**Предложение Департамента информационных технологий**

1. **Онлайн подписание электронных документов**

Предлагается осуществить разработку программного пакета для онлайн подписания электронных документов из веб-браузера с использованием криптопровайдеров государств-членов.

Состав программного пакета:

1. Расширение (плагин) для веб-браузера.
2. Подсистема взаимодействия с криптопровайдером – ПО для взаимодействия плагина веб-браузера с криптопровайдерами государств-членов по интерфейсу CryptoAPI или PKCS#11.

Типовая процедура предлагаемого онлайн-подписания электронных документов:

1. Пользователь переходит на веб-портал торговой площадки и инициирует процесс подписания документа, размещенного на портале.
2. Данные электронного документа с портала загружаются на ПЭВМ пользователя по протоколу http.
3. Веб-портал вызывает плагин для формирования электронной подписи.
4. Плагин вызывает подсистему взаимодействия с криптопровайдером для формирования ЭЦП.
5. Подсистема взаимодействия с криптопровайдером с помощью национального криптопровайдера государств-члена выполняет формирование ЭЦП в заранее определенном формате (XAdES, CAdES и др.) и возвращается результат плагину веб-браузера.
6. Сформированная ЭЦП загружается на сервер торговой площадки.

Реализация программного пакета позволит поставщику осуществлять онлайн подписание электронных документов при помощи национального криптопровайдера своего государств-члена.

Для работы программного пакета требуется:

1. Веб-браузер на платформе Chromium (Microsoft Edge, Google Chrome, Яндекс Браузер и др.) или Mozilla Firefox, которые поддерживают технологию Native Messaging – взаимодействие веб-браузера с ПО на ПЭВМ пользователя.
2. Интегрировать в интернет-портал торговой площадки функционал взаимодействия с плагином для подписания электронных документов.
3. Криптопровайдеры государств-членов должны поддерживать программный интерфейс CryptoAPI или PKCS#11.

Для разработки программного пакета предлагается определить конечные перечни национальных криптопровайдеров, веб-браузеров, стандарты хранения ЭЦП, которые будут применяться поставщиками.

Реализовать разработку программного пакета, поддерживающего все криптопровайдеры государств-членов можно при помощи привлечения компаний разработчиков данных криптопровайдеров, либо поручить Комиссии осуществить данную разработку и обеспечивать его поддержку и развитие в будущем. Тем самым в ЕАЭС для торговых площадок (в том числе других веб-ресурсов) будет создана возможность организовать взаимодействие с поставщиками из государств-членов с использованием ЭЦП.

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

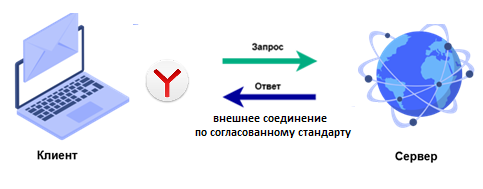
Предлагается рассмотреть возможность создания отдельного международного УЦ ЕАЭС для выпуска TLS сертификатов (в соответствии с утверждённым стандартом) для торговых площадок (в том числе других веб-ресурсов) для возможности построения защищенных каналов передачи данных с поставщиками.

В качестве альтернативы могут использоваться сертификаты, выпускаемые национальным УЦ одного из государств – членов, в этом случае необходимо принятие соответствующего решения.

По мнению Комиссии, создание международного УЦ ЕАЭС является более перспективным для развития ЕАЭС.

Установка защищенного канала передачи данных по протоколу TLS может осуществляться в порядке односторонней или двусторонней аутентификации. При односторонней аутентификации на ПЭВМ поставщика проверяется TLS сертификат торговой площадки (или другого веб ресурса). При обеспечении выпуска TLS сертификатов для поставщиков из государств-членов ЕАЭС будет возможность аутентификации торговыми площадками (в том числе другими веб-ресурсами) поставщиков в порядке двусторонней аутентификации по протоколу TLS.

При использовании на ПЭВМ поставщика браузеров, уже поддерживающих согласованный криптографический стандарт службы ДТС, ничего дополнительно делать не придется. ПЭВМ поставщика через браузер будет сразу устанавливать защищенное соединение с сервером торговой площадки. Поддержку стандартов ГОСТ, например, обеспечивают Яндекс Браузер, Chromium-Gost, ГосБраузер, Sputnik Browser.

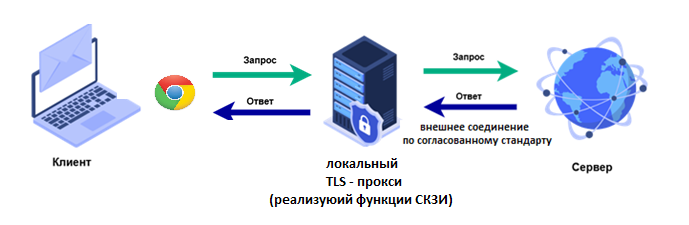


В случае необходимости использования на ПЭВМ поставщика браузеров, не поддерживающих согласованный стандарт, предлагается для обеспечения возможности построения защищенных каналов передачи данных между поставщиками и торговыми площадками разработать программный пакет TLS-прокси (реализующий функции СКЗИ) для установки на ПЭВМ поставщика. Программный пакет позволяет, осуществляя поддержку согласованных браузеров на ПЭВМ поставщиков, устанавливать соединение по протоколу TLS с использованием утвержденных стандартов шифрования, обеспечивая защищенный канал передачи данных с торговой площадкой (в том числе другими веб-ресурсами). При этом программный пакет TLS-прокси также будет предоставлять возможность аутентификации поставщика с использованием ключевых носителей (при необходимости).

Для разработки программного пакета предлагается определить конечные перечни ОС и браузеров, используемыми поставщиками.

Реализовать разработку программного пакета TLS-прокси можно при помощи национальных компаний разработчиков ПО в случае их заинтересованности, либо поручить Комиссии осуществить данную разработку. При этом исходные коды программного пакета TLS-прокси при необходимости будут передаваться в уполномоченные органы 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 по согласованному криптостандарту с использованием основных мировых браузеров.



Программный пакет TLS-прокси будет обеспечивать безопасное соединение с использованием туннелей по протоколам TLS v1.2 и TLS v1.3. Туннели, создаваемые программным пакетом, обеспечивают защищенный доступ к сетевым ресурсам, а также предоставляют возможность аутентификации на этих сетевых ресурсах. Когда служба программного пакета TLS-прокси будет запущена и активна на ПЭВМ поставщика, браузер будет через него устанавливать защищенное TLS соединение с сервером, используя шифронаборы утвержденного криптостандарта.