Сервис облачной криптографии ООО «Такском»

Сервис облачной криптографии (далее – СОК) - специально разработанный и сопровождаемый ООО «Такском» сервис, реализованный на базе программного обеспечения «Такском-ISS», правообладателем которого является ООО «Такском», установленного на технических средствах ООО «Такском» на территории РФ. СОК предназначен для защищенного хранения на технических средствах ООО «Такском» ключей электронной подписи (ЭП) и удалённого осуществления криптографических операций с использованием ключей ЭП.

Для использования СОК требуется специальный ключ ЭП, который записывается и хранится в индивидуальной ячейке в течение срока действия сертификата. Ключ ЭП помещается на хранение в защищенную ячейку в момент изготовления и не может быть изъят из ячейки. Воспользоваться ключом ЭП можно, имея приложение, совместимое с СОК, и зная параметры доступа к ключу ЭП.

СОК обеспечивает надежный уровень безопасности от несанкционированного доступа к ключу ЭП и дополнительный контроль владельца за использованием ключа (с помощью одноразовых паролей и других методов контроля).

Использование ключа ЭП производится в соответствии с пользовательской документацией по работе с облачной подписью на приложение, которое использует клиент. Перечень приложений, совместимых с СОК, уточняйте на сайте ООО «Такском».

Функционал СОК:

- размещение ключа электронной подписи в индивидуальной защищенной ячейке на технических средствах ООО «Такском»;
- хранение ключа ЭП в ячейке в течение срока действия сертификата;
- управление доступом к ключу ЭП (параметрами доступа), параметры доступа назначаются пользователем:
    - логин и пароль для доступа к ячейке (непосредственно пароль в СОК не хранится);
    - ПИН-код к ключу ЭП (непосредственно ПИН-код в СОК не хранится);
- обеспечение доступа к ячейке при вводе параметров доступа;
- выполнение операций с использованием ключа ЭП (создание ЭП, расшифровывание) по запросу;
- аутентификация запроса средствами СОК;
- подтверждение владельцем ключа запроса на создание ЭП с помощью одноразового пароля.

Обработка запроса на использование ключа ЭП с подтверждением запроса с помощью одноразового пароля, получаемого по SMS:

- СОК производит аутентификацию запроса на использование ключа ЭП (проверяется соответствие параметров доступа);
- СОК формирует уникальный случайный код аутентификации (одноразовый пароль) и вместе с сопроводительной информацией отправляет в форме SMS-сообщения на номер мобильного телефона владельца ключа – для получения подтверждения запрашиваемой операции;
- сформированный код аутентификации сохраняется в СОК вместе с видом запрашиваемой операции (создание ЭП, расшифровывание);
- владелец сертификата, используя код аутентификации, подтверждает запрос на операцию с ключом ЭП
- после получения подтверждения запроса на создание ЭП, на указанной владельцем ключа адрес электронной почты направляется электронное письмо, содержащее файл ЭП.