Приложение №6 к Регламенту

## Приложение №11. Реализуемые функции Сервиса электронной подписи

**Реализуемые функции Сервиса электронной подписи**

1. **Назначение сервиса**

Сервис электронной подписи ООО «КРИПТО-ПРО» (СЭП) предназначен для централизованного:

1. Хранения ключей электронной подписи Пользователей Удостоверяющего центра.

2. Создания и проверки электронной подписи электронных документов различного формата криптографических сообщений.

3. Взаимодействия Операторов и Пользователей Удостоверяющего центра с Удостоверяющим центром для управления сертификатами ключей проверки электронной подписи.

1. **Поддерживаемые форматы и стандарты**

Электронная подпись создается с использованием криптографических алгоритмов в соответствии с ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» и ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

Поддерживаемые форматы криптографических сообщений:

1. «Чистая» (необработанная) Электронная подпись ГОСТ 34.10 – 2001, ГОСТ 34.10 – 2012;

2. Усовершенствованная подпись в соответствии с ETSI TS 101 733 "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)", рекомендациями RFC 5652, "Cryptographic Message Syntax" (CAdES-BES и CAdES-X Long Type 1);

3. Подпись XML-документов (XML Digital Signature, XMLDSig);

4. Подпись документов PDF (Open Document Format);

5. Подпись документов Microsoft Office (Office Open XML).

1. **Используемые средства электронной подписи**

Для хранения ключей электронной подписи Пользователей Удостоверяющего центра, создания электронной подписи электронных документов в составе Сервиса электронной подписи используется сертифицированное средство электронной подписи ПАКМ «КриптоПро HSM».

Для проверки электронной подписи электронных документов используется сертифицированное средство электронной подписи СКЗИ «КриптоПро CSP».

1. **Предоставление доступа к сервису**

Доступ к Сервису электронной подписи осуществляется круглосуточно в режиме 24х7 по каналам связи посредством Веб-интерфейса, предоставляемого Исполнителем, или Прикладного интерфейса, используемого для подключения Информационных систем Уполномоченной организации в соответствии руководством разработчика программного обеспечения «КриптоПро DSS».

Аутентификация пользователей осуществляется с использованием штатного Центра идентификации в составе ПАК «КриптоПро DSS» или по протоколу SAML (WS Security) или OpenID с использованием Стороннего центра идентификации Уполномоченной организации, подключаемого к Сервису электронной подписи в соответствии с документацией на программное обеспечение «КриптоПро DSS».

Руководства доступны по адресу <https://www.cryptopro.ru>.

Вторичная аутентификация пользователей осуществляется посредством ключа аутентификации в мобильном приложении (программе для ЭВМ) «КриптоПро DSS Client» из состава ПО «Модуль аутентификации DSS Client для ПАК «КриптоПро DSS» версии 2.0» на устройствах Пользователей УЦ; одноразового кода, высылаемого Пользователям УЦ в информационном сообщении или формируемого с помощью ОТР-токена.

Допускается прерывание функционирования СЭП для проведения плановых регламентных работ не более чем на 1 час. В случае возникновения внештатных ситуаций восстановление функционирования СЭП осуществляется в течение 1 часа рабочего времени.

1. **Информирование Пользователей Удостоверяющего центра**

СЭП позволяет информировать Пользователей Удостоверяющего центра посредством отправки информационных сообщений, содержащих сведения о подключении к СЭП и подписываемых электронных документах от имени Пользователя Удостоверяющего центра, выполняемых операциях с ключом электронной подписи, принадлежащих Пользователю Удостоверяющего центра.

1. **Защита информации**

Защита от несанкционированного доступа ключей электронной подписи пользователей осуществляется с использованием сертифицированного средства криптографической защиты информации ПАКМ «КриптоПро HSM».

Защита информации, передаваемой при подключении Информационной системы, осуществляется Уполномоченной организацией с использованием средств криптографической защиты, совместимых со средствами Удостоверяющего центра.

Защита аутентификационной информации, передаваемой при подключении Стороннего центра идентификации, осуществляется Уполномоченной организацией с использованием средств криптографической защиты, совместимых со средствами Удостоверяющего центра.

Защита информации, передаваемой при подключении SMS-шлюза, осуществляется Уполномоченной организацией с использованием средств криптографической защиты, совместимых со средствами Удостоверяющего центра. Обеспечение информационной безопасности подтверждается аттестатом соответствия объекта информатизации автоматизированной системы Сервиса электронной подписи требованиям по защите информации от несанкционированного доступа.

1. **Правила пользования Сервисом электронной подписи**

Ключи электронной подписи формируются в СЭП в неэкспортируемом формате, т.е. недоступном для сохранения и использования на съемных ключевых носителях и рабочем месте пользователя.

При создании ключа электронной подписи в СЭП Пользователем Удостоверяющего центра может быть установлен индивидуальный PIN-код доступа к ключевому контейнеру, содержащему ключ электронной подписи.

Создание сертификата ключа проверки электронной подписи для использования в СЭП осуществляться подключенным к СЭП Удостоверяющим центром.

Использование ключа электронной подписи в СЭП должно подтверждаться владельцем соответствующего сертификата ключа проверки электронной подписи (Пользователем УЦ) с помощью ключа аутентификации в мобильном приложении (программе для ЭВМ) «КриптоПро DSS Client» на устройстве Пользователя УЦ; или одноразового пароля, формируемого персональным ОТР-токеном владельца сертификата ключа проверки электронной подписи или высылаемого в информационном сообщении на указанный при регистрации Пользователем УЦ мобильный телефон владельца сертификата ключа электронной подписи Пользователя УЦ, а также (опционально) индивидуальным PIN-кодом доступа к ключевому контейнеру, содержащему используемый ключ электронной подписи.

Пользователь Удостоверяющего центра должен хранить в тайне индивидуальный PIN код доступа к ключевому контейнеру, аутентификационную информацию, обеспечить сохранность персональных средств аутентификации (ключ аутентификации для мобильного приложения (программы для ЭВМ) «КриптоПро DSS Client», ОТР-токен, мобильный телефон и SIM-карту для получения одноразового пароля), используемые для подтверждения использования ключа электронной подписи для подписания электронного документа, принимать все возможные меры для предотвращения их потери, раскрытия и несанкционированного использования.

Пользователь Удостоверяющего центра обязан немедленно обратиться к Оператору СЭП с заявлением на прекращение действия соответствующего сертификата ключа проверки электронной подписи в случае раскрытия, искажения персонального ключа электронной подписи, компрометации аутентификационной информации и утери специальных устройств, используемых для аутентификации (ключа аутентификации для мобильного приложения (программы для ЭВМ) «КриптоПро DSS Client», мобильного телефона, SIM-карты и (или) ОТР-токена), а также в случае, если Пользователю Удостоверяющего центра стало известно, что этот ключ электронной подписи используется или использовался ранее другими лицами, в том числе если Пользователь УЦ получил сообщение от СЭП о выполнении каких-либо операций от его имени в то время, когда он их не выполнял.

На рабочих местах Пользователей Удостоверяющего центра должны использоваться сертифицированные средства антивирусной защиты в соответствии с эксплуатационной документацией.

1. **Аудит Сервиса электронной подписи**

Регистрация всех операций, выполняемых Операторами и Пользователями Удостоверяющего центра, осуществляется средствами СЭП. Журналы аудита выгружаются средствами СЭП и используются для контроля и анализа выполненных операций при разборе спорных вопросов и разрешении конфликтных ситуаций. Оператор СЭП доступ к журналу аудита имеет посредством Веб-интерфейса, предоставляемого Удостоверяющим центром.