Памятка пользователю средств электронной подписи

Памятка разработана в соответствии с требованиями закона Донецкой Народной Республики «Об информации и информационных технологиях» и закона Донецкой Народной Республики «Об электронной подписи», а также эксплуатационной документации на сертифицированные средства криптографической защиты информации (далее - СКЗИ).

ГП «Почта Донбасса» является Аккредитованным Удостоверяющим Центром (далее – АУЦ) Донецкой Народной Республики. Аккредитация выдана согласно приказа Министерства связи Донецкой Народной Республики от 27.11.2017 года № 373 «О внедрении программного комплекса Головного Удостоверяющего Центра».

В соответствии с требованиями законодательства Донецкой Народной Республики электронная подпись выдается физическому или юридическому лицу без права передачи.

Выпуская сертификат на Ваше имя, АУЦ выступает в качестве третьей доверенной стороны защищенного электронного взаимодействия и подтверждает, что открытый криптографический ключ, указанный в Вашем сертификате, принадлежит Вам, и соответствует закрытому ключу, имеющемуся только у Вас. Кроме того, в сертификате в соответствии с требованиями закона Донецкой Народной Республики «Об электронной подписи» указывается необходимая информация, позволяющая идентифицировать Вас как участника защищенного электронного взаимодействия.

С помощью сертификата Вы можете совершать юридически значимые действия в системах электронного документооборота, а также другие действия в информационно-телекоммуникационных системах: защита соединений в Интернет для проверки подлинности сервера и клиента, шифрование и т. п.

Вы должны осознавать, что все функции сертификата могут быть обеспечены только при условии сохранения Вами в тайне Вашего закрытого ключа. В связи с этим, обращаем Ваше внимание на некоторые правила пользования сертификатом.

1. Термины и определения

Удостоверяющий центр - юридическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Законом ДНР «Об электронной подписи».

Аккредитация удостоверяющего центра (сокращенное наименование – АУЦ) - признание республиканским органом исполнительной власти, уполномоченным в сфере использования электронной подписи соответствия удостоверяющего центра требованиям Закона ДНР «Об электронной подписи».

Электронная подпись (далее - ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Квалифицированный сертификат ключа проверки электронной подписи (далее - сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром.

Ключ электронной подписи (крипто ключ) – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Носитель ключевой информации – носитель, содержащий криптоключ.

Средства криптографической защиты информации (СКЗИ) – средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов, ключевые документы.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном законодательством порядке выдан сертификат ключа проверки электронной подписи.

Компрометация криптографических ключей – потеря, разглашение, несанкционированное копирование и другие действия, в результате которых криптографические ключи могут стать доступными посторонним лицам.

2. Взаимодействие с АУЦ

АУЦ выпускает сертификаты в порядке, определенном Регламентом АУЦ Донецкой Народной Республики.

Пользователь может обращаться в АУЦ в рабочий день в промежуток времени с 8.00 до 17.00 с понедельника по четверг и с 8.00 до 16.00 в пятницу, за исключением выходных и праздничных нерабочих дней согласно законодательству Донецкой Народной Республики.

Пользователь должен своевременно сообщать об изменении атрибутов (параметров), в том числе включаемых в сертификат (изменение ФИО, паспортных данных, ИНН и т.д.).

При разрешении конфликтных ситуаций, связанных с установлением подлинности и/или авторства спорного документа или иных конфликтных ситуаций, связанных с использованием ЭП, Пользователь вправе предоставить АУЦ, все документы и материалы, относящиеся к предмету конфликтной ситуации.

Более подробную информацию Вы можете получить в АУЦ Донецкой Народной Республики, по адресу: 283001, г. Донецк, ул. Артема, д. 72, тел. (062) 303-36-46, Феникс 450, эл. адрес: ovfu@postdonbass.com.

3. Рекомендации по обращению с ключевой информацией и ключевыми носителями

Недопустимо пересылать файлы с ключевой информацией для работы в системах обмена электронными документами по электронной почте сети Интернет или по внутренней электронной почте (кроме запросов на сертификат и открытых ключей).

Работать со средствами электронной подписи необходимо на персональном компьютере не доступном для доступа третьих лиц.

В случае невозможности обеспечить безопасность компьютера с установленным программным обеспечением для работы с электронной подписью необходимо придерживаться следующих правил безопасности:

1. Ключевая информация должна размещаться на сменном носителе информации (USB-flash накопитель). Не рекомендуется размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами электронной подписи и средствами криптографической защиты, т.к. данное действие способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

2. Носители ключевой информации должны использоваться только их владельцем либо уполномоченным лицом на использование данного носителя, и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

3. Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами электронной подписи и средствами криптографической защиты операций формирования и проверки электронной подписи,

шифрования и расшифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

4. Пользователю запрещается:

   - осуществлять несанкционированное копирование ключевых носителей;
   - вносить какие-либо изменения в программное обеспечение СКЗИ;
   - изменять настройки, установленные программой установки СКЗИ или администратором;
   - разглашать состав информации на собственном носителе ключевой информации или пароль доступа к нему, а также передавать этот носитель другим лицам, выводить значение личных криптоключей и других ключевых данных на дисплей, принтер или другие средства визуального отображения информации;
   - записывать на носители ключевой информации другую информацию кроме такой, которая предусмотрена для функционирования программного комплекса;
   - оставлять криптоключ в считывателе после окончания работы с ним;
   - оставлять персональный компьютер без контроля включенным, либо незаблокированным (средствами операционной системы), после считывания криптоключа;
   - пользователь несет ответственность за хранение собственного носителя ключевой информации и пароля доступа к нему.

4. Порядок действий пользователя при компрометации криптоключей и носителей ключевой информации

Прекратить обмен электронными документами с использованием скомпрометированных ключей.

В случае компрометации ключевых данных, утери носителя ключевой информации или возникновения обоснованного подозрения относительно такой компрометации пользователь немедленно сообщает об этом в АУЦ, и действует в соответствии с указаниями ответственного лица и согласно Регламенту работы АУЦ.

Пользователь, допустивший компрометацию собственных криптоключей, несет полную ответственность за ущерб связанный с их использованием, а также за все издержки, связанные с генерацией новых ключей, их сертификацией и вводом в действие.