ТАБЛИЦА

предложений и замечаний Оперативно-аналитического центра при Президенте Республики Беларусь по проекту Правил взаимного признания электронной цифровой подписи (электронной подписи), изготовленной в соответствии с законодательством одного государства-члена, другим государством-членом для целей государственных (муниципальных) закупок

№ п/п	Структурн. элемент	Предложение или замечание	Текущая редакция в проекте Правил	Предложение ЕЭК
1	Пункт 12 (в предыдущей редакции 11)	В пункте 11 (в представленной редакции пункт 12) слова «в соответствии с положениями раздела IV настоящих Правил» дополнить словами «в соответствии с договорами (соглашениями) между доверенными третьими сторонами, их регламентами и с учетом положений раздела IV настоящих Правил»	12. Доверенные третьи стороны во взаимодействии друг с другом обеспечивают проверку ЭЦП электронного документа в соответствии с положениями раздела IV настоящих Правил. Документом, определяющим результат проверки ЭЦП, является квитанция доверенной третьей стороны, передаваемая инициатору запроса доверенной третьей стороной, которой был направлен запрос на проверку ЭЦП электронного документа.	**Предложение было учтено в пункте 17 проекта Правил.** Пункт 12 указывает, что проверка ЭЦП электронного документа осуществляется в соответствии с положениями раздела IV. При этому пункт 17 Раздела IV содержит в себе указание, что 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.** На основании вышеизложенного указание предложенной информации в пункте 12 считаем избыточным.
2	Пункт 20 (в предыдущей редакции 19)	Пункт 19 (в представленной редакции пункт 20) дополнить абзацем «Оператор электронной торговой площадки (электронной площадки) направляет запрос на проверку ЭЦП не позднее суток с момента предоставления поставщиком электронного документа».	20. Проверка ЭЦП электронного документа заключается в проверке соблюдения следующих условий в совокупности: целостность электронного документа не нарушена, что проверяется путем сравнения хэш-значения электронного	**Предлагается дополнить пункт 10 проекта Правил предлагаемой информацией.** В соответствии с текущим содержанием проекта Правил предлагаем предложенную информацию включить в пункт 10

			документа, вычисленного доверенной третьей стороной проверяемого участника, с хэш-значением электронного документа, переданным доверенной третьей стороной инициатора запроса; ЭЦП сформирована с использованием закрытого (личного) ключа (ключа ЭЦП), соответствующий открытый ключ которого (сертификат ключа проверки ЭЦП) указан в составе этой ЭЦП; сертификат ключа проверки ЭЦП действителен на момент проверки электронного документа или его подписания при наличии штампа времени; каждый сертификат ключа проверки ЭЦП из цепочки сертификатов ключей проверки ЭЦП удостоверяющих центров действителен на момент подписания электронного документа при наличии штампа времени или на момент проверки; сертификат ключа проверки ЭЦП предназначен для проверки ЭЦП электронного документа; подтверждена действительность штампа времени электронного документа (при наличии). Доверенная третья сторона проверяемого участника вправе дополнительно осуществлять проверку ЭЦП проверяемого участника государственных (муниципальных) закупок на межгосударственном (трансграничном) уровне в электронном документе, в том числе в соответствии с требованиями	проекта Правил и представить данный пункт в следующей редакции: «10.В случае представления поставщиком или иными субъектами электронного взаимодействия электронного документа, подписанного ЭЦП, изготовленной с использованием криптографических стандартов и в соответствии с требованиями государства-члена места регистрации поставщика или иных субъектов электронного взаимодействия, оператор электронной торговой площадки (электронной площадки) формирует и передает запрос на проверку ЭЦП электронного документа (далее – инициатор запроса) доверенной третьей стороне своего государства-члена. **Инициатор запроса направляет запрос на проверку ЭЦП электронного документа доверенной третьей стороне своего государства-члена начиная с момента получения электронного документа, подписанного поставщиком или иными субъектами электронного взаимодействия.** В случаях, предусмотренных законодательством государств-членов, инициатором запроса к

			законодательства своего государства-члена. В случае если все указанные условия при проверке ЭЦП электронного документа выполняются, подлинность электронного документа считается подтвержденной (положительный результат проверки). Если хотя бы одно из условий для проверки ЭЦП электронного документа не выполняется, подлинность электронного документа считается неподтвержденной (отрицательный результат проверки). Все указанные проверки осуществляются на текущие дату и время проверки ЭЦП электронного документа или на дату и время, указанные в штампе времени при его наличии. Максимальный срок проверки ЭЦП электронного документа и подготовки квитанции доверенной третьей стороны не должен превышать срок, установленный в заключенных соглашениях между доверенными третьими сторонами.	доверенной третьей стороне может выступать оператор веб-портала этого государства-члена.
3	Пункт 20 (в предыдущей редакции 19)	Исключить из части пятой пункта 19 временные ограничения «60 секунд».		**Предлагается принять предложение.** Последний абзац пункта 20 проекта Правил представить в следующей редакции: «Срок на проверку ЭЦП электронного документа и подготовки квитанции доверенной третьей стороны устанавливается в соглашениях между доверенными третьими сторонами.» **Дополнительно** подпункт «г» пункта 29 представить в следующей редакции: «г) время ожидания квитанции доверенной третьей стороны проверяемого участника доверенной третьей стороной инициатора запроса превышает срок, установленный в заключенных соглашениях между доверенными третьими сторонами;»
4	Приложение № 2	В приложении 2 предусмотреть использование формата, структур запросов (ответов), определенных стандартом RFC 3029 как обязательных для взаимодействия между доверенными третьими сторонами, а формат, структуры запросов (ответов), определенные стандартом OASIS DSS (version 1.0), указать в качестве рекомендуемых.	–	**Предлагается принять предложение.** Приложение № 1 и № 2 переработаны. Использование RFC 3029 носит обязательный характер, OASIS DSS – рекомендательный. Информация об этом также указана в пункте 14 проекта Правил.

5	Приложение № 3	В приложении 3: абзац второй пункта 4 дополнить следующим содержанием «, СТБ 34.101.50-2019 и СТБ 34.101.80-2019;»; абзац третий пункта 4 дополнить следующим содержанием «, СТБ 34.101.23-2012.»; пункт 5 и 6 исключить. Это предложение касается форматов, которые применяются в национальном сегменте и не распространяется на квитанции, которыми обмениваются ДТС между собой.	4. Формат ЭЦП электронного документа, ее атрибуты и элементы должны соответствовать одному из перечисленных стандартов в зависимости от типа ЭЦП: ЭЦП в формате XML: Signature Syntax and Processing (XMLDsig,https://www.w3.org/TR/xmldsig-core1), XML Advanced Electronic Signatures (XAdES, XAdES-T, https://www.w3.org/TR/XAdES); ЭЦП в двоичном формате: Cryptographic Message Syntax (CMS, RFC 5652, https://datatracker.ietf.org/doc/html/rfc5652), CMS Advanced Electronic Signatures (CADES-BES, CADES-EPES, CADES-T, RFC 5126, https://datatracker.ietf.org/doc/html/rfc5126). Применение расширений указанных стандартов при формировании ЭЦП не допускается.	**Предлагается следующее предложение.** Абзац четвертый в пункте 4 Приложения № 3 изменить и представить в следующей редакции: «Допускается применение расширений указанных стандартов при формировании ЭЦП в соответствии с законодательством государств-членов»[и1]
6	Приложение № 4	В приложении 4 необходимо предусмотреть организацию обмена сообщениями при взаимодействии с доверенной третьей стороной с использованием RFC 3029	–	**Предлагается принять предложение.** Приложение № 4 переработано, организация обмена сообщениями при взаимодействии с доверенной третьей стороной с использованием RFC 3029 предусмотрена.