Порядок использования комплектаций ПАКМ «КриптоПро HSM» с компонентой «КриптоПро DSS» для работы с квалифицированной электронной подписью

- Пользователь заключает с Оператором DSS Договор об оказании услуг DSS и передаёт Оператору DSS заявление на создание ключа ЭП и запроса на СКПЭП на бумажном носителе с собственноручной подписью. В заявлении содержится:
  - поручение инициировать генерацию ключа ЭП в ПАКМ «КриптоПро HSM», к которому подключен компонент «КриптоПро DSS», и осуществлять эксплуатацию данного HSM, в котором находится ключ пользователя, а также компонента «КриптоПро DSS» в соответствии с документацией на данные СКЗИ (в частности, с учетом запрета подключения DSS к средствам УЦ);
  - поручение создать запрос на выпуск СКПЭП для пользователя в электронном виде и подписать его УКЭП Оператора DSS;
  - поручение сформировать и сохранить ключ аутентификации на личный ключевой носитель Пользователя.
- Ответственный сотрудник Оператора DSS с использованием штатных средств компонент «КриптоПро DSS» после аутентификации по своему личному ключу осуществляет следующие действия:
  - создаёт учётную запись Пользователя в DSS;
  - заполняет данные Пользователя на основании предоставленных заявительных документов;
  - инициирует генерацию ключа ЭП в ПАКМ «КриптоПро HSM», к которому подключен компонент «КриптоПро DSS» с формированием запроса в электронном виде на создание СКПЭП, соответствующего ключу ЭП в ПАКМ «КриптоПро HSM»;
  - запрос в виде файла сохраняется на съёмном носителе;
  - с использованием СКЗИ, установленного на рабочем месте ответственного сотрудника Оператора DSS, создаёт ключ аутентификации на личном ключевом носителе Пользователя, регистрирует данный ключ в DSS как личный ключ аутентификации данного Пользователя, передаёт носитель с ключом аутентификации Пользователю;
  - Распечатывает заявление на регистрацию средства аутентификации, в котором указан уникальный идентификатор ключа аутентификации Пользователя;
  - Оператору DSS запрещается копировать ключи аутентификации пользователей.
- Пользователь подписывает заявление на регистрацию средства аутентификации собственноручной подписью, оставляет заявление Оператору DSS.
- При наличии Договора между Оператором DSS и УЦ (существенным условием которого является поручение от УЦ Оператору DSS устанавливать личность Заявителя, после чего принимать у Заявителя заявительные документы, предоставленные для создания сертификата ключа проверки ЭП, и предоставлять эти документы в УЦ) ответственный сотрудник Оператора DSS, посещает УЦ и предоставляет:
  - заявление о присоединении к Договору на обслуживание в УЦ от имени пользователя;
  - заявление на выпуск СКПЭП на бумажном носителе, подписанное Пользователем, вместе с комплектом необходимых документов для подтверждения информации, заносимой в СКПЭП, и доверенностью Пользователя;
  - съёмный носитель, содержащий запрос на СКПЭП Пользователя в электронном виде;
  - иные документы, предоставленные Пользователем, подтверждающие сведения, заносимые в СКПЭП.

  В данном случае Пользователь в дальнейшем посещает Оператора DSS для получения Заявления о присоединении к Договору на оказание услуг УЦ с отметкой УЦ.
- При отсутствии Договора между Оператором DSS и УЦ (существенным условием которого является поручение от УЦ Оператору DSS устанавливать личность Заявителя, после чего принимать у Заявителя заявительные документы, предоставленные для создания сертификата ключа проверки ЭП, и предоставлять эти документы в УЦ) пользователь в соответствии с установленным порядком, в том числе Регламентом УЦ (лично или третье лицо по доверенности Пользователя), посещает УЦ и предоставляет необходимые для выпуска СКПЭП документы, включая запрос на СКПЭП в электронном виде. В данном случае в дальнейшем после получения от ответственного сотрудника УЦ СКПЭП Пользователь посещает Оператора DSS для передачи ответственному сотруднику Оператора DSS данного СКПЭП.
- Пользователь с использованием клиентского СКЗИ (той версии, что указана в исполнении DSS КриптоПро HSM в его сертификате) и ключа аутентификации на его съемном носителе осуществляет в соответствии с документацией аутентифицированный доступ к серверным компонентам КриптоПро HSM/DSS для использования своего КЭП.