Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

Сведения об аккредитованном Удостоверяющем центре:
Общество с ограниченной ответственностью «АйТи Мониторинг»
Фактический адрес: 350051, г. Краснодар, ул. Рашпилевская, д.287
Тел.: 8 (800) 770-01-31; E-mail: support@e-signature.pro
https://e-signature.pro/

Настоящее Руководство предназначено для обязательного ознакомления использующих средства электронной подписи владельцев сертификатов ключей проверки электронной подписи, выданных Удостоверяющим центром «АйТи Мониторинг» (далее - УЦ).

1. Термины и определения

Квалифицированный сертификат ключа проверки электронной подписи - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом № 63-ФЗ от 06.04.2011 г. «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган), и являющийся в связи с этим официальным документом;

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном Федеральным законом № 63-ФЗ от 06.04.2011 г. «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи;

Электронная подпись - 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;

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

АРМ - автоматизированное рабочее место; совокупность аппаратных и программных средств, позволяющая автоматизировать бизнес-процессы и повысить эффективность работы.

2. Обязанности владельца сертификата ключа проверки электронной подписи

2.1. Обеспечивать конфиденциальность своих ключей электронной подписи, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия.

2.2. Не использовать ключ электронной подписи, сертификат которой выдан УЦ, и немедленно обратиться в УЦ с заявлением об аннулировании сертификата, при наличии оснований полагать, что конфиденциальность этого ключа электронной подписи нарушена.

2.3. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление, на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.

2.4. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

2.5. Обеспечивать незамедлительное уничтожение принадлежащих ему ключей электронных подписей по истечении сроков действия данных ключей в отношении усиленных квалифицированных электронных подписей. Для уничтожения ключей электронных подписей должны применяться прошедшие в установленном порядке процедуру оценки соответствия средства электронной подписи, в составе которых реализована функция уничтожения информации.

3. Порядок применения средств квалифицированной электронной подписи

3.1. Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи.

3.2. Для предотвращения заражения компьютера с установленными средствами усиленной электронной подписи необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского программного обеспечения и других вредоносных программ антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления антивирусных баз.

3.3. Помещения, в которых установлены средства квалифицированной электронной подписи или хранятся носители ключей электронной подписи должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

3.4. Используемые или хранимые средства квалифицированной электронной подписи, эксплуатационная и техническая документация к ним, носители ключей проверки электронной подписи подлежат учету в соответствии с требованиями Приказа ФАПСИ от 13 июня 2001 г. № 152.

4. Настройка АРМ для работы с электронной подписью

4.1. На рабочем месте должны быть установлены сертифицированные средства электронной подписи и, при необходимости, соответствующие системные драйвера, обеспечивающие работу с имеющимися у владельца сертификата ключевыми носителями.

4.2. Для корректной настройки АРМ владелец сертификата ключа проверки электронной подписи может обратиться в техническую поддержку УЦ по адресу электронной почты support@e-signature.pro.