№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
Предложения и замечания ЗАО «ЭКЕНГ», Республика Армения				
1.	п. 21 пп. б)	В целях исключения неоднозначности в формулировке пункта 21 проекта Правил предлагается следующая редакция: 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;	21. Доверенная третья сторона инициатора запроса после получения квитанции доверенной третьей стороны проверяемого участника проверяет соблюдение следующих требований в совокупности: 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;	**Предлагается принять предложение**
2.	п. 6 Приложения 1 и п. 5 Приложения 2	Касательно передачи запроса на проверку ЭЦП электронного документа, содержащего 2 и более ЭЦП, сформированных с использованием	Не допускается передача запроса на проверку ЭЦП в электронном документе, подписанного с использованием криптографических стандартов разных государств-членов	**Текущая редакция соответствует предложению.**

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
		криптографических стандартов разных государств-членов, ЗАО «ЭКЕНГ» считает приемлимым подход формирования отдельных запросов на проверку ЭЦП для каждой ЭЦП в отдельности с целью упрощения данной процедуры.	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 в электронном документе для каждой ЭЦП.	
3.	п. 12 Приложения 1 и п. 11 Приложения 2	Мы также отмечаем, что 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	. 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	**Текущая редакция соответствует предложению.**

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
		времени при помощи установленных криптографических стандартов.	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». 11. Формирование штампа времени (элемент	

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			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	

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			информации. Функция хэширования» и ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».	
4.	п. 13	В отношении протокола взаимодействия поставщика или заказчика с оператором веб-портала органа государственной власти, юридического лица или индивидуального предпринимателя на территории государств-членов, считаем целесообразным использовать положения, определенные стандартом RFC 3029, с целью унификации реализации схемы ДТС в целом.	13. Требования к формату и структуре запроса на проверку ЭЦП, а также требования к формату и структуре квитанции доверенной третьей стороны, определенные Правилами в качестве основного варианта реализации информационного обмена между доверенными третьими сторонами, установлены в приложении № 1. В качестве альтернативного варианта реализации информационного обмена могут быть использованы формат и структура запроса на проверку ЭЦП, а также формат и структура квитанции доверенной третьей	**Текущая редакция соответствует предложению.**

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			стороны, представленные в приложении № 2. Используемые для взаимодействия между доверенными третьими сторонами стандарты, определяющими формат и структуру запроса на проверку ЭЦП в электронном документе, передаваемом доверенной третьей стороне, и квитанции доверенной третьей стороны, формируемой доверенной третьей стороной в ответ на запрос на проверку ЭЦП в электронном документе, с учетом требований настоящих Правил указывается в соглашении, заключаемом между доверенными третьими сторонами.	
5.	-	Считаем также целесообразным применение механизмов для обеспечения конфиденциальности информации, передаваемой поставщиками одного государства-члена ЕАЭС	-	Данный вопрос выходит за рамки правил проверки и признания ЭЦП. Тем не менее предлагается для конфиденциального взаимодействия разрешить использование шифрования

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
		электронным торговым площадкам другого государства-члена ЕАЭС, а также дополнить проект Правил соответствующими положениями.		канала связи при помощи одностороннего TLS соединения с использованием международного сертификата. По аналогии с работой электронных площадок РФ, например, используемый Сбербанком. По крайне мере разрешить это в качестве временного решения для запуска государственных закупок в рамках ЕАЭС до тех пор, пока странами не будет выработан другой механизм защиты (которое потребует длительного времени так как вопрос применения национальных сертификатов полностью не решен ни одной страной ЕАЭС даже на национальном уровне а тем более трансграничном).
Предложения и замечания Минцифры России, Российская Федерация				
6.	п. 13 (в предыдуще	Полагаем целесообразным уточнить в абзаце 2 (стр. 9) п.	14. Требования к формату и структуре запроса на проверку	**Предлагается принять предложение, пункт 13**

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
	й редакции п. 14)	14 раздела III «Процедура подтверждения подлинности», п. 14, абзац 2 (стр. 9) информацию о сценариях «альтернативной реализации информационного обмена»	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. Используемые для взаимодействия между доверенными третьими сторонами стандарты, определяющими 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	**представить в следующей редакции:** 13. Требования к формату и структуре запроса на проверку ЭЦП, а также требования к формату и структуре квитанции доверенной третьей стороны, определенные Правилами в качестве основного варианта реализации информационного обмена между доверенными третьими сторонами, установлены в приложении № 1. В качестве альтернативного варианта реализации информационного обмена могут быть использованы формат и структура запроса на проверку ЭЦП, а также формат и структура квитанции доверенной третьей стороны, представленные в приложении № 2.

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			электронного документа, с учетом требований настоящих Правил указывается в соглашении, заключаемом между доверенными третьими сторонами.	Используемые для взаимодействия между доверенными третьими сторонами стандарты, определяющими формат и структуру запроса на проверку ЭЦП в электронном документе, передаваемом доверенной третьей стороне, и квитанции доверенной третьей стороны, формируемой доверенной третьей стороной в ответ на запрос на проверку ЭЦП в электронном документе, с учетом требований настоящих Правил указывается в соглашении, заключаемом между доверенными третьими сторонами.
7.	Приложение № 1	В Приложении № 1 к Правилам отсутствует уточнение о применяемом формате передачи данных (MIME, XML) и заголовках сообщений.	-	**Текущая редакция соответствует предложению.** В Приложении 1 обозначено требование по заполнению блока requestInformation.extensions.M

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
				imeType запроса на проверку ЭЦП электронного документа для указания типа документа, передаваемого на проверку: 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"
8.	п. 3, п. 4 Приложения № 4	В соответствии с п. 3 Приложения № 3 к Правилам для передачи сообщений между участниками предлагается применение протокола HTTPS, что противоречит	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/r	**Данное предложение не может быть учтено:** поскольку реализация Правил не предусматривает использование инфраструктуры и ресурсов интегрированной информационной системы

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
		п. 3 Приложения № 1 к Правилам электронного обмена данными в интегрированной информационной системе внешней и взаимной торговли, утвержденным Решением Коллегии Евразийской экономической комиссии от 27.01.2015 № 5, поскольку в настоящее время на транспортном уровне интеграционные шлюзы обмениваются между собой транспортными сообщениями в формате программного обеспечения брокера обмена сообщениями IBM MQ, оформляемыми в соответствии с пунктами 8 – 11 обозначенного документа. 2 В соответствии с п. 4 Приложения № 3 к Правилам предполагается	fc2818) 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. 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 рекомендаций стандарта RFC 3029 (Internet	Союза, в связи с чем противоречий с вышеуказанными документами не возникает.

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
		информационный обмен с использованием протокола SOAP 1.2. При этом, согласно п. 5 Приложения № 3 к Правилам признания электронной цифровой подписи (электронной подписи) в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии юридических лиц (хозяйствующих субъектов) с уполномоченными органами государств–членов Евразийского экономического союза и Евразийской экономической комиссии с использованием службы доверенной третьей стороны (далее — ДТС), утвержденных Решением	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.	

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
		Коллегии Евразийской экономической комиссии от 22.08.2023 № 120, должен применяться формат стандарта MIME.		
9.	п. 9 (ранее п. 10)	Необходимо предоставить пояснения относительно необходимости соответствия электронного документа, созданного для участия в торгах на электронной торговой площадке, требованиям п. 10 (стр. 7-8) раздела III «Процедура подтверждения подлинности», в случае, если была успешно выполнена проверка электронной (цифровой) подписи.	9. В случае представления поставщиком электронного документа, подписанного ЭЦП, изготовленной с использованием криптографических стандартов и в соответствии с требованиями государства-члена места регистрации поставщика, оператор электронной торговой площадки (электронной площадки) формирует и передает запрос на проверку ЭЦП в электронном документе (далее – инициатор запроса) доверенной третьей стороне своего государства-члена. Инициатор запроса направляет запрос на проверку ЭЦП в электронном документе доверенной третьей стороне своего государства-члена, начиная	**Необходимо разъяснение вопроса**

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			с момента получения электронного документа, подписанного поставщиком. В случаях, предусмотренных законодательством государств-членов, инициатором запроса к доверенной третьей стороне может выступать оператор веб-портала этого государства-члена.	
10.	п. 5 Приложения 1, п.4 Приложения 2	Необходимо указать причины, по которым запрещается передача в составе одного запроса нескольких документов.	Приложение 1: 5. В запросе на проверку ЭЦП в электронном документе может быть передан только 1 электронный документ. Приложение 2: 4. В запросе на проверку ЭЦП в электронном документе может быть передан только 1 электронный документ.	Структура RFC 3029 не предусматривает передачу в блоке data нескольких объектов SignedData («электронных документов»). Помимо этого передача нескольких электронных документов в запросе на проверку ЭЦП существенно усложнит реализацию ДТС и формирования квитанций от других ДТС.
11.	п. 19	Необходимо предоставить пояснения относительно распространения максимального срока на	19. Проверка ЭЦП в электронном документе заключается в проверке соблюдения	Ранее исходя из технической возможности и требований торговых площадок к скорости обработки запросов было

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
		проверку электронной (цифровой) подписи электронного документа в размере 60 секунд на весь процесс проверки электронного документа или исключительно на работу ДТС (в соответствии с п.4 Приложения № 1 к Правилам).	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	предложено ограничение 60 сек. В результате обсуждений была представлена текущая редакция, в соответствии с которой сроки на проверку ЭЦП и подготовке квитанции устанавливаются в соглашении между ДТС.

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			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 в электронном документе; 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.	

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			В случае если все указанные условия при проверке ЭЦП в электронном документе выполняются, подлинность (действительность) электронного документа считается подтвержденной (положительный результат проверки). Если хотя бы одно из условий для проверки ЭЦП в электронном документе не выполняется, подлинность (действительность) электронного документа считается неподтвержденной (отрицательный результат проверки). Все указанные проверки осуществляются на текущие дату и время проверки ЭЦП в электронном документе или на дату и время, указанные в штампе времени при его наличии. Срок на проверку ЭЦП в электронном документе и подготовки квитанции доверенной третьей стороны устанавливается	

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			в соглашениях между доверенными третьими сторонами.	
12.	п. 12 Приложения 1, п. 11 Приложения 2	Необходимо указать причины, по которым в соответствии с п. 11 Приложения № 1 к Правилам и с п. 11 Приложения № 2 к Правилам штамп времени проверяемого участника формируется с использованием сервиса штампа времени удостоверяющего центра службы ДТС интегрированной информационной системы Евразийского экономического союза, а не сервиса штампа времени государства-члена ЕАЭС	Приложение 1: 12. 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	ДТС инициатора запроса при получении квитанции от ДТС проверяемого участника должен иметь возможность проверить штамп времени ДТС проверяемого участника, поэтому для формирования штампа времени квитанции проверяемого участника должен использоваться сервис штампа времени удостоверяющего центра службы доверенной третьей стороны.

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			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». Приложение 2: 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	

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			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».	

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
Предложения и замечания ФСБ России, Российская Федерация				
13.	-	Используемые термины не приведены в соответствие с терминами, применяемыми в международных стандартах и актах Комиссии	-	Термины, используемые в проекте Правил, скорректированы в новой редакции проекта Правил.
14.		Отсутствуют положения о проверке полномочий лица, подписавшего электронный документ своей электронной цифровой подписью		Предлагается оставить текущую редакцию. Порядок проверки полномочий лица, подписавшего электронный документ своей электронной цифровой подписью для осуществления закупок противоречит Договору о Союзе и находятся за пределами регулирования настоящего проекта Правил.
15.		Отсутствуют положения, устанавливающие требование об обеспечении конфиденциальности информации, передаваемой		Данный вопрос выходит за рамки правил проверки и признания ЭЦП. Тем не менее предлагается для конфиденциального

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
		потенциальными поставщиками одного государства-члена Союза на электронные площадки другого государства-члена Союза, а также порядок обеспечения этого требования.		взаимодействия разрешить использование шифрования канала связи при помощи одностороннего TLS соединения с использованием международного сертификата. По аналогии с работой электронных площадок РФ, например, используемый Сбербанком. По крайне мере разрешить это в качестве временного решения для запуска государственных закупок в рамках ЕАЭС до тех пор, пока странами не будет выработан другой механизм защиты (которое потребует длительного времени так как вопрос применения национальных сертификатов полностью не решен ни одной страной ЕАЭС даже на национальном уровне, а тем более трансграничном).
16.	Приложение 1	В приложении 1 указать сведения о подписании ЭЦП	-	Считаем нецелесообразным подписание запросов от

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
		запроса DVCSRequest, а также сведений об алгоритмах создания такой подписи и хэш значения (поле requestInformation.extensions.DocumentHash) для запросов, направляемых как к ДТС инициатора, так и ДТС проверяемого участника.		торговых площадок и веб порталов к ДТС, поскольку это усложнить как работу торговых площадок и веб порталов так и ДТС. Взаимодействие торговых площадок и веб порталов с ДТС регулируется национальным законодательством.
17.	Приложение 1	В приложении 1 указать сведения об алгоритмах создания ЭЦП квитанций DVCSResponse, направляемых как инициатору запроса, так и ДТС инициатора запроса	-	**Текущая редакция соответствует предложению.** В соответствии с RFC 3029 при подписании квитанции DVCSResponse с помощью ЭЦП, для ЭЦП используется структура SignedData, определяемая стандартом CMS. Данная структура содержит поля, идентифицирующие конкретные алгоритмы создания ЭЦП. Требования к использованию конкретных алгоритмов указаны в

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
				основной части Правил. В целях однозначного понимания каким образом в структуре квитанции указываются сведения об алгоритмах создания ЭЦП.
18.	п. 13 (ранее п. 14)	Указать в пункте 14 проекта Правил (в том числе в Приложении 2) на необязательность использования стандарта OASIS DSS, поскольку данный стандарт не реализован в средствах ДТС Комиссии	Редакция пункта предыдущей редакции проекта Правил: 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. Используемые для взаимодействия между доверенными третьими сторонами	**Предлагается принять предложение. Предлагается следующая редакция п.13:** 13. Требования к формату и структуре запроса на проверку ЭЦП, а также требования к формату и структуре квитанции доверенной третьей стороны, определенные Правилами в качестве основного варианта реализации информационного обмена между доверенными третьими сторонами, установлены в приложении № 1. В качестве альтернативного варианта реализации информационного обмена могут быть использованы

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			стандарты, определяющими 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.	формат и структура запроса на проверку ЭЦП, а также формат и структура квитанции доверенной третьей стороны, представленные в приложении № 2. Используемые для взаимодействия между доверенными третьими сторонами стандарты, определяющими формат и структуру запроса на проверку ЭЦП в электронном документе, передаваемом доверенной третьей стороне, и квитанции доверенной третьей стороны, формируемой доверенной третьей стороной в ответ на запрос на проверку ЭЦП в электронном документе, с учетом требований настоящих Правил указывается в соглашении, заключаемом между доверенными третьими сторонами.

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
19.		Указать в приложении 2 сведения о подписании ЭЦП запроса VerifyRequst, а также сведений об алгоритмах создания такой подписи и хэш-значения (поле dss.DocumentHash) для запросов, направляемых как в ДТС инициатора, так и к ДТС проверяемого участника		Считаем нецелесообразным подписание запросов от торговых площадок и веб порталов к ДТС, поскольку это усложнить как работу торговых площадок и веб порталов так и ДТС. Взаимодействие торговых площадок и веб порталов с ДТС регулируется национальным законодательством.
20.		Указать в приложении 2 сведения о подписании ЭЦП квитанции VerifyResponse, а также сведений об алгоритмах создания такой подписи для квитанций, направляемых как инициатору запроса, так и ДТС инициатора запроса		В структуре квитанции VerifyResponse передается ЭЦП квитанции в блоке ds:Signature, сведений об алгоритмах создания такой подписи указываются в блоке ds:Signature/ds:SignedInfo/ ds:SignatureMethod@Algorithm Предлагается актуализировать описание блоков структуры для соответствия основному тексту Правил.

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
21.	Раздел I	Определение хэш-значения в разделе 1 проекта Правил привести в соответствие с определением, описанным в криптографическом стандарте ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»	«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; Определения из ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»: Хэш-код (hash-code): строка бит, являющаяся выходным результатом хэш-функции. Хэш-функция (collision-resistant hash-function): функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая следующим свойствам: 1) по данному значению	Предлагается обсудить на рабочей группе. Речь идет о замене термина «хэш-значение» на «хэш-код», а также добавления определения «хэш-функция».

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			функции сложно вычислить исходные данные, отображаемые в это значение; 2) для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в то же значение функции; 3) сложно вычислить какую-либо пару исходных данных, отображаемых в одно и то же значение.	
22.	Раздел 1	В определении электронного документа в разделе 1 проекта Правил указывается необходимость его соответствия требованиям общей инфраструктуры документирования информации в электронном виде. Вместе с тем такие требования правом Союза для информационного взаимодействия хозяйствующих субъектов не установлены. В связи с этим	Определение в предыдущей редакции Правил: «электронный документ» – документ в электронном виде, заверенный электронной цифровой подписью (электронной подписью) и отвечающий требованиям общей инфраструктуры документирования информации в электронном виде.	**Предлагается принять предложение. Предлагается следующая редакция:** «электронный документ» – документ в электронном виде, заверенный электронной цифровой подписью (электронной подписью).

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
		указанное определение необходимо скорректировать.		
23.	Приложение 2	Описание алгоритмов создания хэш-значений электронного документа (поле dss:DocumentHash) в таблице 4 приложения № 2 привести в соответствие с пунктом 9 данного приложения	Из таблицы 4 Приложения 2: «хэш-значение электронного документа, переданного для проверки ЭЦП Не заполняется в случае формирования квитанции с отрицательным результатом проверки ЭЦП, если электронный документ отсутствовал в запросе» Пункт 9 Приложения 2: 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	Предлагается при описании поля поле dss:DocumentHash в таблице 4 Приложения № 2 указать ссылку на пункт 9 Приложения 2

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
			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.	
24.	Приложение 2	Описание штампа времени в таблице 4 приложения № 2 привести в соответствие с пунктами 11 и 13 данного приложения		Аналогично предыдущему предложению указать ссылки в таблице 4 Приложения 2 на пункты 11 и 13 Приложения 2.

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
25.	п. 15, Приложение 4	Исключить обязательность реализации положений приложения № 4, поскольку использование стандарта OASIS DSS не является обязательным и требования к информационному взаимодействию между инициатором запроса и ДТС юрисдикции инициатора запроса, в том числе требования к протоколам обеспечения аутентичности и конфиденциальности соединений, а также криптографическим алгоритмам, определяются государством-членом Союза.		**Текущая редакция соответствует предложению.** Стандарт OASIS DSS определен в Правилах в качестве альтернативного варианта. В пункте 15 правил установлено что порядок информационного взаимодействия между инициатором запроса и доверенной третьей стороной государства-члена инициатора запроса устанавливаются на национальном уровне.