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 расчетного 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 в квитанции доверенной третьей стороны.

12. 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:EncapsulatedTimeStamp (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 инициатора запроса формируется с применением криптографического стандарта функции хэширования государства инициатора запроса;

время подписания квитанции доверенной третьей стороны указывается в блоке xades: SigningTime;

хэш сертификата ключа доверенной третьей стороны, указанный в блоке .//xades:SignedSignatureProperties/xades:SigningCertificate/xades:Cert/xades:CertDigest/ds:DigestValue должен совпадать с хэшем, вычисленным 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/xades: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:SignedSignatureProperties/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 (действительность) штампа времени квитанции доверенной третьей стороны подтверждена на основании переданного в штампе времени значения ЭЦП и вычисленного хэша 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 в электронном документе выполнена	urn:oasis:names:tc:dss:1.0:resultmajor:Success
Процедура проверки ЭЦП в электронном документе не выполнена в связи с ошибкой в запросе на проверку ЭЦП в электронном документе	urn:oasis:names:tc:dss:1.0:resultmajor:RequesterError
Процедура проверки ЭЦП в электронном документе не выполнена в связи с ошибкой на стороне ДТС	urn:oasis:names:tc:dss:1.0:resultmajor:ResponderError
Процедура проверки ЭЦП в электронном документе 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 (действительности) ЭЦП выполнена (Success)	подлинность (действительность) ЭЦП и штамп времени (при наличии) подтверждена	urn:oasis:names:tc:dss:1.0:result minor:valid:signature:OnAllDocuments
	подлинность (действительность) ЭЦП не подтверждена	urn:oasis:names:tc:dss:1.0:result minor:invalid:IncorrectSignature
	подлинность (действительность) ЭЦП подтверждена, но не подтверждена подлинность (действительность) штампа времени ЭЦП	urn:oasis:names:tc:dss:1.0:result minor:valid:signature:InvalidSignatureTimestamp
Процедура подтверждения подлинности (действительности) ЭЦП не выполнена в связи с ошибкой в запросе на проверку ЭЦП в электронном документе (RequesterError)	электронный документ, указанный в ds:Reference блока ds:Signature, отсутствует в запросе на проверку ЭЦП в электронном документе	urn:oasis:names:tc:dss:1.0:result minor:ReferencedDocumentNotPresent
	сведения о сертификате проверки ЭЦП, ожидаемые сервером, отсутствуют в запросе на проверку ЭЦП в электронном документе	urn:oasis:names:tc:dss:1.0:result minor:KeyInfoNotProvided
	сервер не смог обработать передаваемый электронный документ	urn:oasis:names:tc:dss:1.0:result minor:NotParseableXMLDocument
	сервер не смог обработать запрос, так как составе передаваемого электронного документа не найдена ЭЦП	urn:oasis:names:tc:dss:1.0:result minor:NotSupported
	ЭЦП или ее содержимое не соответствуют криптографическому стандарту (стандартам) используемым ДТС, указанному в запросе на проверку ЭЦП в электронном документе	urn:oasis:names:tc:dss:1.0:result minor:Inappropriate:signature

Основной ответ	Статус проверки	URI
Процедура подтверждения подлинности (действительности) 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 (действительности) 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

ОБЩИЕ ТРЕБОВАНИЯ
к структуре, формату и организации обмена сообщениями при взаимодействии доверенных третьих сторон между собой

1. Настоящие Требования устанавливают общие требования к структуре, формату и организации обмена сообщениями при взаимодействии доверенных третьих сторон между собой.

При реализации электронного взаимодействия между доверенными третьими сторонами государств-членов для вычисления хэша электронного документа и формирования ЭЦП должны применяться следующие криптографические стандарты:

ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

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

2. Для обеспечения доставки данных от одной доверенной третьей стороны до другой доверенной третьей стороны, 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 рекомендательной реализации электронного взаимодействия в дополнение к RFC 3029.

3. Электронное взаимодействие между доверенными третьими сторонам на технологическом уровне организовывается посредством сообщений в формате SOAP 1.2 (Simple Object Access Protocol, http://www.w3.org/TR/soap12-part1) 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 в том числе выбран в качестве рекомендательной реализации электронного взаимодействия в дополнение к RFC 3029.

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

6. Коды типовых ошибок к использованию при формировании технологического сообщения об ошибке приведены в таблице.

Коды типовых ошибок

Класс ошибки	Код ошибки*	Описание и особенности применения
	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 электронного взаимодействия

Класс ошибки	Код ошибки*	Описание и особенности применения
Sender	ttp:InvalidRequest	структура запроса на проверку ЭЦП в электронном документе не соответствует установленным требованиям в соответствии с приложением № 1 (приложением № 2 в случае реализации рекомендательного варианта электронного взаимодействия), вследствие чего запрос не может быть обработан
Sender, Receiver	ttp:InvalidReceipt	структура квитанции доверенной третьей стороны не соответствует установленным требованиям в соответствии с приложением № 1 (приложением № 2 в случае реализации рекомендательного варианта электронного взаимодействия), вследствие чего квитанция не может быть обработана
Sender	ttp:TTPNotFound	запрос на подтверждение подлинности (действительности) ЭЦП в электронном документе доверенной третьей стороне проверяемого участника не передан в связи с невозможностью определить, какой именно доверенной третьей стороне должен быть передан запрос
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 в электронном документе либо формирования и отправки квитанции доверенной третьей стороны; указанный код используется в случае, если ошибка не описана в спецификации SOAP или настоящей таблице

* Префиксу «ttp» соответствует пространство имен:

«urn:EEC:TTP:VSD:ETP:1.0» при осуществлении электронного взаимодействия по стандарту DVCS;

«urn:EEC:TTP:DSS:1.0» при осуществлении электронного взаимодействия по стандарту OASIS DSS.