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: ca@docshell.ru
https://e-signature.pro

Настоящее Руководство предназначено для обязательного ознакомления Пользователей Удостоверяющего центра «АйТи Мониторинг», использующих средства электронной подписи.

1. Термины и определения

Квалифицированный сертификат ключа проверки электронной подписи - сертификат ключа проверки электронной подписи, соответствующий требованиям, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи;

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом 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 ключа проверки электронной подписи

2.1. Обеспечить конфиденциальность ключей проверки электронных подписей.

2.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.

2.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

2.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи, если такие ограничения были установлены.

2.5. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

2.6. 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.

2.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено.

2.8. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

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 должен быть установлен сертифицированный криптопровайдер; драйвера, обеспечивающие работу с электронными ключами. ВНИМАНИЕ! Перед установкой драйвера, убедитесь, что электронный ключ не вставлен в разъем компьютера.
4.2. ВАЖНО! Не использовать электронную подпись непредназначенную для работы с ЕГАИС на ПК с установленной программой УТМ (Универсальный Транспортный Модуль).