**ТАБЛИЦА**

замечаний и предложений Федеральной службы безопасности РФ (письмо от 09.07.2025) к 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 Комиссии /****Позиции государств-членов** |
| --- | --- | --- | --- | --- |
| **1** | Таблица 7 приложения № 2 | Приведение используемых в таблице 7 приложения № 2 проекта правил терминов в соответствие с терминами, применяемыми в международных стандартных и в актах Евразийской экономической комиссии | – | **Предлагается принять предложение.**Текст таблицы скорректирован в части использования термина «сертификат ключа проверки ЭЦП» и представлен в обновленной редакции проекта Правил (v.0.4.4). |
| **2** | Проект Правил | Отсутствия положений о проверке полномочий лица, подписавшего электронный документ своей ЭЦП | – | **Предлагается сохранить текущую редакцию.**Как ранее отмечалось, регулирование механизма проверки полномочий **выходит за рамки Договора** о Евразийском экономическом и предметной области Правил.Согласно Договору, обеспечение беспрепятственного доступа потенциальных поставщиков и поставщиков государств-членов к участию в закупках, проводимых в электронном формате, **обеспечивается путем взаимного признания ЭЦП**, изготовленной в соответствии с законодательством одного государства-члена, другим государством-членом. Обеспечение полномочий представителя поставщика находится в национальной юрисдикции при выдаче ЭЦП. Проверка ЭЦП осуществляется при помощи национальных доверенных третьих сторон. |
| **3** | Проект Правил | Дополнения проекта правил положениями, устанавливающими требование по обеспечению конфиденциальности информации, передаваемой между участниками информационного взаимодействия государств-членов Союза при совершении государственных (муниципальных) закупок, и порядок реализации этого требования | – | Включение в Правила единых требований к национальным торговым площадкам в части защиты канала взаимодействия с иностранными поставщиками выходит за рамки Договора и предметной области Правил.Защита канала взаимодействия национальных торговых площадок с иностранными поставщиками осуществляется в соответствии с национальным законодательством государств-членов.**В этой связи Комиссия полагает возможным** для взаимодействия иностранного поставщика с национальной ЭТП рекомендовать использование шифрования канала связи при помощи одностороннего TLS соединения с использованием международного сертификата. Использование национальных сертификатов для защиты канала взаимодействия всеми поставщиками из других государств-членов является практически нереализуемым для трансграничного взаимодействия в рамках ЕАЭС, в том числе потому что затрагивается вопрос национального суверенитета.Средства шифрования в Комиссии (абонентское шифрование) разработано для шифрования информации между абонентами государственных органов и не может применяться для защиты канала взаимодействия в связи с техническими ограничениями.**Позиции сторон:** РА, РБ, РК, КР – за предложение ЕЭК; РФ – настаивают на своём предложении.**По предложению РФ от 17.03.2025 (создание шлюза):** **РА –** за предложение ЕЭК поиспользованию механизма защиты канала взаимодействия с международными сертификатами в качестве временного решения. **РБ –** готовы рассмотреть предложение. Просят ФСБ предоставить схему взаимодействия.**РК** – резерв позиции.**КР** – резерв позиции. |
| **4** | Приложение № 1 проекта Правил | Необходимость подписания ЭЦП запроса DVCSRequest, а также указания в приложении № 1 проекта правил сведений об алгоритмах создания такой подписи для запросов, направляемых к доверенной третьей стороне (далее – ДТС) проверяемого участника | – | **Предлагается сохранить текущую редакцию.**Вопрос подписания ЭЦП запросов к ДТС уже поднимался на предыдущих заседаниях рабочих групп (без фиксации в протоколе). Высказывалось мнение об избыточности такой меры вследствие усложнения взаимодействия с ДТС. |
| **5** | Приложение № 2 проекта Правил | Необходимость подписания ЭЦП запроса VerifyRequest, а также указания в приложении № 2 проекта правил сведений об алгоритмах создания такой подписи для запросов, направляемых к ДТС проверяемого участника | – | **Предлагается сохранить текущую редакцию.**Вопрос подписания ЭЦП запросов к ДТС уже поднимался на предыдущих заседаниях рабочих групп (без фиксации в протоколе). Высказывалось мнение об избыточности такой меры вследствие усложнения взаимодействия с ДТС. |
| **6** | Приложение № 2 проекта Правил | Указание в приложении № 2 проекта правил сведений о данных, подписываемых ЭЦП в квитанции VerifyResponse, в частности данных о результате проверки ЭЦП (поле dss:Result), хэш-значении электронного документа, вычисленного в соответствии с законодательством государства места регистрации электронного торговой площадки | – | **Предлагается принять предложение.**На рабочей группе, проходившей 22.05.2025, было предложено следующее:Элемент dss:VerifyResponse/dss:OptionalOutputs/ds:Signature/ds:SignedInfo/ds:Reference[1]/ds:Transforms/ds:Transform[2] содержит значение "[http://www.w3.org/2000/09/xmldsig#enveloped-signature".](http://www.w3.org/2000/09/xmldsig#enveloped-signature%22.) Согласно стандарту XMLDSig это означает, что при проверке подписываемых с помощью ЭЦП данных, сама ЭЦП (блок ds:Signature) исключается из структуры квитанции, а ЭЦП охватывает всю квитанцию в целом, включая данные о результате проверки ЭЦП (поле dss:Result), хэш-значении электронного документа, переданного для проверки ЭЦП (поле dss:DocumentHash), данные о времени формирования квитанции и другие**Для того, чтобы более явно подчеркнуть это,** описание элемента dss:VerifyResponse/dss:OptionalOutputs/ds:Signature/ds:SignedInfo/ds:Reference[1]/ds:Transforms/ds:Transform[2] предлагается дополнить фразой «таким образом, подпись охватывает все блоки квитанции», а также скорректировать требования к заполнению элемента dss:VerifyResponse/dss:OptionalOutputs/ds:Signature/ds:SignedInfo/ds:Reference[1] убрав значение "urn:EEC:TTP:v1.0:verify:response", поставить вместо этого пустые кавычки "". |
| **7** | Пункт 18, приложение № 1, приложение № 2 проекта Правил | Указание в абзаце втором пункта 18, приложениях № 1 и № 2 проекта правил сведений о месте размещения хэш-значения электронного документа, переданного ДТС инициатора запроса, с которым при проверке ЭЦП сравнивает хэш-значение, вычисленное ДТС проверяемого участника | «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;…» | **Предлагается частично принять предложение.**В подпункт а пункта 17 (ранее пункт 18) предлагается внести изменение, касающееся указание место размещения хэша электронного документа. Предлагается следующая редакция:«17. Доверенная третья сторона проверяемого участника, получившая запрос на проверку ЭЦП от доверенной третьей стороны инициатора запроса, выполняет проверку ЭЦП в электронном документе, переданном в запросе. Проверка ЭЦП в электронном документе заключается в проверке соблюдения следующих требований в совокупности:а) целостность электронного документа не нарушена, что проверяется путем сравнения хэша электронного документа, вычисленного доверенной третьей стороной проверяемого участника в соответствии с законодательством государства-члена доверенной третьей стороны проверяемого участника, с хэшем электронного документа, **входящим в состав ЭЦП**;…»Предложенная редакция однозначно указывает место размещения хэша.При этом в приложениях № 1 и № 2 указание размещения данного хэша не целесообразно, так как состав ЭЦП в указанных приложениях не представлен.В редакцию Раздела 3 проекта Правил были изменения, касающиеся последовательности электронного взаимодействия и обработки данных ДТС. Новая редакция Раздела 3 содержит последовательное описание действий ДТС инициатора запроса и ДТС проверяемого участника. |
| **8** | Таблица 4 и пункт 10 Приложения № 2 | Для устранения противоречий в новой редакции проекта правил предлагаем описание штампа времени в таблице 4 (поле ttp:ValidationTimeStamp) и пункте 10 приложения № 2 привести в соответствие с описанием поля responseTime таблицы 2 приложения № 1 | «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.» | Предлагаем исключить штамп времени ttp:ValidationTimeStamp, поскольку после ревизии структуры квитанции определено, что оно является в целом избыточным в связи с наличием в составе квитанции штампа времени xades:SignatureTimeStamp.Поле responseTime квитанции DVCS описывается в стандарте DVCS следующим образом: Аналогом поля responseTime в приложении № 2 являются следующие поля:* xades:SigningTime - аналог responseTime/ genTime
* xades:SignatureTimeStamp - аналог responseTime/timeStampToken

В связи с этим наличие дополнительного штампа времени ttp:ValidationTimeStamp в приложении № 2 представляется избыточным.Изначально штамп времени ttp:ValidationTimeStamp появился в тексте Правил в связи с дискуссией о необходимости разделять в явном виде моменты времени проверки ЭЦП и время формирования квитанции. С учетом того, что в связи с позицией сторон отказались от обязательного формирования штампа времени в квитанции ДТС проверяемого участника (время формирования квитанции фиксируется без использования штампа времени), то фиксация момента времени проверки ЭЦП с помощью штампа времени ttp:ValidationTimeStamp утратила свой смысл. |