Документы, необходимые для получения квалифицированного сертификата электронной подписи:

Физическому лицу (Гражданину РФ):

→ Российский паспорт (оригинал или заверенная копия);
→ Заявление на выдачу сертификата (только оригинал);
→ Страховое свидетельство Пенсионного Фонда (СНИЛС) (оригинал или заверенная копия);
→ Свидетельство ИНН.

Юридическому лицу (в качестве владельца указана организация и генеральный директор организации):

→ Российский паспорт генерального директора (оригинал или заверенная копия);
→ Заявление на выдачу сертификата генерального директора (только оригинал);
→ Страховое свидетельство Пенсионного Фонда (СНИЛС) генерального директора (оригинал или заверенная копия);
→ Свидетельство ИНН генерального директора.

Юридическому лицу (в качестве владельца указана организация и уполномоченное лицо)*:

→ Российский паспорт уполномоченного лица (оригинал или заверенная копия);
→ Заявление на выдачу сертификата уполномоченного лица (только оригинал);
→ Страховое свидетельство Пенсионного Фонда (СНИЛС) уполномоченного лица (оригинал или заверенная копия);
→ Свидетельство ИНН уполномоченного лица;
→ Доверенность на право подписи (оригинал или заверенная копия);
→ Доверенность на получение сертификата (оригинал или заверенная копия).

* Применение электронной подписи регулируется федеральным законом "Об электронной подписи" от 06.04.2011 N 63-ФЗ

Способы идентификации личности

Удостоверяющий центр обязан провести идентификацию вашей личности – в вашем присутствии либо дистанционно. Дистанционно – при наличии у вас действующей квалифицированной электронной подписи, биометрического паспорта гражданина, подтвержденной учетной записи на Едином портале государственных и муниципальных услуг (Госуслуги) или учетной записи в Единой биометрической системе России (ЕБС).

Как получить и использовать квалифицированную электронную подпись?

Для получения сертификата электронной подписи вам необходимо обратиться в удостоверяющий центр – специализированную организацию, аккредитованную Министерством цифрового развития, связи и массовых коммуникаций, заполнить заявление и предоставить **необходимые документы.**

Пройдя **идентификацию** вашей личности, удостоверяющий центр создаст **ключевую пару,** запишет закрытый ключ на **ключевой носитель,** и выдаст вам сертификат ключа проверки электронной подписи, который подтверждает, что вы являетесь владельцем сертификата и электронной подписи.

Если вы используете программно-аппаратный ключевой носитель, вы можете самостоятельно создать ключевую пару, и предоставить ее в удостоверяющий центр и получить в нем ваш сертификат ключа проверки электронной подписи.

Для подписания электронных документов электронной подписью необходимо использовать специализированную программу – **средство электронной подписи.**

ИНТЕРНЕТ-ВЕРСИЯ

→ **Электронная подпись** – это аналог собственноручной подписи для подписания электронных документов.

→ **Ключевая пара** – это набор из открытого и закрытого ключей электронной подписи, однозначно привязанных к друг другу.

→ **Открытый ключ** (ключ проверки электронной подписи) это уникальный набор символов (байт), сформированный средством электронной подписи и однозначно привязанный к закрытому (секретному) ключу. Открытый ключ необходим для того, чтобы любой желающий мог проверить электронную подпись на электронном документе. Он передается получателю электронного документа в составе файла электронной подписи и может быть известен всем.

→ **Закрытый** (секретный) **ключ** электронной подписи – это уникальный набор символов (байт), сформированный средством электронной подписи. Используется для формирования самой электронной подписи на электронном документе и хранится в зашифрованном виде на ключевом носителе. Доступ к закрытому ключу защищен PIN-кодом и его нужно хранить в секрете.

→ **Сертификат ключа проверки электронной подписи** (сертификат электронной подписи, квалифицированный сертификат электронной подписи) – это электронный и бумажный документ, который подтверждает связь электронной подписи с ее владельцем (человеком или организацией). Сертификат содержит сведения о его владельце, открытый ключ, информацию о сроке действия сертификата, информацию о выдавшем электронную подпись удостоверяющем центре, серийный номер сертификата и иные сведения.

→ **Ключевой носитель** – это устройство для хранения закрытого ключа. Ключевой носитель внешне напоминает "флешку" для компьютера, но отличается по своим свойствам: память у него защищена паролем (PIN-кодом). Может иметь встроенное средство электронной подписи. В этом случае он является программно-аппаратным ключевым носителем и позволяет максимально безопасно формировать электронную подпись на электронном документе.

→ **Средство электронной подписи** – это программно-аппаратное или только программное средство, предназначенное для создания ключевой пары, формирования и проверки электронной подписи на электронном документе. Его еще называют "криптопровайдером" или СКЗИ (средством криптографической защиты информации). Устанавливается на компьютерное устройство (мобильный телефон, смартфон, компьютер, планшет) или на ключевой носитель.

Формирование электронной подписи

При подписании электронного документа формируется уникальный набор символов (хэш-код), однозначно привязанный к содержанию электронного документа и созданный средством электронной подписи путем обработки этого электронного документа с помощью криптографического преобразования (хэш-функции). Такой уникальный набор символов неразрывно связан с электронным документом: если в текст добавят незаметно для вас, например, пробел, электронный документ уже не будет соответствовать этому уникальному набору символов.

Средство электронной подписи шифрует уникальный набор символов (хэш-код) используя ваш закрытый ключ. Зашифрованный уникальный набор символов и есть электронная подпись на электронном документе. Она может быть как встроенной в электронный документ, так и отсоединенной от него и преобразованной в отдельный файл.

Направляя адресату подписанный электронный документ, необходимо направлять также ваш сертификат ключа проверки электронной подписи, который содержит открытый ключ, чтобы адресат (получатель) мог проверить авторство и неизменность документа.

Проверка электронной подписи

Для проверки электронной подписи получатель документа использует средство электронной подписи, которое:

→ расшифровывает уникальный набор символов (хэш-код), содержащийся в электронной подписи электронного документа;

→ формирует уникальный набор символов путем обработки проверяемого электронного документа с помощью различных криптографических алгоритмов;

→ сравнивает указанные выше уникальные наборы символов (хэш-коды). Их соответствие друг другу является подтверждением того, что в проверяемый электронный документ не вносились изменения после его подписания электронной подписью;

→ проверяет соответствие электронной подписи в электронном документе и направленном вместе с ним сертификате ключа проверки электронной подписи, подтверждая авторство электронного документа;

→ Если хотя бы одна из проверок завершится с ошибкой, средство электронной подписи сообщит, что электронная подпись на электронном документе недействительна и авторство электронного документа не подтверждено.

Как получить и использовать квалифицированную электронную подпись?

Для получения сертификата электронной подписи вам необходимо обр[illegible] удосто[illegible]ющий центр, специализирующ[illegible]ющих, в оказании [illegible] Министерством цифр[illegible]вития, связи [illegible] массовых коммуникаций, запол[illegible]явление и предоставить **необходимые документы.**

Провед[illegible] удостов[illegible] запиш[illegible] и выдас[illegible] подписи, [illegible] владельцем сертификата и электронной подписи.

Если вы используете программно-аппаратный ключевой носитель, вы можете самостоятельно создать ключевую пару и предоставить ее в удостоверяющий центр и получить в нем ваш сертификат ключа проверки электронной подписи.

Для подписания электронных документов электронной подписью необходимо использовать специализированную программу – **средство электронной подписи.**



ФЕДЕРАЛЬНАЯ НАЛОГОВАЯ СЛУЖБА

Вы получили квалифицированный сертификат электронной подписи?



Будьте внимательны и осторожны!

Электронная подпись – это аналог собственноручной подписи, ключ к вашему имуществу, деньгам и репутации!