**Электронная подпись: что это такое и как с ней обращаться?**

**(Пособие для «чайников»)**

1. Все утверждения данной статьи направлены только на достижение ограниченной цели: донести хоть и узкое, но не искажённое произвольными терминологией и трактовкой понятий понимание принципов применения электронной подписи широким кругом пользователей, не являющихся подготовленными или опытными специалистами в этой сфере деятельности. Следствием получения означенных знаний должна стать **теоретическая основа** для получения пользователями прочных **навыков** применения электронной подписи.

2. Основным нормативным документом, определяющим применение электронной подписи, а также деятельность удостоверяющих центров в Российской Федерации, является Федеральный закон [от 6 апреля 2011 года № 63-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_112701/) «Об электронной подписи» (далее по тексту – 63фз). Следует заметить, что с 2011 года этот закон неоднократно подвергался «усовершенствованиям», т.е. в него вносились существенные и несущественные поправки. Поэтому обращаться нужно к актуальной на день прочтения редакции 63фз.

3. Одним из основных технических руководящих документов, которым руководствуются большинство операторов информационных систем и аккредитованные удостоверяющие центры, является приказ ФСБ России [от 27.12.2011 № 795](http://www.consultant.ru/document/cons_doc_LAW_125557/) «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи». Данный приказ в 2021 году подвергся изменениям вслед за 63фз (внесены приказом ФСБ России от 29.01.2021 № 31).

4. Каждый аккредитованный удостоверяющий центр (далее по тексту – УЦ) имеет собственный основной локальный нормативный акт, называемый чаще всего регламентом или порядком работы удостоверяющего центра. Данный документ, кроме всего прочего, определяет взаимоотношения удостоверяющих центров с клиентами, владельцами сертификатов, полученных в данных УЦ, а также (после письменного заявления клиента о присоединении к данному документу) является договором оферты[[1]](#footnote-1).

5. Основные термины, необходимые[[2]](#footnote-2) клиентам УЦ для понимания смысла и содержания получаемых в УЦ услуг[[3]](#footnote-3):

- *удостоверяющий центр* – орган, выдающий клиентам сертификаты ключа проверки электронной подписи; в данном контексте будут подразумеваться удостоверяющие центры, аккредитованные Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации – Минцифры (для выдачи квалифицированных сертификатов); [перечень](https://digital.gov.ru/ru/activity/govservices/2/) аккредитованных УЦ;

- *заявитель* (в рамках данной статьи) – лицо, обратившееся в удостоверяющий центр с заявлением о выдаче ему сертификата (в т.ч. квалифицированного сертификата);

- *сертификат ключа проверки электронной подписи* (далее по тексту – *сертификат*) – электронный документ, подтверждающий в автоматизированных системах и системах электронного документооборота принадлежность ключа электронной подписи и ключа проверки электронной подписи владельцу сертификата; является файлом с любым названием, но с расширением \*.cer, реже \*.crt или \*.p7b[[4]](#footnote-4); файл сертификата является электронным документом, подписанным электронной подписью издателя сертификата (т.е. удостоверяющего центра); последний факт подтверждает ответственность издателя за выпущенный им сертификат и содержащиеся в нём сведения; кроме того, 63фз (ст. 2, п. 2) называет сертификатом ещё и документ на бумажном носителе, являющийся произвольной распечаткой содержания файла сертификата; «бумажный» сертификат росписью владельца сертификата подтверждает удостоверяющему центру выдачу сертификата пользователю и ознакомление его с содержанием сертификата; владельцу сертификата он подтверждает то же самое, ну, и ещё законность владения сертификатом;

- *квалифицированный сертификат* – сертификат, 1) выданный **аккредитованным** УЦ и 2) **соответствующий заданным требованиям**[[5]](#footnote-5) по формату и содержанию;

- *ключ электронной подписи* – уникальная последовательность символов, предназначенная для создания электронной подписи; такой ключ чаще всего является файлом или набором файлов, содержащих означенную последовательность; записывается на [носитель](#носитель); по старым терминам-понятиям назывался «закрытым ключом»[[6]](#footnote-6);

- *ключ проверки электронной подписи* – уникальная последовательность символов, однозначно связанная с ключом электронной подписи, предназначенная для проверки подлинности электронной подписи; иногда является отдельным файлом, но чаще он содержится «вперемешку» с файлами (или внутри файлов) ключа электронной подписи; также символьное значение этого ключа (иногда его называют «открытым») содержится в сертификате;

- *владелец сертификата* – лицо, которому (после подтверждения его подлинности; согласно 63фз – идентификации) удостоверяющий центр выдал сертификат. Следует заметить, что к категории лиц Гражданский кодекс относит юридических лиц и физических лиц. К последним (в контексте данной статьи) относятся и индивидуальные предприниматели. И если с физическими лицами и индивидуальными предпринимателями всё ясно – чьи личные данные (фамилия, имя, отчество, ИНН, ОГРНИП, СНИЛС, e-mail…) указаны в поле «Субъект» сертификата, тот и владелец сертификата – то с юридическими лицами обстоит немного сложнее. В этом случае сертификат выдаётся именно юридическому лицу, и в поле «Субъект» указываются идентификационные данные юридического лица, но наряду с ними там же указываются некоторые данные (фамилия, имя, отчество, СНИЛС) физического лица, действующего от имени этого юридического лица без доверенности или на другом основании. Непонятно, как это трактует закон, но по факту (на практике) получается, что такой сертификат может использоваться в электронном документообороте и правоотношениях[[7]](#footnote-7) и юридического лица, и физического лица, указанного в поле «Субъект» в качестве «совладельца»;

- *подписывание электронных документов*[[8]](#footnote-8) (файлов) – процесс программного криптографического преобразования выбранных файлов, следствием которого становится получение электронной подписи «под» этими электронными документами; чаще всего подписывание производится с помощью специальных программ, иных прикладных программ со встроенной функцией подписывания файлов или встроенных в Интернет-сайты программных механизмов, которые формируют электронные подписи во взаимодействии с криптопровайдерами[[9]](#footnote-9);

- *электронная подпись* (далее по тексту – ЭП[[10]](#footnote-10)) – отдельный файл или встроенный в подписываемый электронный документ массив символов, криптографически связанный с подписываемым электронным документом[[11]](#footnote-11); электронная подпись, в основном, имеет две функции: а) доказательство того, что документ подписан лицом (физическим или юридическим лицом), являющимся владельцем сертификата, с помощью которого была создана ЭП; б) доказательство того, что у документа, подписанного этой электронной подписью, отсутствуют искажения (изменения) по отношению к его исходному виду (символьному содержанию);

- *квалифицированная электронная подпись* – электронная подпись, полученная с помощью **квалифицированного**[[12]](#footnote-12) сертификата, выданного аккредитованным УЦ;

- *средства электронной подписи* – если не учитывать персональный компьютер с операционной системой на нём, то к ним относятся: программные средства (криптографические и программы для подписывания), сочетание ключа электронной подписи, ключа проверки электронной подписи и сертификата, записанных на носитель ключа электронной подписи, и сам этот носитель;

- *носитель ключа электронной подписи* – аппаратное средство, чаще всего специально предназначенное для размещения на нём ключей электронной подписи в сочетании с соответствующими сертификатами; наиболее часто в качестве носителей ключей применяются устройства, имеющие в своём названии буквосочетание токен или token, например, Рутокен (Rutoken), Етокен (eToken) и другие; технически допускается запись ключей на флэш-накопители (т.н. флэшки), но такие носители не одобряются контролирующими органами (ФСБ России)[[13]](#footnote-13);

- *отзыв (аннулирование) сертификата* – публичное объявление сертификата прекратившим своё действие. Следует уточнить, что сертификат сам по себе прекращает своё действие после даты и времени, указанных в его сроке действия (поле «Действует до…»). Но в ряде случаев может потребоваться прекратить действие сертификата до данного момента, например, в случае компрометации ключа электронной подписи, сменой владельца сертификата, а также в иных, оговоренных законом случаях. Для аннулирования сертификата по инициативе владельца сертификата последний должен представить в удостоверяющий центр, выдавший этот сертификат, заявление с просьбой (требованием) аннулировать конкретный сертификат. Разумеется, сертификат должен однозначно идентифицироваться, для чего надо указать (как минимум) серийный номер сертификата, дату и время его издания, имя (наименование) владельца сертификата (другие сведения тоже не помешают). Убедившись в правомерности запроса на аннулирование, удостоверяющий центр аннулирует указанный сертификат, для чего вносит сведения о нём в *список отозванных (аннулированных) сертификатов* – специальный файл (формата \*.CRL), круглосуточный доступ к которому в Интернете УЦ обеспечивает согласно собственному регламенту деятельности. Любые желающие человек или информационная система, получив доступ к актуальной версии списка отозванных сертификатов, могут убедиться в наличии или отсутствии проверяемого ими сертификата среди отозванных.

6. По опыту общения с заявителями известно, что они часто (зачастую с невероятной настойчивостью) применяют слова «электронная подпись» (или того хуже – «ЭЦП»), не вникая в сущность термина[[14]](#footnote-14), установленную законом. Пока отношения между участниками электронного документооборота не перешли в конфликтную ситуацию, такая путаница не наносит существенного вреда, но при разбирательствах, там, где это важно (например, в суде), неправильное употребление терминов может сыграть против «путаников». Поэтому рекомендую: усвойте понятия о терминах[[15]](#footnote-15) «квалифицированный сертификат», «ключ электронной подписи» и «электронная подпись» до такой степени, чтобы в них не путаться. Это – полезно для достаточного понимания сущности электронного документооборота.

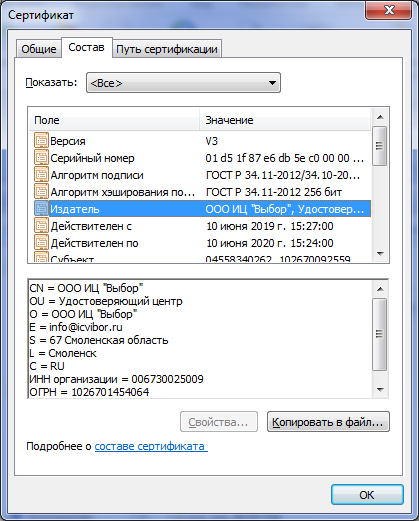
7. **Срок действия** сертификатов и соответствующих им ключей электронной подписи обычно устанавливается равным 1 году (12 месяцам). Например, если сертификат начал действовать 20 августа 2019 года в 16 часов 22 минуты 36 секунд, то его действие закончится 20 августа 2020 года в 16 часов 22 минуты 36 секунд[[16]](#footnote-16). Ряд УЦ своим решением допускает и обеспечивает задание произвольного срока действия сертификатов (как окончания, так и начала).

Во-первых, срок действия сертификата/ключа ЭП может быть увеличен до 15 месяцев. Это даёт определённые удобства пользователю (например, надо реже менять сертификат), но имеет и некоторые отрицательные последствия. Разумеется, цена такого сертификата для его владельца пропорционально возрастает.

Во-вторых, продолжительность срока действия может быть уменьшена от почти нулевой (в днях) до нескольких месяцев (например, до 3-х). Обычно удостоверяющие центры (у которых есть такая возможность) уменьшают срок действия тех сертификатов, для которых предполагается кратковременное или одноразовое использование. Разумеется, цена такого сертификата – льготная.

Иногда (по соображениям владельца сертификата) сдвигается в будущее (относительно времени издания сертификата удостоверяющим центром) дата начала действия сертификата[[17]](#footnote-17).

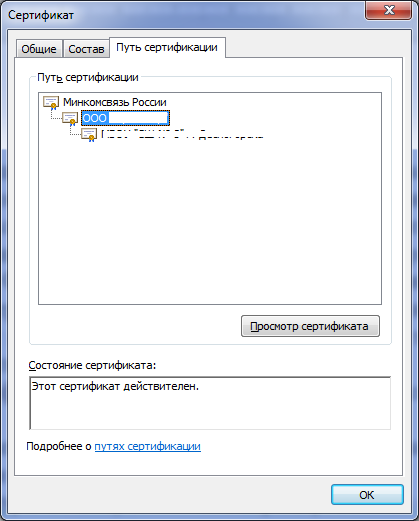
8. **Важные** сведения[[18]](#footnote-18) о сертификате, содержащиеся в файле сертификата, если его открыть[[19]](#footnote-19).

8.1. Серийный номер. Уникальное (для данного УЦ-издателя) сочетание символов, не повторяющееся на протяжении всей деятельности данного УЦ. Позволяет быстро и точно установить, какой сертификат рассматривается в тех или иных обстоятельствах или коллизиях.

8.2. Издатель сертификата (т.е. удостоверяющий центр). Позволяет получить данные, достаточные для точной идентификации УЦ, выпустившего данный сертификат.

8.3. Срок действия. Заставляет владельца сертификата задуматься (минимум) о мерах по получению нового сертификата при приближении дня окончания действия текущего сертификата. Ряд УЦ осуществляет автоматизированное заблаговременное информирование владельцев сертификата о приближении окончания действия текущего сертификата (как правило, по электронной почте).

8.4. Владелец сертификата (поле Субъект). Позволяет убедиться, что данные о владельце сертификата точны (не искажены и не содержат опечаток). Как правило, это данные о названии организации, фамилии, имени, отчестве, ИНН, ОГРН, СНИЛС, электронной почте, юридическом адресе или адресе регистрации и другие.

8.5. Дополнительные назначения сертификата (поле Улучшенный ключ). Ряд информационных систем[[20]](#footnote-20), в которых может применяться инструмент электронной подписи, требуют в это поле включать объектные идентификаторы (OID) (такие специальные признаки), при наличии которых в сертификате он становится дееспособным именно в данных информационных системах. Просмотр поля позволяет убедиться в наличии (или отсутствии!) нужных объектных идентификаторов.

8.6. Точки распространения списков отзыва (CRL)[[21]](#footnote-21). В последнее время процесс применения электронной подписи у многих информационных систем не требует от клиентов установки на персональный компьютер списков отозванных сертификатов удостоверяющего центра, выпустившего сертификат для применения в данной информационной системе. Но в отдельных случаях это может потребоваться. В данном поле указан адрес (адреса) информационных ресурсов в Интернете, по которым можно скачать нужный список отозванных сертификатов.

8.7. Путь сертификации. Показан вверху на правой вкладке окна сертификата. Отображает иконками цепь удостоверяющих центров[[22]](#footnote-22), участвовавших в издании данного сертификата. Для квалифицированных сертификатов цепь доверия (сверху вниз) начинается с сертификата[[23]](#footnote-23) Головного удостоверяющего центра Министерства цифрового развития, связи и массовых коммуникаций РФ, которым подписан сертификат уполномоченного лица аккредитованного УЦ (в цепи располагается на ступень ниже). Ещё ниже показывается сертификат владельца текущего сертификата. Если на иконках в этой цепи нет каких-либо предупреждающих символов (?, х), значит, в персональном компьютере владельца сертификата установлено доверие ко всем сертификатам из цепи. В находящемся на той же вкладке (внизу) поле «Состояние сертификата» будет отражён статус сертификата «действителен». Если есть вопросы и статус отличается от «действителен», то надо либо самому устранить причину, либо обратиться за консультацией к специалисту[[24]](#footnote-24).

9. Зачем нужен сертификат, распечатанный на бумажном носителе? В принципе, в файле сертификата содержится данных больше, чем это можно распечатать на бумаге. На бумаге видны не только наиболее важные данные, но и подписи и печати УЦ и владельца сертификата. Последнее обстоятельство важно тем, что подтверждает удостоверяющему центру факт выдачи сертификата и ознакомления владельца с содержанием сертификата. Поэтому один экземпляр «бумажного» сертификата УЦ оставляет себе. Второй экземпляр вручается владельцу сертификата, который с этого момента имеет на руках подтверждение того, что ему был выдан именно этот сертификат, а не иной. В некоторых случаях «бумажный» сертификат может пригодиться как доказательство владения сертификатом (например, в суде или при отчёте в бухгалтерию организации).

Новации в 63фз предполагают также, что подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, может осуществляться посредством использования заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи. Т.е. файл со сведениями из выданного сертификата должен быть предоставлен заявителем удостоверяющему центру с квалифицированной или простой электронной подписью.

10. **Безопасное использование электронной подписи**. Требования по конфиденциальности ключа ЭП изложены в государственных нормативно-правовых актах, а также локальных актах организаций, определяющих меры информационной безопасности. Им и надо следовать. В кратком изложении рекомендации пользователям таковы: электронная подпись равнозначна собственноручной (ст. 4 п. 3 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»). Поэтому любой суд будет прежде всего учитывать именно эту норму, а уже потом рассматривать версии пострадавших лиц о путях (способах, обстоятельствах), которыми инструмент ЭП (закрытый ключ электронной подписи) попал в руки злоумышленников[[25]](#footnote-25) или растяп[[26]](#footnote-26). Во многих случаях версии потерпевших для суда выглядят неубедительными (бездоказательными), отчего и выносится вердикт: сам виноват! Поскольку для неопределённой[[27]](#footnote-27) категории владельцев сертификата нет общих требований по хранению ключей (их носителей), то многим приходится самим определять методы хранения. Но в любом случае подход типа «а-а, ну и пусть мой закрытый ключ ЭП будет доступен всем желающим» является опасным для владельца сертификата[[28]](#footnote-28) и весьма желанным для разного рода мошенников. Обеспечат также безопасное использование вашей ЭП (в том числе) правильные действия при нарушении тайны (компрометации) ключа электронной подписи. Такие ключи следует безотлагательно выводить из обращения, заявив в УЦ просьбу об аннулировании сертификата, соответствующего скомпрометированному ключу ЭП. Одновременно с этим можно заказать для себя новый сертификат и ключ ЭП.

Если вы уверены (есть достаточные основания полагать), что с применением вашего ключа электронной подписи совершены какие-либо неправомерные (мошеннические, преступные) действия, или такие действия были совершены от вашего имени, но без вашего участия (согласия) и без применения вашего ключа[[29]](#footnote-29) (или у вас нет и никогда не было квалифицированного сертификата[[30]](#footnote-30)), то следует без промедления **обратиться в правоохранительные органы**[[31]](#footnote-31) с официальным заявлением о подозрении на совершение в отношении вас противоправных действий. Ведение при этом самостоятельного разбирательства тоже не повредит делу восстановления правопорядка, но только результаты расследования правоохранительных структур дадут основания для принятия справедливых судебных решений. Не лишним будет привлечение в качестве экспертов (консультантов) работников удостоверяющих центров, которым вы доверяете.

11. Основные **области применения** квалифицированной ЭП:

11.1. Документооборот в открытых или корпоративных системах электронного документооборота[[32]](#footnote-32).

11.2. Обращение к государственным услугам, предоставляемым или запрашиваемым в электронной форме[[33]](#footnote-33).

11.3. Предоставление отчётности и иной документооборот с контролирующими органами государства, совершаемые в электронной форме.

11.4. Участие в аукционах (торгах) на предоставление товаров (услуг), совершаемых в электронной форме.

11.5. Ведомственный[[34]](#footnote-34) электронный документооборот.

11.6. Иные услуги, оказываемые государственными и частными структурами.

12. **Выбор криптопровайдера** (СКЗИ)[[35]](#footnote-35) зависит от ряда факторов, но в любом случае он определяется желанием и возможностями владельца сертификата. Рассуждать о преимуществах и недостатках конкретных криптопровайдеров в этой статье не вижу смысла. Постараюсь сформулировать вопросы, на которые должен ответить пользователь[[36]](#footnote-36) ключа электронной подписи и сертификата прежде, чем сделать выбор:

12.1. В каких информационных системах я собираюсь использовать ключ? Работу с какими криптопровайдерами поддерживают эти информационные системы?

12.2. Будет ли совместим выбранный криптопровайдер с операционной системой и (возможно) другими криптопровайдерами на данном персональном компьютере?

12.3. Выберу ли я бесплатный (есть и такие) криптопровайдер или стоящий денег? Какие есть преимущества и недостатки у тех и других?

12.4. Должен ли криптопровайдер иметь подтверждение соответствия государственным требованиям (иными словами: сертификат соответствия от ФСБ России)?

12.5. Какой вид лицензии выбрать (ограниченная по времени или бессрочная)?

12.6. На скольких автоматизированных рабочих местах (персональных компьютерах) я собираюсь использовать электронную подпись (сколько понадобится лицензий)?

12.7. И (разумеется) насколько удобен для меня криптопровайдер в эксплуатации[[37]](#footnote-37)?

13. **Подписание** электронных документов и **проверка** электронной подписи в электронных документах совершается при участии криптопровайдеров, но для этого нужны и иные прикладные программы, имеющие такую функцию. Выбор их на рынке достаточно велик. Лицензии на часть из них распространяются безвозмездно.

14. Основные процедуры по получению квалифицированных сертификатов ключа проверки ЭП.

Условия получения квалифицированных сертификатов строго определены 63фз, поэтому аккредитованные удостоверяющие центры обязаны им следовать. Некоторым заказчикам процедурные требования удостоверяющих центров кажутся избыточными или необоснованными, что вызывает их недовольство. Однако вряд ли эти требования «придуманы» удостоверяющими центрами ради «перестраховки», практически всегда они направлены на точное выполнение требования закона, которое в свою очередь строго контролируется государством. Если удостоверяющий центр предлагает своим клиентам предельно упрощённую процедуру получения квалифицированного сертификата, то это является поводом заподозрить его в невыполнении требований 63фз или участии в мошенничестве (например: удалённая идентификация заявителя по копии паспорта, без визита в офис УЦ, достаточно только оплаты! и прочие «удобства»).

Первым и необходимым условием получения квалифицированного сертификата является однозначное подтверждение личности потенциального владельца сертификата (63фз называет это идентификацией). Этим занимаются и заказчик (63фз называет его заявителем), и удостоверяющий центр.

Для идентификации заявитель должен явиться в удостоверяющий центр сам и (кроме прочего) предъявить удостоверяющему центру паспорт или иной документ, удостоверяющий его личность на территории Российской Федерации. Однако, с 01.07.2020 г. согласно ст. 18 Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» этот первый[[38]](#footnote-38) (1) метод идентификации не является единственным. Закон допускает ещё 3 метода идентификации заявителя, но уже без его личного присутствия в офисе удостоверяющего центра:

2) с использованием квалифицированной электронной подписи при наличии у заявителя действующего квалифицированного сертификата;

3) с применением информационных технологий путем предоставления информации, указанной в документе, удостоверяющем личность гражданина РФ за пределами территории РФ (иначе говоря: в загранпаспорте нового образца, выдаваемом на 10 лет), содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные;

4) путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным [законом](consultantplus://offline/ref=DCBA1FB77081ECE92D4AE44BDFEC26329DD6E7FD3457B4D2F7EADD273CEFFEA6B32E653A761C254C90FD9A1D28k25FM) от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Более-менее понятным (для удостоверяющих центров) является (кроме первого) второй метод, хотя, как и все остальные, он плохо конкретизирован в подзаконных нормативных документах. Некоторые УЦ на своё усмотрение реализуют третий и четвёртый методы, но легитимность такой реализации пока вызывает ряд вопросов без внятного ответа.

**Второй метод** состоит в том, что заявитель направляет в удостоверяющий центр электронный документ (наиболее подходящим для этого является файл запроса на выдачу квалифицированного сертификата), предварительно подписав его своей электронной подписью. Данная электронная подпись должна быть создана с использованием квалифицированного сертификата, принадлежащего заявителю, срок действия которого (сертификата) не истёк на момент подписания. Удостоверяющий центр сравнивает данные о заявителе, которые последний предлагает включить во вновь создаваемый квалифицированный сертификат, с данными в сертификате, содержащемся в электронной подписи. Если субъект (владелец сертификата, использованного для создания электронной подписи) полностью идентичен тому, который предполагается владельцем вновь создаваемого сертификата, то удостоверяющий центр принимает решение о выдаче квалифицированного сертификата (при выполнении иных условий). Иначе говоря, таким образом выполняется первое из условий – идентификация заявителя.

Кроме этого заказчик в заявлении на получение в удостоверяющем центре квалифицированного сертификата сообщает о себе данные, которые нужны для внесения их в сертификат, и иные необходимые для деятельности УЦ данные. При необходимости удостоверяющий центр может запрашивать от заказчика иные документы или их копии[[39]](#footnote-39).

Часть этих данных проверяется удостоверяющим центром с помощью государственных информационных систем, в т.ч. действительность документа, удостоверяющего личность, СНИЛС, ИНН физического лица, ОГРН или ОГРНИП. Также удостоверяющий центр убеждается в наличии правомочий заявителя обращаться в УЦ за получением квалифицированного сертификата.

Если аккредитованный УЦ является коммерческой организацией, то необходимым условием получения сертификатов является оплата услуг удостоверяющего центра.

Ключ электронной подписи может быть выдан владельцу сертификата как на предоставленном им носителе, так и на закупленном им в УЦ (если тот ими торгует).

15. Трудно оставить без внимания тему мошенничества с применением квалифицированных сертификатов и сформированных с их помощью электронных подписей. К сожалению, уполномоченные и правоохранительные федеральные органы (как всегда) с опозданием взялись за борьбу с этим явлением (преступлениями, чего уж там). Преступления, «бьющие по карману» государство и/или нарушающие имущественные права граждан, совершаются со всё возрастающей частотой. Видимо, мошенники всех мастей почувствовали «слабину» именно в этой «отрасли народного хозяйства» и «успешно» ею пользуются.

Наиболее частыми с использованием электронной подписи стали налоговые преступления. От имени либо «честных» коммерческих организаций, либо фирм-однодневок подаётся ложная налоговая отчётность по налогу на добавленную стоимость (НДС), после чего мошенники требуют с государства незаконного возврата НДС. Для регистрации фирм-однодневок и отправки за них отчётности требуются «липовые» директора. Вот на их имя и получаются в недобросовестных удостоверяющих центрах (или через их жуликоватых сотрудников) квалифицированные сертификаты. В качестве «липового» директора может выступить какое-нибудь лицо «с низкой социальной ответственностью», готовое за мзду малую выступить в любой роли, или вполне приличный и законопослушный человек, личными данными которого преступники воспользовались, чтобы в сговоре с уполномоченным представителем удостоверяющего центра выпустить квалифицированный сертификат на ничего не подозревающего гражданина.

Ещё одним вариантом[[40]](#footnote-40) незаконного использования чужой электронной подписи является выдача квалифицированного сертификата на ничего не подозревающего гражданина[[41]](#footnote-41) для совершения действий, якобы закрепляемых его электронной подписью (юридически равнозначной собственноручной подписи на бумажном документе), например, сделок с недвижимостью, взятия кредитов, демонстрации деловой активности подставных фирм (подписания договоров, участия в электронных торгах…), и других незаконных действий. Пострадавший порой долго не подозревает о том, что творится у него за спиной от его имени, а узнаёт об этом только тогда, когда к нему приходят судебные приставы.

К сожалению, нынешнее состояние правовой машины государства и частных структур не даёт нам уверенности в том, что мы не станем очередными жертвами такого рода мошенничеств. В том же направлении «бьёт» беспечность и слабая правовая культура[[42]](#footnote-42) граждан.

Что же делать добросовестному (и добропорядочному) гражданину (в т.ч. руководителю организации), если он узнал или заподозрил нелегальное существование квалифицированного сертификата, за получением которого он лично (или его организация) не обращался? Универсальных и стопроцентно эффективных советов не даст никто, но с чего-то же надо начинать? Итак:

1) Узнать, каким удостоверяющим центром на его имя был выпущен квалифицированный сертификат, посредством которого были подписаны фальшивые электронные документы. Возможно, что эту информацию от пострадавшего будут скрывать, но следует добиться предоставления ему файла сертификата и (желательно) подписанного этим сертификатом электронного документа[[43]](#footnote-43). Из сертификата нужно получить информацию об издателе (удостоверяющем центре).

2) Найти контакты удостоверяющего центра-издателя в Интернете. Написать, позвонить, иным образом официально стребовать с УЦ файл квалифицированного сертификата, выпущенного якобы на его имя, тем самым подтвердить факт выпуска данного сертификата. Практически у всех УЦ есть сайт и функция на нём, с помощью которой должно осуществляться получение от УЦ сертификата.

3) Убедившись, что все данные, указанные в сертификате (особенно СНИЛС и ИНН, ну, и, конечно, фамилия, имя, отчество, адрес и прочее), соответствуют его данным, срочно обратиться любым (а лучше несколькими) способом: по телефону, по электронной почте, по Почте России с требованием аннулировать выпущенный сертификат и предоставить ему внятные объяснения, каким образом получилось, что сертификат на его имя был выпущен без его реального обращения[[44]](#footnote-44). Любые ответы (даже по телефону и электронной почте) приобщать «к делу». Добиваться, чтобы ответы были авторизованы (под ними были указаны должности и фамилии работников удостоверяющего центра).

4) Когда УЦ сообщит, что сертификат аннулирован, скачать с информационного ресурса удостоверяющего центра список отозванных сертификатов (файл) и убедиться, что в него включен ваш аннулированный сертификат.

5) На всякий случай (в ваших интересах не лениться) написать бумажные или по электронной почте письма в организации, где, как предполагается, могут быть совершены мошеннические действия с использованием подложной электронной подписи. В частности, такие письма пишут в Росреестр, через который как раз и отнимают квартиры у людей. Везде просить не принимать к рассмотрению электронные документы, подписанные электронной подписью с незаконным сертификатом (указать серийный номер, дата выдачи и другие реквизиты сертификата).

6) Не дожидаясь завершения действий 1÷5:

- опротестовать официальным обращением (письмом) совершённые от его имени действия;

- обратиться в правоохранительные органы (например, в полицию и – копию – в прокуратуру). Кроме самого сообщения о подозрительных или явно преступных действиях с его электронной подписью, не лишним будет сообщить правоохранительным органам и ставшие известными сведения о сертификате и выдавшем его удостоверяющем центре. Это должно существенно ускорить нейтрализацию неблагоприятных последствий и разбирательство по существу дела.

Разумеется, далеко не все УЦ вовлечены в мошеннические «схемы». Подавляющее большинство из них добросовестно выполняет требования законов и иных нормативных актов и не вступает с мошенниками в сговор. И оглашаемые вышеописанные случаи (хочешь – не хочешь) незаслуженно наносят ущерб и их репутации. Но зачислять все аккредитованные удостоверяющие центры в пособники мошенников (как минимум) неконструктивно[[45]](#footnote-45). Мошенники не сегодня появились и не только в сфере применения электронной подписи. Бороться с ними и можно, и нужно. Так же, как ведётся с ними (с разной степенью успешности) борьба в других сферах человеческой деятельности. В этой борьбе вряд ли будет кем-то одержана безоговорочная победа, но со временем против мошенничества в данной сфере будет найдено «противоядие», что приведёт к спаду успешности данного «бизнеса» и постепенной его маргинализации. В последнее время законодатель внёс в 63фз существенные изменения, направленные (такова их официально декларируемая цель) на снижение рисков неправомерного получения и использования квалифицированных сертификатов. Весь комплекс поправок должен вступить в силу не позднее 01.01.2022 г., после чего широкий круг лиц сможет оценить его эффективность.

\*\*\*

Вопреки желанию автора «отсечь» всё лишнее (несущественное для целей данной статьи) статья получилась довольно большой. Всё же надеюсь, что каждый читатель[[46]](#footnote-46) найдёт в ней для себя необходимый минимум знаний и понятий для разумного и квалифицированного применения электронной подписи в своей деятельности.

Замечания и пожелания по содержанию статьи читатели могут направить мне по адресу электронной почты. Обещаю исправлять неточности и разъяснять неясности, если таковые будут обнаружены.

Свободное распространение текста и ссылок на него не запрещено, даже приветствуется. При этом желательно указывать на реальное авторство.

Жоголев Александр Александрович, руководитель Удостоверяющего центра ООО ИЦ «Выбор»

e-mail: [a.zhogolev@icvibor.ru](mailto:a.zhogolev@icvibor.ru)

корпоративный сайт: [http://www.icvibor.ru](http://www.icvibor.ru/)

1. **Офе́рта** (лат. offero – предлагаю) – предложение о заключении сделки, в котором изложены существенные условия **договора**, адресованное определённому лицу, ограниченному или неограниченному **кругу** лиц. [↑](#footnote-ref-1)
2. неискушённому взгляду может показаться, что терминов многовато, но предельное упрощение терминологии и понятийного аппарата лишит человека, желающего разобраться, понимания необходимых нюансов проблематики; автор придерживается мнения, что понимание предмета достигается быстрее, когда диалог ведётся с применением единой системы терминов, а не жаргонных словечек, придуманных в разных группах из-за лени и нежелания думать [↑](#footnote-ref-2)
3. автор статьи намеренно упрощает по сравнению с 63фз толкование терминов или (как их называет закон) понятий, чтобы не отпугивать «чайников» тяжеловесными формулировками, которых (увы!) и ему порой не удаётся избежать [↑](#footnote-ref-3)
4. особенный формат, строго говоря не являющийся сертификатом; скорее его можно охарактеризовать как некий пакет, который может содержать от одного до бесконечного множества сертификатов, а также списков отозванных сертификатов [↑](#footnote-ref-4)
5. приказа ФСБ от 27.12.2011 № 795 «Об утверждении требований к форме квалифицированного сертификата…» [↑](#footnote-ref-5)
6. некоторые даже некорректно называют его «секретным ключом», что может вносить сумятицу в мозг людей, имеющих понятия о государственных грифах секретности; лучше следовать терминологии из 63фз, хотя и её не назовёшь удачной [↑](#footnote-ref-6)
7. например, в личном кабинете физического лица на портале Госуслуг [↑](#footnote-ref-7)
8. электронный документ – это чаще всего какой-либо электронный файл [↑](#footnote-ref-8)
9. одно из названий средств криптографической защиты информации [↑](#footnote-ref-9)
10. очень часто даже работники аккредитованных удостоверяющих центров к месту и не к месту применяют аббревиатуру ЭЦП (ранее означала «электронная цифровая подпись»); с 2011 года этот термин не подтверждается законами, к тому же вносит в мысли неспециалистов лишний раздрай, чем и вреден [↑](#footnote-ref-10)
11. автором «вынесена за скобки» т.н. простая электронная подпись, т.к. она практически никогда не является результатом выполнения услуги аккредитованного УЦ [↑](#footnote-ref-11)
12. в принципе, аккредитованный удостоверяющий центр для специальных назначений может выдавать **неквалифицированные** сертификаты, но такие назначения в последнее время в редки в широком обиходе [↑](#footnote-ref-12)
13. если владелец сертификата не зависим от «мнения» ФСБ России, то он волен выбрать и такой носитель; другое дело, что от «мнения» ФСБ России сильно зависит аккредитованный УЦ, вынужденный выполнять требования и ФСБ, и 63фз [↑](#footnote-ref-13)
14. самый распространённый случай: заявитель просит УЦ выдать ему «электронную подпись» или «ЭЦП», при этом на самом деле речь ведётся о выдаче квалифицированного сертификата; электронную подпись владелец сертификата с помощью этого сертификата формирует уже в целях ведения электронного документооборота и (реже) аутентификации (подтверждения подлинности) пользователя в некоторых информационных системах; т.е. УЦ не «выдаёт» электронные подписи, он даже не участвует в их создании [↑](#footnote-ref-14)
15. хотя бы этих трёх [↑](#footnote-ref-15)
16. иногда время окончания действия может отличаться от начального на несколько минут [↑](#footnote-ref-16)
17. довольно редко [↑](#footnote-ref-17)
18. следует отметить, что под словом «важные» автор на своё усмотрение выбрал те сведения, которые должны (по его мнению) представлять наибольший интерес при использовании сертификатов широким кругом потребителей; нормативно же данные из сертификатов не делятся на важные и второстепенные; значимость (в т.ч. юридическая) каждого поля или массива данных совпадает со значимостью самого сертификата в целом [↑](#footnote-ref-18)
19. открытие сертификата производится двойным кликом по файлу в Проводнике Windows; действие «Открыть файл» [↑](#footnote-ref-19)
20. не все, но довольно многие, как государственные, так и коммерческие [↑](#footnote-ref-20)
21. [↑](#footnote-ref-21)
22. иногда её называют «цепочкой доверия» [↑](#footnote-ref-22)
23. т.н. корневого [↑](#footnote-ref-23)
24. лучше всего – в техническую поддержку удостоверяющего центра, выдавшего сертификат [↑](#footnote-ref-24)
25. если уж стало о них известно что-то конкретное (что очень часто не удаётся выяснить) [↑](#footnote-ref-25)
26. ну, бывает, что ключ электронной подписи владелец передал в руки какому-то «особо доверенному» лицу, а оно оказалось растяпой: потеряло ключ, кому-то передало на время, что-то не то подписало… [↑](#footnote-ref-26)
27. так сказать, «негосударственной» категории [↑](#footnote-ref-27)
28. самое «невинное», что можно привести: вы – должностное лицо; якобы от вас другому должностному лицу приходит файл с грязными ругательствами в его адрес, при этом файл подписан вашей электронной подписью; возможно, инцидент будет замят (с извинениями и пр.), но «осадочек» останется: а как это вы храните свой ключ? тот ли вы работник, которому можно доверять серьёзные дела? за другими примерами – в Интернет [↑](#footnote-ref-28)
29. **своим** владелец сертификата должен считать ключ электронной подписи, который создан им лично или получен в удостоверяющем центре для собственных потребностей и находится в его личном владении и под контролем [↑](#footnote-ref-29)
30. к сожалению, всё чаще имеют место случаи, когда мошенникам удаётся получать квалифицированные сертификаты на имя субъектов, даже не подозревающих о выдаче сертификатов на их имя; в этом случае под угрозой может оказаться широкий перечень интересов лиц, в первую очередь, конечно, имущественных [↑](#footnote-ref-30)
31. полиция, прокуратура [↑](#footnote-ref-31)
32. Этим можно было бы и закончить, т.к. это – исчерпывающе. Далее будет с некоторыми подробностями [↑](#footnote-ref-32)
33. чаще всего это ассоциируется с Порталом Госуслуг РФ: пользование личным кабинетом налогоплательщика, заявка на получение заграничного паспорта, покупку земельных участков, запись на приём в поликлинику, регистрация автомобиля, представление налоговой отчётности или документов во внебюджетные фонды (ФСС, ФОМС и ПФР), доступ к информационным ресурсам Росреестра и много иного [↑](#footnote-ref-33)
34. в открытых государственных информационных системах [↑](#footnote-ref-34)
35. **криптопровайдер** (Cryptography Service Provider, CSP) или (другое название) средство криптографической защиты информации (извините, объяснение своими словами будет хуже, чем в Википедии) – это независимый модуль, позволяющий осуществлять криптографические операции в операционных системах Microsoft, управление которым происходит с помощью функций CryptoAPI. Проще говоря, это посредник между операционной системой, которая может управлять им с помощью стандартных функций CryptoAPI, и исполнителем криптографических операций (это может быть как программа, так и аппаратный комплекс); в любом случае, без него не обойтись [↑](#footnote-ref-35)
36. возможно, не сам, а с помощью консультантов [↑](#footnote-ref-36)
37. такой вопрос, как правило, задаёт уже опытный пользователь электронной подписи; остальным не грех обратиться к консультантам [↑](#footnote-ref-37)
38. по порядку перечисления в законе [↑](#footnote-ref-38)
39. иногда заверенные, иногда нет [↑](#footnote-ref-39)
40. все возможные варианты рассмотреть нет возможности [↑](#footnote-ref-40)
41. с использованием тех же уловок [↑](#footnote-ref-41)
42. несерьёзное отношение к инструменту электронной подписи, как к игрушке, вроде мобильного телефона [↑](#footnote-ref-42)
43. могут говорить о том, что документ конфиденциален (но это – ложные доводы), но обязательства по нему кто-то требует выполнять; поэтому прежде, чем требовать, должны предоставить вещественные доказательства этих требований [↑](#footnote-ref-43)
44. особо интересной информацией является то, каким из перечисленных в данной статье методов проводилась идентификация лица, обратившегося за получением данного спорного сертификата [↑](#footnote-ref-44)
45. как максимум – несправедливо [↑](#footnote-ref-45)
46. вступивший в возраст и сферу деятельности, заставляющие обратиться к инструменту электронной подписи [↑](#footnote-ref-46)