**Предложения для реализации Правил признания ЭЦП для закупок**

В рамках разработки 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, со стороны Российской Федерации были подняты сопутствующие аспекты необходимые для реализации в рамках закупок.

1. **Построение защищенных каналов передачи данных между поставщиками и торговыми площадками.**

Предлагается рассмотреть возможность наделения УЦ службы ДТС правом выпускать TLS сертификаты (в соответствии с утверждённым криптографическим стандартом) для торговых площадок (в том числе других веб ресурсов в рамках ЕАЭС) для возможности построения защищенных каналов передачи данных с поставщиками.

При этом осуществить разработку программного клиента, который бы устанавливался на ПК поставщиков и во взаимодействии с национальными криптопровайдерами обеспечивал построение защищенного TLS канала передачи данных в одностороннем режиме.

Для разработки клиента необходимо будет определить поддерживаемые ОС и национальные криптопровайдеры.

Реализовать разработку клиента целесообразно поручить Комиссии для обеспечения его централизованной поддержки и развития в будущем. Исходные коды клиента будут передаваться уполномоченным органам государств-членов.

Тем самым в ЕАЭС для торговых площадок (в том числе других веб ресурсов) будет создана возможность организовать взаимодействие с поставщиками из государств-членов с построением защищенного канала передачи данных.

1. **Онлайн подписание электронных документов на торговой площадке**

Предлагается осуществить разработку плагина(-ов) для веб браузеров поставщиков поддерживающих национальные криптопровайдеры государств-членов для возможности онлайн подписания электронных документов на торговых площадках.

Для разработки плагина(-ов) необходимо будет определить поддерживаемые браузеры и национальные криптопровайдеры, а также технологии, используемые торговыми площадками.

Реализовать разработку плагина(ов) целесообразно также поручить Комиссии для обеспечения его централизованной поддержки и развития в будущем. Исходные коды плагина(ов) будут передаваться уполномоченным органам государств-членов.

Тем самым поставщик при помощи плагина в своем веб браузере сможет осуществлять онлайн подписание электронных документов при помощи национального криптопровайдера.

1. **Проверка ЭЦП конфиденциальных электронных документов и документов большого объема.**

На заседаниях рабочей группы в том числе поднимался вопрос о направлении в ДТС конфиденциальных электронных документов и документов большого объема. Данный вопрос является актуальным, так как, во-первых, ДТС является дополнительным звеном возможной утечки конфиденциальных электронных документов, во-вторых вероятней всего будет затрачивать продолжительное время на проверку ЭЦП для электронных документов большого объема.

Одним из решений данных аспектов может стать определение возможности отправки торговой площадкой в ДТС не самого электронного документа, а его хэш значения. На текущий момент данная реализация невозможна прежде всего в связи с использованием в государствах-членах разных стандартов.

В этой связи для трансграничного участия в закупках предлагается определить необходимость использования единого алгоритма хэширования при подписании электронных документов в рамках трансграничных закупок, не затрагивая при этом алгоритмы ЭЦП. Текущая ситуация показывает, что в Республике Казахстан, Кыргызской Республики и Российской Федерации юридическими лицами используются криптопровайдеры уже поддерживающие единый алгоритм хэширования. В Республике Армения используется американский стандарт SHA и Республике Беларусь национальный стандарт СТБ 34.101.77.

Поэтому определение единого алгоритма хэширования при подписании электронных документов в рамках трансграничных закупок потребует обеспечить его поддержку в криптопровайдерах Республики Армения и Республики Беларусь. Республика Беларусь в настоящий момент имеет техническую возможность добавить в национальный криптопровайдер AVEST поддержку единого алгоритма хэширования. Республика Армения в виду отсутствия национального криптопровайдера собственной разработки могла быть либо осуществить его разработку и функционирование соответствующего УЦ или использовать техническое решение одного из государств-члена.

Тем самым поставщик при помощи плагина и национального криптопровайдера подписывал электронные документы на торговой площадке на едином алгоритме хэширования и национальном стандарте ЭЦП. В таком случае у торговой площадки при помощи своего национального криптопровайдера появляется возможность работать с хэш значением электронного документа подписанного иностранным поставщиком и передавать его в ДТС вместо всего электронного документа. Это в свою очередь исключит необходимость передачи в ДТС конфиденциальных документов и существенно ускорит проверку ЭЦП со стороны ДТС.

При это нужно понимать, что в таком случае ДТС будет осуществлять подтверждение актуальности ЭЦП к хэш значению электронного документа, поэтому подтверждение ЭЦП электронного документа по факту будет осуществляться самоц торговой площадкой при помощи национального криптопровайдера и квитанции ДТС.

ДТС при этом предлагается сделать универсальным с возможностью проверки ЭЦП хэш значения, так ЭЦП электронного документа. Торговая площадка сможет сама решать что ей нужно отправлять в ДТС на проверку.

1. **Проверка полномочий подписанта электронного документа.**

Несмотря на то что проверка полномочий подписанта электронного документа не связана с проверкой ЭЦП, для многих получателей проверка полномочий может являться важным аспектов для работы с электронным документом. Учитывая различные системы проверки полномочий подписантов в государствах-членах и степень их внедрения на национальном уровне, создание единой, объединяющей системы на трансграничном уровне ЕАЭС является сложно выполнимой задачей. В этой связи наиболее простым и эффективным вариантом скорее всего является принятие решения о возможности выпуска отдельных сертификатов для участия в закупках на трансграничном уровне ЕАЭС национальными УЦ. В этом случае поставщик обращался бы в национальный УЦ, который в свою очередь проверял бы его полномочия и выдавал отдельный сертификат для участия в закупках на трансграничном уровне ЕАЭС. ДТС в свою очередь осуществлял свою прямую функцию по проверке ЭЦП и актуальности данного сертификата. В этом случае торговая площадка на основании квитанции ДТС сможет быть уверена в полномочиях подписанта электронного документа.

Для реализации данного варианта вероятно всего потребуется определение минимальных требований к сертификатам для участия в закупках на трансграничном уровне ЕАЭС со стороны Комиссии по согласованию с государствами-членами, с целью обеспечения последующей возможности идентификации данного сертификата со стороны торговой площадки. При этом порядок выдачи данных сертификатов национальными УЦ определялся бы национальным законодательством.

1. **Проверка актуального статуса поставщика.**

В идеале решение данного аспекта должно быть реализовано исключительно на национальном уровне в государствах-членах при управлении жизненным циклом сертификатов. Например, в Республике Казахстан при ликвидации юридического лица в автоматическом режиме отзываются все сертификаты, выпущенные на него. Тем самым сертификаты аннулированных юридических лиц просто не смогут пройти проверку через ДТС.

Альтернативным вариантом решения данного аспекта на трансграничном уровне ЕАЭС является создание открытого реестра статуса юридических лиц государств-членов в сети Интернет, в объеме информации достаточном для проверки торговыми площадками статуса поставщиков. Ведение и актуализация данного реестра возможна через реализацию общего процесса через ИИС ЕАЭС, при помощи которого государства-члены смогут направлять информацию в Комиссию для обеспечения реестра в актуальном состоянии.