Электронная подпись

1.1 Общая информация

В современном мире происходит постепенная замена бумажной технологии обработки информации ее электронным аналогом. Всё большее распространение получают автоматизированные системы обработки информации. Тенденция ведет в будущем к полной замене бумажного документооборота электронным. Однако защитных атрибутов бумажных документов, таких как подписей, печатей, водяных знаков и специальной фактуры поверхности, - у электронного представления документа нет. Поэтому возникла задача разработки такого механизма электронной защиты, который смог бы заменить подпись и печать на бумажных документах. Во-первых, такой механизм должен подтверждать, что подписывающее лицо не случайно подписало электронный документ. Во-вторых, он должен подтверждать, что только подписывающее лицо, и только оно, подписало электронный документ. В-третьих, он должен зависеть от содержания подписываемого документа и времени его подписания. В-четвертых, подписывающее лицо не должно иметь возможности впоследствии отказаться от факта подписи документа. Таким механизмом стала электронно-цифровая подпись.

Электронная подпись (ЭП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Согласно Федеральному закону **№63-ФЗ «Об электронной подписи»**, имеет место деление на:

- простую электронную подпись;
- усиленную неквалифицированную электронную подпись;
- усиленную квалифицированную электронную подпись.

Простая электронная подпись посредством использования кодов, паролей или иных средств подтверждает факт формирования ЭП определенным лицом.

Усиленную неквалифицированную электронную подпись получают в результате криптографического преобразования информации с использованием закрытого ключа подписи. Данная ЭП позволяет определить лицо, подписавшее электронный документ, и обнаружить факт внесения изменений после подписания электронных документов.

Усиленная квалифицированная электронная подпись соответствует всем признакам неквалифицированной электронной подписи, но для создания и проверки ЭП используются средства криптозащиты, которые сертифицированы ФСБ РФ. Кроме того, сертификаты квалифицированной ЭП выдаются исключительно аккредитованными удостоверяющими центрами (Перечень аккредитованных УЦ).

Согласно ФЗ № 63 «Об электронной подписи» электронный документ, подписанный простой или усиленной неквалифицированной ЭП, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью. При этом обязательным является соблюдение следующего условия: между участниками электронного взаимодействия должно быть заключено соответствующее соглашение.

Усиленная квалифицированная подпись на электронном документе является аналогом собственноручной подписи и печати на бумажном документе. Контролирующие органы, такие как ФНС, ПФР, ФСС, признают юридическую силу только тех документов, которые подписаны квалифицированной ЭП.

Резервное копирование – услуги по копированию КЭП на резервные ключевые носители. Данная услуга доступна только в случае если при выпуске КЭП был установлен признак экспортируемости. Все подписи, выпускаемые нашим УЦ, выпускаются как *не экспортируемые*. Т.е. их нельзя перенести на другой ключевой носитель т.е. скопировать – сделать резервную копию. Тем самым мы повышаем

уровень защищенности выпускаемой КЭП, снижая риск несанкционированного копирования. Если клиент изъявляет желание сделать резервную копию ключа, то необходимо продать услугу по **а.** возможности экспортирования **б.** в случае если клиент сам не может скопировать – услуги по копированию **в.** ключевой носитель, в случае если продана кэп АЭТП и услуга по копированию.

Экспортируемая\неэкспортируемая КЭП – признак КЭП присваиваемый при генерации закрытой части ключа, позволяющий в последующем производить резервное копирование КЭП на другие носители. Данный признак возможно присвоить только на этапе генерации закрытой части КЭП.

1.2 Процедура получения ЭП

Для получения сертификата **для юридического лица** на руководителя организации, **для ИП** и **физического лица** следует предоставить в УЦ следующие документы (документы предоставляет владелец сертификата лично), *первый пункт «Заявления» является общим для всех:*

1. **Заявления** (http://itk23.ru/printq/a1.php):

1. 1. Заявление о присоединении к Регламенту Удостоверяющего центра ООО «ИТК» (оригинал с подписью и печатью при наличии; передается в Удостоверяющий центр);

1.2. Заявление на регистрацию и изготовление квалифицированного сертификата (оригинал с подписью и печатью при наличии; передается в Удостоверяющий центр);

1.3. Согласие на обработку персональных данных (оригинал с подписью и печатью при наличии; передается в Удостоверяющий центр);

Для юридического лица:

2. **Свидетельство о государственной регистрации юридического лица** (ОГРН) (предоставляется оригинал и копия заверенная печатью организации и подписью руководителя организации; в Удостоверяющем центре остается копия заверенная печатью организации и подписью руководителя организации);

3. **Свидетельство о постановке на учет в налоговом органе** (ИНН) (предоставляется оригинал и копия заверенная печатью организации и подписью руководителя организации; в Удостоверяющем центре остается копия заверенная печатью организации и подписью руководителя организации);

4. **Копия документа о назначении руководителя** (приказ), заверенный печатью организации и подписью руководителя организации;

5. **Паспорт владельца сертификата** (стр. с фотографией и актуальной пропиской) оригинал и копия заверенная печатью организации и подписью руководителя организации;

6. **Страховое свидетельство государственного пенсионного страхования** (СНИЛС) владельца сертификата (предоставляется оригинал и копия заверенная печатью организации и подписью руководителя организации; в Удостоверяющем центре остается копия заверенная печатью организации и подписью руководителя организации)

Для ИП:

2. **Свидетельство о государственной регистрации физического лица в качестве индивидуального предпринимателя** (ОГРНИП), предоставляется оригинал или нотариально заверенная копия (или копия, заверенная печатью организации и подписью руководителя организации, в случае, если документы будет предоставлять доверенное лицо);

3. **Свидетельство о постановке на учет в налоговом органе** (ИНН), предоставляется оригинал или нотариально заверенная копия (или копия, заверенная печатью организации и подписью руководителя организации, в случае, если документы будет предоставлять доверенное лицо);

4. **Паспорт владельца сертификата** (стр. с фотографией и актуальной пропиской) оригинал (или копия, заверенная печатью организации и подписью руководителя организации, в случае, если документы будет предоставлять доверенное лицо);

5. **Страховое свидетельство государственного пенсионного страхования** (СНИЛС) владельца сертификата, предоставляется оригинал (или копия, заверенная печатью организации и подписью руководителя организации, в случае, если документы будет предоставлять доверенное лицо);

6. Доверенность на представителя организации, уполномоченного на предоставление документов (оригинал с подписью и печатью; передается в Удостоверяющий центр) - в случае, если документы будет предоставлять доверенное лицо;

7. Паспорт представителя организации, уполномоченного на предоставление документов - в случае, если документы будет предоставлять доверенное лицо.

Для физического лица:

2. **Свидетельство о постановке на учет в налоговом органе** (ИНН) (предоставляется оригинал (или нотариально заверенная копия) и копия заверенная подписью владельца сертификата, в Удостоверяющем центре остается копия заверенная подписью владельца сертификата);

3. **Паспорт владельца сертификата** (стр. с фотографией и актуальной пропиской), предоставляется оригинал и копия заверенная подписью владельца сертификата, в Удостоверяющем центре остается копия заверенная подписью владельца сертификата;

4. **Страховое свидетельство государственного пенсионного страхования** (СНИЛС) владельца сертификата (предоставляется оригинал и копия заверенная подписью владельца сертификата, в Удостоверяющем центре остается копия заверенная подписью владельца сертификата)

Примечание. **Срок действия ЭЦП составляет 1 год. По истечении этого срока ЭЦП необходимо перевыпускать.**

1.3 Как применяется ЭП

Функциями электронной подписи является подпись и шифрование электронных документов. Данные функции могут быть использованы в различных информационных системах, где есть необходимость:

- подтвердить факт подписания документа конкретным лицом

- доказать, что документ не был изменен с момента подписания

-зашифровать документ перед отправкой и до получения адресатом для невозможности получения содержимого письма посторонним лицам

Перечень информационных ресурсов, где применяется наша КЭП можно посмотреть тут:

http://itk23.ru/oids/certs.php

Электронный документооборот. Технология ЭП широко используется в системах электронного документооборота различного назначения: внешнего и внутреннего обмена, организационно-распорядительного, кадрового, законотворческого, торгово-промышленного и прочего. Это продиктовано главным свойством электронной подписи – она может быть использована в качестве аналога собственноручной подписи и/или печати на бумажном документе.

Во внутреннем документообороте ЭП используется, как средство визирования и утверждения электронных документов в рамках внутренних процессов. Например, во время согласования договора директор подписывает его ЭП, что значит, что договор утвержден и может быть передан в исполнение.

При построении *межкорпоративного документооборота (B2B)* наличие ЭП является критически важным условием обмена, поскольку является гарантом юридической силы. Только в этом случае электронный документ может быть признан подлинным и использоваться в качестве доказательства в судебных разбирательствах. Подписанный усиленной электронной подписью документ также может длительное время храниться в цифровом архиве, сохраняя при этом свою легитимность.

Электронная отчетность для контролирующих органов. Многие компании, наверняка, уже оценили удобство сдачи отчетности в электронном виде. Современный подход к сдаче отчетности через интернет состоит в том, что клиент может выбрать любой удобный для себя способ: отдельное ПО, продукты семейства 1С, порталы ФНС, ФСС. Основа этой услуги – сертификат электронной подписи, который должен быть выпущен надежным удостоверяющим центром, метод же отправки не имеет решающего значения. Такая подпись нужна для придания документам юридической значимости.

Государственные услуги. Каждый гражданин Российской Федерации может получить электронную подпись для получения госуслуг. С помощью ЭП гражданин может заверять документы и заявления, отправляемые в ведомства в электронном виде, а так же получать подписанные письма и уведомления о том, что обращение принято на рассмотрение от соответствующих органов власти.

Пользователь имеет возможность подписать электронной подписью заявление, отправляемое в орган исполнительной власти (при готовности органа исполнительной власти принимать заявления, подписанные электронной подписью). При реализации этого механизма используются отечественные стандарты ЭП (ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001) и применяются сертифицированные в системе сертификации ФСБ России средства криптографической защиты информации.

Электронные торги. Электронные торги проходят на специальных площадках (сайтах). Электронная подпись необходима поставщикам на государственных и коммерческих площадках. ЭП поставщиков и заказчиков гарантируют участникам, что они имеют дело с реальными предложениями. Кроме того, заключенные контракты приобретают юридическую силу только при его подписании обеими сторонами.

Арбитражный суд. При возникновении каких-либо споров между организациями в качестве доказательства в суде могут использоваться электронные документы. Согласно Арбитражному процессуальному кодексу РФ, полученные посредством факсимильной, электронной или иной связи, подписанные электронной подписью или другим аналогом собственноручной подписи, относятся к письменным доказательствам. Об этом подробнее ниже.

Документооборот с физическими лицами. Надо признать, данная сфера применения ЭП весьма специфична и пока редко используема, тем не менее, возможна. С помощью ЭП заверять различные документы могут физические лица. Благодаря этой возможности удаленные работники на основании договоров оказания услуг, например, могут выставлять акты приемки-сдачи работ в электронном виде.

1.4 Криптографическая защита информации – шифрование

Шифрование — это способ преобразования открытой информации в закрытую и обратно. Оно применяется для хранения важной информации в ненадежных источниках или передачи ее по незащищенным каналам связи. По закону сдавать отчетность в электронном виде и обмениваться юридически значимыми документами можно только в том случае, если документооборот защищен. Шифрование необходимо для того, чтобы надежно защитить информацию. Цель шифрования – это сделать невозможным прочтение хранящейся в документе информации посторонними людьми. Таким образом, шифрование информации является важнейшим этапом электронного документооборота. Осуществляется оно с помощью электронной подписи (криптоключа).

Использование шифрования позволяет:

- Сохранить конфиденциальность переписки – никто посторонний не сможет прочитать документ. В бумажной технологии это аналогично тому, что письмо запечатано в конверт, и никто не может его прочесть ни при хранении, ни при передаче.
- Обеспечить целостность документа – в зашифрованном документе ничего нельзя изменить. Это все равно, что пытаться ручкой исправить что-то в бумажном подписанном документе. Одно зачеркнутое слово – и документ становится недействительным.
- Гарантировать однозначность идентификации отправителя – закрытый ключ уникален и позволяет однозначно определить лицо, подписавшее документ.
- Контролировать доступ – шифруя документ, владелец ключа сам выбирает, кто его сможет прочитать.

Благодаря этому удается сделать ЭДО надежным, безопасным, и обеспечить юридическую значимость электронных документов.

Шифрование подразделяется на процесс зашифровывания и расшифровывания. В зависимости от того как осуществляются эти 2 этапа шифрования выделяют – симметричное и асимметричное шифрование.

Симметричное шифрование — способ шифрования, в котором для зашифровывания и расшифровывания информации применяется один и тот же криптографический ключ. Ключ в этом случае выбирается сторонами до начала обмена сообщениями и хранится в секрете обеими сторонами.

Одним из первых примеров симметричного шифрования информации применил Юлий Цезарь. Он отправлял в удаленные провинции послания, где вместо буквы A ставил букву D, вместо буквы B —

букву Е и т. д. То есть использовал алфавитный сдвиг на три буквы. И вплоть до недавнего времени ничего принципиально нового наука о шифровании не изобретала. Однако в семидесятые годы прошлого века был изобретен принципиально новый способ криптографической защиты информации. Он не требует предварительного обмена секретом шифра.

Асимметричное шифрование использует два разных ключа – открытый и закрытый. Открытый ключ зашифровывает данные, а соответствующий ему закрытый ключ их расшифровывает. Вместе они образуют ключевую пару. Открытый ключ известен всем заинтересованным лицам, в то время как закрытый держится в тайне. Любой человек с копией открытого ключа может зашифровать информацию, которую сможет прочитать только владелец закрытого ключа. Главное достижение асимметричного шифрования в том, что оно позволяет людям, не имеющим особой договоренности о безопасности, обмениваться секретными сообщениями. Необходимость отправителю и получателю согласовывать тайный ключ по специальному защищенному каналу полностью отпала. Все коммуникации затрагивают только открытые ключи, тогда как закрытые хранятся в безопасности.

Процессы создания ключевых пар, зашифровывания и расшифровывания документов осуществляется программами криптозащиты или средствами криптозащиты информации (СКЗИ).

Без этой программы не удастся использовать ЭП на компьютере. Наиболее популярные программы криптозащиты это:

Крипто-Про

Lissi-CSP

Signal-ComCSP

VipNet-CSP

Наш удостоверяющий центр выпускает ЭП только по Крипто-Про. Крипто-Про может использоваться без лицензии в течение 3-х месяцев в тестовом режиме!!!

Виды Крипто-Про:

Крипто-Про **CSP** и **JCP** – две версии одного криптопровайдера. Функции обоих версий данного ПО идентичны. JCP используется для работы с помощью Java – платформа для реализации определенных задач и механизмов внутри ОС, распространяется бесплатно. Ряд информационных систем-порталов (например СМЭВ) используют именно эту платформу. CSP наиболее распространен с учетом применения в больших информационных система (ФЭТП и пр.)

ПО для работ с ЭП. Сама по себе электронная подпись делать ничего не может. Физически это просто набор информации на ключевом носителе, которую можно применить для определенных целей. Далее рассмотрим назначение продаваемого ПО:

1. **Крипто-ПРО CSP\JCP**- мы применяем электронную подпись на компьютере, где установлена операционная система Windows- разработка зарубежного вендора Microsoft. Цели использования электронной подписи – защитить информацию от потенциального злоумышленника, которым также может являться разработчик Windows. Такие же цели будет преследовать любое государство, поставившее перед собой задачу защитить информацию. Поскольку на территории США Российское законодательство в области защиты информации не имеет силы – отечественные уполномоченные программисты разработали свой алгоритм шифрования и подписи. Для того, что бы применять этот

алгоритм шифрования и подписи поверх используемых нами операционных систем, и было разработано ПО Крипто-Про CSP\JCP – оно называется КРИПТОПРОВАЙДЕР. Он «согласует» наши компьютеры со способами шифрования и подписи информации применяемыми на территории РФ.

Алгоритмы шифрования и подписи это набор определенных правил и формул. Компания Крипто-Про одна из разработчиков (наиболее популярных на территории РФ), предлагающая оболочку для использования этих алгоритмов (Крипто-Про CSP). Помимо нее на рынке присутствуют аналогичные криптопровайдеры разработанные другими компаниями, но не столь распространенными (Лиси CSP, VipNet CSP и пр.). **КриптоПро выдается на 1 год либо бессрочно.**

2. **КриптоАРМ** – используя криптопровайдер, мы «подружили» наш компьютер с электронной подписью, теперь необходимо дать нашему компьютеру инструменты, чтобы использовать эту подпись. Для этого было разработано большое количество ПО, позволяющих реализовать возможности КЭП. Одна из таких программ КриптоАрм. Программа позволяет подписывать любые документы, подтверждая подлинность документа и лицо, его подписавшее. После подписи данное ПО может зашифровать документ, чтобы никто до момента получения адресатом этого документа не смог его прочитать. Соответственно после получения документа, адресат может использовать КриптоАрм в обратном направлении – расшифровать документ, проверить подпись отправителя. Данное ПО является инструментом для подписи, т.е. оно само не отправляет документ и не является способом организации электронного документооборота. **КриптоАрм будет работать без лицензии 1 месяц, при условии, что никогда не устанавливалась на используемом компьютере. КриптоАрм выдается на неограниченный срок.**

3. **Крипто-Про office signature (Сигнатура)** – еще один продукт компании Крипто-Про. Является аналогом ПО КриптоАрм. Область применения чуть более узкая – подписывает только документы из пакета MS Office, т.е. он учит программы, входящие в состав MS Office, использовать нашу отечественную КЭП. Несмотря на более узкую область применения, имеет большую популярность, так как большинство муниципальных заказчиков принимают только документы формата MS Office.

4. **VipNet** – Одним из разработчиков ПО для применения отечественных алгоритмов шифрования является компания Инфотекс, разработавшая линейку продуктов под общим названием VipNet. Данный вендор предлагает комплексное решение, включающее все функции вышеописанного ПО:

- Электронную подпись
- КриптоПровайдер
- Инструмент для подписи и шифрования
- Программное обеспечения организующее защищенное соединение между участниками обмена электронными сообщениями – ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Целью нашей организации является реализация услуг в области электронной отчетности и электронных торгов. Линейка VipNet же позиционирует себя как организатор электронного документооборота, не относящегося к текущим целям нашей организации. Несмотря на это, данное программное обеспечение имеет огромный потенциал и даже в нашей работе ему есть применение – портал Росаккредитации использует средства ПО VipNet для организации защищенного соединения между своим порталом и пользователем. Помимо этого, ряд муниципальных заказчиков может использовать данное ПО для организации защищенного соединения между своими филиалами и соответственно подключения к такому защищенному соединению конечных пользователей своих сервисов.

1.5 Ключевые носители для записи электронной подписи

Для записи электронной подписи можно использовать разные виды ключевых носителей. Речь идет именно о видах, т.е. это может быть:

- реестр
- дискета

- флэшка\карта памяти
- СД диск
- смарткарта

Технически мы можем записать КЭП на любой из выше перечисленных типов носителей. Все перечисленные носители, за исключением смарткарты, не имеют должного уровня защищенности и являются не надежными. Смарткарта - это специально разработанное устройство для хранения ключевой информации и СЕРТИФИЦИРОВАННОЕ соответствующими контролирующими органами по классу защищенности (ФСБ и ФСТЭК). При определенных обстоятельствах, по мнению ФСБ и ФСТЭК, данный носитель сможет сохранить ключевую информацию в безопасности. А все остальные типы носителей нет. Поскольку алгоритмы, используемые для применения КЭП одинаковые, то и требования к носителям также одинаковые. Желающим производить такие носители достаточно выполнить требования и начать продавать продукт. Поэтому мы видим, что на рынке присутствую рутокены, етокены и пр. Наиболее популярные носители приведены ниже. Характеристики у всех похожи. Выбор что продавать и что покупать остается за нами\пользователем.

Тип USB-носителя	Внешний вид USB-носителя	Ссылка на загрузку драйверов	PIN-код
ruToken		Драйверы Rutoken 32-bit (x86) Драйверы Rutoken 64-bit (x64)	12345678
eToken		eToken PKI Client 5.1 SP1 для Microsoft Windows x32 eToken PKI Client 5.1 SP1 для Microsoft Windows x64	1234567890
JaCarta LT		JC-PROClient-1.5.0.199_x32 JC-PROClient-1.5.0.199_x64	1234567890
MS-Key		MS_Key_driver_x64 MS_Key_driver_x86	11111111
Esmart*		ESMART PKI Client. CryptoPro ESMART Token (для КриптоПро CSP ниже 3.6 R3)	12345678
JaCarta LT Nano		JC-PROClient-1.5.0.199_x32 JC-PROClient-1.5.0.199_x64	1234567890

*Примечание: Для работоспособности данного носителя нужно установить оба драйвера.

Чтобы воспользоваться ЭП, понадобятся:

- Средства криптозащиты информации (программы)
- Носитель для хранения закрытого ключа
- **Сертификат ЭП** – это файл, который представляет из себя открытый ключ клиента, подписанный ЭЦП удостоверяющего центра. Бумажный сертификат содержит открытый ключ ЭП, ФИО его владельца, срок действия сертификата, область применения ключа, информация об организации, представителем которой является владелец ключа. Если у контрагента есть сертификат ЭП, он без труда сможет читать документы, подписанные этой ЭП.

Существует 2 основных варианта использования ключевой пары:

1. Вы подписываете документ ЭЦП, подтверждая свое авторство
2. Вы зашифровываете документ для одного единственного получателя

С технической точки зрения документооборот осуществляется так:

1. Электронный документ подписывается закрытым ключом организации. В подписанном ЭП документе ни получатель, ни отправитель уже не могут изменить ни одного символа.

2. При получении документ расшифровывается открытым ключом организации. Это дает ответ на два вопроса: вносились ли какие-то изменения в отчет после его подписания и действительно ли данная ЭП принадлежит организации, сдавшей отчетность.

1.7 Безопасность ЭП

Компрометация ключа – после получения клиентом в УЦ КЭП вся ответственность за его сохранность возлагается на клиента. Компрометация ключа происходит, в случае если клиенту известен факт несанкционированного доступа к его ключевой информации или есть на это подозрения. Теоретически к факту компрометации можно отнести и утерю ключевого носителя, и факт его кражи.

Случаи компрометации:

-Физическая утеря носителя информации

-Передача информации по открытым каналам связи

-Несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации, визуальный осмотр носителя информации посторонним лицом или подозрение, что данные факты имели место быть (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков, взлом учётной записи пользователя и т. п.)

-Перехват информации вредоносным ПО

-Перехват (подслушивание) звуковой информации

-Перехват ключа при распределении ключей

-Перехват информации с электрических каналов утечки

-Сознательная передача информации постороннему лицу

и другие, в зависимости от вида носителя защищаемой информации и способов работы с ним.

Действия при компрометации ключа:

Скомпрометированный ключ сразу же выводится из действия, взамен его вводится запасной или новый ключ – для отзыва сертификат клиент может обратиться к нам по телефону и, используя КОДОВУЮ ФРАЗУ из заявления на выпуск, ПРИОСТАНОВИТЬ действие ключа. Либо предоставить ЗАЯВЛЕНИЕ НА ОТЗЫВ сертификата. После чего сертификат будет отозван.

О компрометации немедленно оповещаются все участники обмена информацией. Ключ или сертификат вносятся в специальные списки, содержащие скомпрометированные ключи (стоп-листы, списки отзыва сертификатов и т. п.)

1.6 Нормативно-правовое поле использования электронной подписи

Основные нормативно-правовые акты (далее – НПА), регулирующие межкорпоративный обмен электронными документами:

Гражданский кодекс РФ регулирует использование электронных документов и электронной подписи при совершении сделок и заключении договоров (ст. 160, 434, 847 ГК РФ).

Федеральный закон № 63-ФЗ «Об электронной подписи» от 06.04.2011 регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 дает понятие электронного документа и смежных с ним областей, а также регулирует отношения, возникающие при обеспечении защиты информации, применении информационных технологий, осуществлении права на поиск, получение, передачу, производство и распространение информации.

Федеральный закон № 402-ФЗ «О бухгалтерском учете» от 06.12.2011 устанавливает единые требования к бухгалтерскому учету, а также разрешает составление первичных учетных документов в электронном виде и регулирует их использование.

Налоговый кодекс РФ определяет возможность использования электронных счетов-фактур (ст. 169, счёт-фактура).

Приказ Минфина РФ от 25.04.2011 № 50н «Об утверждении порядка выставления и получения счетов-фактур в электронном виде по телекоммуникационным каналам связи с применением электронной цифровой подписи» определяет порядок обмена электронными юридически значимыми счетами-фактурами.

Представленное выше законодательство составляет основу обмена электронными документами между организациями. Для того чтобы начать обмен необходимо подключиться к оператору электронного документооборота или заключить с контрагентами соглашения об обмене электронными документами напрямую.

1.7 ЭП для порталов

ЭП для Государственных услуг

Согласно 63 ФЗ об электронной подписи, мы выпускаем подписи для разных услуг, порталов и площадок.

Для использования подписи необходимо установить Крипто-Про и КриптоАРМ (к какому именно направлению требуется Крипто АРМ описано ниже в блоках о каждом портале).

Начнем с того что подпись могут получить как юридические лица так и физические лица.

Юридические лица выпускают подпись ЕПГУ для разных направлений указанных ниже:

ЭП ФСТ Федеральная служба по тарифам (ФСТ) осуществляет контроль за формированием тарифов (цен на товары, работы, услуги) организаций, относящихся к сфере государственного регулирования.

ЭП Россакредитация В российском законодательстве аккредитация определяется как ,подтверждение национальным органом по аккредитации соответствия юр лица или ИП критериям аккредитации, являющееся официальным свидетельством компетентности юр лица или ИП осуществлять деятельность в определенной области аккредитации.

ЭП Центральный Банк России.

223 ФЗ Для заказчиков бюджетных учреждений. Участие в аукционах.

ЭП Росфинмониторинг Федеральная служба по финансовому мониторингу является федеральным органом исполнительной власти, осуществляющим функции по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, а также функции национального центра по оценке угроз национальной безопасности, возникающих в результате отмывания доходов, полученных преступным путем.

ЭП Росимущество Федеральное агентство по управлению государственным имуществом (Росимущество) является федеральным органом исполнительной власти, осуществляющим функции по управлению федеральным имуществом функции по организации продажи приватизируемого федерального имущества, реализации имущества, арестованного во исполнение судебных решений

ЭП для Запрещенных сайтов В октябре 2012 года правительство осчастливило всех операторов связи Постановлением №1101 от 26 октября 2012 года "О единой автоматизированной информационной системе "Единый реестр доменных имён, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено".

ЭП для СРО В соответствие с ФЗ №261 "Об энергосбережении и повышении энергоэффективности" организации, сфера деятельности которых связанна с использованием энергетических ресурсов, должны сдавать копии энергетических паспортов в системе Министерства энергетики Российской Федерации.

ЭП для Ресурсоснабжающих организаций управляющие организации, ТСЖ, ЖК, ЖСК; иные лица, выполняющие работы по содержанию и ремонту общего имущества собственников помещений в многоквартирных домах должны представлять в форме электронного документа, подписанного усиленной квалифицированной электронной подписью: электронный паспорт многоквартирного дома;

электронный паспорт жилого дома; электронный документ о состоянии объектов коммунальной и инженерной инфраструктуры

Физические лица выпускают ЭП для наиболее востребованных государственных электронных услуг на ЕПГУ:

- Штрафы ГИБДД;
- Регистрация автомобилей;
- Налоговая задолженность физических лиц;
- Подача налоговой декларации;
- Сведения о недвижимости организаций;
- Предоставление сведений из государственного кадастра недвижимости;
- Предоставление информации о зарегистрированных организациях;
- Предоставление паспортных данных граждан РФ (открытые сведения);
- Подача налоговой декларации НДФЛ;
- Информирование о действующих налогах и сборах;
- Состояние счета в ПФР;
- Регистрация/снятие с учета по месту жительства
- Выдача загранпаспорта;
- Регистрация/снятие с регистрации авто;
- Дубликат ПТС;
- Справке о ходе, наличии, отсутствии исполнительного производства
- Для участия в торгах по банкротству.

ЭП для портала ЕФРСБ

В соответствии с Федеральным законом «О несостоятельности (банкротстве)» от 26.10.2002г. № 127-ФЗ, с 1 апреля 2011 года становится обязательной публикация сведений о банкротстве на специальном ресурсе в сети Интернет — Едином Федеральном реестре сведений о банкротстве (ЕФРСБ) для следующих участников процедур несостоятельности (банкротства):

арбитражные управляющие;

организаторы торгов;

саморегулируемые организации.

Единый Федеральный реестр сведений о банкротстве в свою очередь призван осуществить обработку собранной информации и раскрытие сведений о несостоятельности организации. ЕФРСБ содержит сведения, необходимые участникам электронных торгов, проводимых на электронных торговых площадках, созданных во исполнение Приказа Минэкономразвития от 15 февраля 2010 года № 54. Для работы в ЕФРСБ участникам необходимо приобрести сертификат ЭЦП в Удостоверяющем центре.

В стоимость комплекта входит Крипто-Про, ключевой носитель, сертификат ЭП, техническая поддержка пользователей.

ЭП для портала ЕФРСДЮЛ

С 1 января 2013 года вступили в силу требования Федерального закона от 18 июля 2011 года № 228-ФЗ публиковать сведения о фактах деятельности юридических лиц в специализированном федеральном информационном ресурсе — fedresurs.ru (Федресурс).

Единый федеральный реестр сведений о фактах деятельности юридических лиц (ЕФРСФДЮЛ) предназначен для раскрытия информации о деятельности юридических лиц и обеспечения прозрачности их работы. Основой данных реестра является информация из ЕГРЮЛ и ЕГРИП, загружаемая в реестр при регистрации новых юридических лиц и ИП или при внесении изменений в данные существующих. Помимо этого новый реестр содержит иную информацию о работе юридических лиц – сведения об уставном капитале, арбитражном производстве, реорганизации и т.д.

Пользователями реестра являются *сотрудники гос. органов, ответственные за публикацию информации о юридических лицах и ИП и сами юридические лица, вносящие дополнительные сведения о себе.*

Fedresurs.ru содержит две группы данных:

1. Часть информации, которую вносят сотрудники ФНС:

- запись о создании юридического лица (в том числе о создании юридического лица путем реорганизации);
- запись о том, что юридическое лицо находится в процессе реорганизации;
- запись о том, что юридическое лицо находится в процессе ликвидации;
- запись об исключении юридического лица из единого государственного реестра юридических лиц или о ликвидации юридического лица;
- запись об уменьшении или увеличении уставного капитала;
- запись об изменении адреса (места нахождения) юридического лица;

2. Часть информации, которую вносит юридическое лицо, на которое возложена обязанность по опубликованию соответствующих сведений:

- сведения о стоимости чистых активов юридического лица, являющегося акционерным обществом, на последнюю отчетную дату;
- сведения о получении лицензии, приостановлении, возобновлении действия лицензии, переоформлении лицензии, об аннулировании лицензии или о прекращении по иным основаниям действия лицензии на осуществление конкретного вида деятельности;
- сведения о вынесении арбитражным судом определения о введении наблюдения;
- сведения, внесение которых предусмотрено другими федеральными законами;
- иные сведения, которые юридическое лицо вносит по своему усмотрению, за исключением сведений, доступ к которым ограничен в соответствии с законодательством Российской Федерации.

ЭП для портала Банка России

Для работы с порталом Банка России требуется получить сертификат ЭП в доверенном Удостоверяющем центре. Сертификат ЭП необходим для подписания документов, представляемых участниками финансовых рынков в Банке России.

Список передаваемых через портал Банка России документов:

1. Отчетность профессиональных участников рынка ценных бумаг (РЦБ);
2. Заявки профессиональных участников РЦБ на выдачу/аннулирование лицензий; переоформление бланка лицензии, выдачу дубликата бланка лицензии, выдачу выписки из реестра лицензий;
3. Отчетность акционерных инвестиционных фондов, негосударственных пенсионных фондов, управляющих компаний инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, специализированных депозитариев инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов (РКИ);
4. Сведения о совершении инсайдером сделки (операции);
5. Уведомления лицензиата о заключении /прекращении действия (расторжении) договора с эмитентом на ведение реестра владельцев ценных бумаг;
6. Сведения о квалифицированных инвесторах;
7. Информация о структуре собственности, а также расчет собственных средств по состоянию на последний календарный день каждого месяца профессиональных участников РЦБ, управляющих компаний инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, товарных бирж и биржевых посредников;
8. Документы аккредитованных организаций, осуществляющих аттестацию специалистов финансовых рынков;
9. Уведомления маркет-мейкеров (*направляет только организатор торгов*);

10. Уведомления о допуске/прекращении допуска к торгам участника торгов (*направляет только организатор торгов*);
11. Иные документы, предусмотренные нормативными документами Банка России.

Подробнее с работой на портале можно ознакомиться на на официальном сайте Банка России по адресу: http://www.cbr.ru/sbrfr/

Для использования портала необходимо: сертификат ЭП, ключевой носитель, Крипто-Про, КриптоАрм.

ЭП для портала ФСТ

21.07.2015 Указом Президента РФ №373 Федеральная служба по тарифам (ФСТ) упразднена. Ее функции переданы Федеральной антимонопольной службе. Задачей ФСТ, а теперь ФАС является контроль за тарифами (цен на услуги, товары) предприятий, относящихся к сфере государственного регулирования.

Предприятия указанной категории (*субъекты естественной монополии в сфере ТЭК; субъекты естественной монополии в отрасли связи, а также в сфере услуг портов, аэропортов и других транспортных терминалов; субъекты естественной монополии, связанные с транзитом нефти и нефтепродуктов; субъекты монополии в области ЖКХ и т.д.*) обязаны подавать отчетность с полным расчетом стоимости тарифа. Регулятор либо одобряет, либо корректирует тариф.

Данный документооборот очень сложный и слабо регламентирован, из-за большой степени самостоятельности каждого местного «регулятора» (мы их будем называть РЭК — региональная энергетическая комиссия, в действительности их названия могут быть различными в каждом из регионов). Для оптимизации процесса сбора информации ФСТ разработала и внедрила Единую информационно-аналитическую систему (ЕИАС ФСТ).

Для работы в данной системе необходимо следующее программно-аппаратное обеспечение:

- ПО КриптоПро CSP
- Модуль ЕИАС ФСТ России: Мониторинг (распространяется бесплатно)
- Сертификат ключа электронной цифровой подписи
- Ключевой носитель

ЭП для портала СМЭВ

СМЭВ это единая Система Межведомственного Электронного Взаимодействия предназначенная для взаимодействия органов власти при предоставлении государственных услуг. СМЭВ это основа всей системы предоставления государственных и муниципальных услуг. Пользователь обращается в орган власти или специальный многофункциональный центр по принципу «единого окна». А все документы от различных ведомств, требуемые при предоставлении пользователю гос. услуги, запрашивают сами ведомства друг у друга через систему СМЭВ.

Информационные ресурсы, посвященные СМЭВ:

Технологический портал СМЭВ федерального уровня: http://smev.gosuslugi.ru/portal/

Информационный портал, посвященный закону 210-ФЗ: http://210fz.ru/mdx/

Согласно одному из пунктов этого документа, с 1 июля 2012 г. чиновники не имеют права требовать с обратившихся к ним за гос. услугами граждан дополнительные справки, которые и так есть в распоряжении других чиновников. Эти сведения органы власти должны получать друг у друга через СМЭВ.

Согласно пункту 1 Постановления Правительства РФ №111 от 9 февраля 2012 г. «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи» при организации межведомственного взаимодействия в целях предоставления гос. услуг применяется ***усиленная квалифицированная подпись***.

Виды подписей:

1. СМЭВ – должностное лицо + Росреестр для ОГВ субъекта РФ (код SMEVDLRR):

Усиленная квалифицированная электронная подпись для Системы межведомственного электронного взаимодействия (СМЭВ) используемая для формирования электронной подписи должностного лица органа государственной власти, уполномоченного направлять межведомственные запросы и ответы на поступившие межведомственные запросы с использованием СМЭВ/РСМЭВ, в том числе в Росреестр.

2. СМЭВ – должностное лицо + Росреестр для органа местного самоуправления (код SMEVDLOMS):

Усиленная квалифицированная электронная подпись для Системы межведомственного электронного взаимодействия (СМЭВ) используемая для формирования электронной подписи должностного лица органа государственной власти, уполномоченного направлять межведомственные запросы и ответы на поступившие межведомственные запросы с использованием СМЭВ/РСМЭВ, в том числе в Росреестр.

3. СМЭВ – должностное лицо (код SMEVDL):

Усиленная квалифицированная электронная подпись для Системы межведомственного электронного взаимодействия (СМЭВ) используемая для формирования электронной подписи должностного лица органа государственной власти, уполномоченного направлять межведомственные запросы и ответы на поступившие межведомственные запросы с использованием СМЭВ/РСМЭВ.

4. СМЭВ – для автоматических систем (код SMEVAS):

Усиленная квалифицированная электронная подпись для Системы межведомственного электронного взаимодействия (СМЭВ) используемая для формирования электронной подписи органа государственной власти.

Согласно вышерассмотренным нормативно-правовым актам, получить ЭП обязаны *все государственные органы любого уровня (федерального и муниципального), в должностные обязанности работников которых входит работа с информацией от других органов государственного профиля.* Основная цель использования ЭП - отправка межведомственных запросов и ответные письма на поступившие запросы с использованием технологического портала СМЭВ/РСМЭВ.

Для использования портала необходимо: сертификат ЭП, ключевой носитель, Крипто-Про JCP.

ЭП для портала Росреестра

1 января 2012 года все регионы России перешли на новый порядок учета объектов капитального строительства (зданий, сооружений, помещений, объектов незавершенного строительства), а услуги, которые ранее населению оказывали работники БТИ, отныне предоставляют новые специалисты – кадастровые инженеры.

Кадастровый инженер — физическое лицо, осуществляющее кадастровую деятельность, которое имеет действующий квалификационный аттестат кадастрового инженера.

С 1 октября 2013 года данная категория служащих обязана все технические планы, межевые планы, и акты обследования оформлять исключительно в электронном виде с использованием **усиленной квалифицированной электронной подписи** и отправляет их на регистрацию в Кадастровую палату.

На портале https://portal.rosreestr.ru осуществляются следующие действия:

- формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество (ЕГРП) и сделок с ним;
- формирование запроса о предоставлении сведений из государственного кадастра недвижимости (ГКН);
- формирование кадастровым инженером документов для получения государственных услуг в сфере ведения государственного кадастра недвижимости и по другим направлениям взаимодействия с Росреестром;
- иные электронные услуги.

В работе с сайтом Росреестра ЭП могут использовать практически все субъекты, в том числе:

- *Индивидуальные предприниматели и другие физлица;*
- *Квалифицированные кадастровые инженеры;*

- *Органы федеральных служб местного самоуправления и государственные органы власти;*
- *Финансовые организации и институты (банки, застройщики, агентства недвижимости и др.)*

Отныне к вышеперечисленным добавилось и основное требование: кадастровый инженер должен обладать квалификационным аттестатом кадастрового и сертификатом электронной цифровой подписи (ЭП) кадастрового инженера.

Для использования портала необходимо: сертификат ЭП, ключевой носитель, Крипто-Про, КриптоАрм.

ЭП для портала Росимущество

Федеральное агентство по управлению государственным имуществом (Росимущество) является федеральным органом исполнительной власти, осуществляющим функции по управлению федеральным имуществом, функции по организации продажи приватизируемого федерального имущества, реализации имущества, арестованного во исполнение судебных решений или актов органов, которым предоставлено право принимать решения об обращении взыскания на имущество, функции по реализации конфискованного, движимого бесхозяйного, изъятого и иного имущества, обращенного в собственность государства в соответствии с законодательством Российской Федерации, функции по оказанию государственных услуг и правоприменительные функции в сфере имущественных и земельных отношений.

В компетенцию Росимущества входит:

- осуществление общих государственных мер в отношении имущественных и земельных связей;
- выделение своих прав собственника в пределах установленных правил;
- конфискация у предприятий и организаций федеральной недвижимости, используемой не по назначению;
- приватизация федерального имущества;
- разделение собственности на ее различные виды;
- участие в проведении процесса банкротства;
- охрана законных прав владения федеральным имуществом;
- учет федерального имущества.

Электронная подпись предназначена для подписания юридически значимых электронных документов в рамках портала, и получить ее могут:

- *Представители Акционерных обществ с долей государственного участия 50% и более*
- *Профессиональные директора*
- *Представители Федеральных государственных унитарных предприятий*
- *Представители Федеральных органов исполнительной власти*

Производить оперативный мониторинг и вести учет данных при помощи ЭП могут и сами сотрудники Росимущества.

Для использования портала необходимо: сертификат ЭП, ключевой носитель, Крипто-Про.

ЭП для портала Росфинмониторинга

Федеральная служба по финансовому мониторингу (Росфинмониторинг) является федеральным органом исполнительной власти, осуществляющим функции по легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, по выработке государственной политики, нормативно-правовому регулированию в этой сфере, по координации соответствующей деятельности других федеральных органов исполнительной власти, а также функции национального центра по оценке угроз национальной безопасности, возникающих в результате легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма и распространения оружия массового уничтожения, по выработке мер противодействия этим угрозам.

Основными направлениями надзорной деятельности Федеральной службы по финансовому мониторингу являются:

- Проведение поверок и ведение учета организаций, осуществляющих операции с денежными средствами или иным имуществом, в сфере деятельности которых отсутствуют надзорные органы.
- Координация деятельности надзорных органов и взаимодействие с ними в области отмывания денег и финансирования терроризма
- Взаимодействие с федеральными органами исполнительной власти, органами прокуратуры, органами исполнительной власти субъектов Российской Федерации, общественными объединениями и иными организациями по вопросам противодействия отмывания денег и финансирования терроризма

Объектами контроля со стороны Росфинмониторинга и его территориальных органов являются:

- *Лизинговые компании*
- *Организации, оказывающие посреднические услуги при осуществлении сделок купли-продажи недвижимого имущества*
- *Операторы по приему платежей*
- *Коммерческие организации, заключающие договоры финансирования под уступку денежного требования в качестве финансовых агентов*
- *Ломбарды*
- *Банки*
- *Микрофинансовые организации*

В соответствии с установленным Федеральным законом № 115-ФЗ от 13.07.2001 порядком предоставления отчетности, сведения о финансовых операциях могут представляться в электронном виде с использование **квалифицированной электронной подписи**.

Организации, представляющие более 10 сообщений в течение одного календарного года, информацию об операциях (сделках) должны представлять исключительно в электронном виде.

Для представления сообщений в электронном виде Росфинмониторинг предлагает следующий комплекс программных средств:

Личный кабинет организации на портале Росфинмониторинга;

АРМ «Организация» — программное обеспечение по предоставлению сведений через сервисы Портала Росфинмониторинга, доступно для скачивания в Личном кабинете.

Среди физлиц на портале Росфинмониторинга обязательно получение ЭЦП для адвокатов и нотариусов. Ниже приведен общий список юридических лиц, получение сертификата электронно-цифровой подписи для которых происходит в обязательном порядке.

- ЭП для потребительских и сельхоз кооперативов, а также других кредитных организаций;
- ЭП для обществ взаимного страхования и страховых компаний;
- ЭП для компаний осуществляющих куплю-продажу драгоценных металлов, в том числе ломбардов;
- ЭП для букмекерских контор, тотализаторов, лотерей и прочих институтов, чья прибыльная деятельность основана на риске и вероятности.
- ЭП для агентств недвижимости, частных риэлтеров и прочих посредников на данном рынке;
- Получение сертификата ЭП для поставщиков услуг связи.

Для использования портала необходимо: сертификат ЭП, ключевой носитель, Крипто-Про.

ЭП для НССО

Согласно Решению президиума НССО о «Порядке защиты информационных ресурсов НССО при предоставлении страховыми компаниями регламентной отчетности», каждое юридическое лицо, осуществляющее деятельность в сфере страховых отношений, либо уполномоченный от такого юридического лица обязаны:

- Зарегистрироваться в закрытом личном кабинете сайта НССО;
- Направить на адрес closedarea@nsso.ru сканированную копию официального письма, за подписью руководителя компании - члена НССО;
- Получить в аккредитованном Удостоверяющем центре квалифицированную ЭП и сертификат ключа.

Страховая компания предоставляет следующие формы регламентной отчетности:

- Акт взаиморасчетов к «Договору облигаторного перестрахования рисков гражданской ответственности владельца опасного объекта за причинение вреда в результате аварии на опасном объекте» от 30.12.2011 года;
- Отчет об отчислениях от страховых премий по заключенным договорам обязательного страхования гражданской ответственности владельца опасного объекта за причинение вреда в результате аварии на опасном объекте для целей осуществления компенсационных выплат;
- Сведения о наличии и движении бланков страховых полисов ОСОПО - Форма 4 - НССО;
- Сведения об утраченных, украденных, испорченных и уничтоженных бланках страховых полисов ОСОПО - Форма 1 - НССО; И т.д.

ЭП для ГИС ГМП

Государственная информационная система о государственных и муниципальных платежах (ГИС ГМП). Федеральный закон от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»

ГИС ГМП является информационной системой, предназначенной для размещения и получения информации об уплате физическими и юридическими лицами платежей за оказание государственных и муниципальных услуг, услуг, указанных в части 3 статьи 1 и части 1 статьи 9 настоящего Федерального закона, платежей, являющихся источниками формирования доходов бюджетов бюджетной системы Российской Федерации, а также иных платежей, в случаях, предусмотренных федеральными законами.

Банк, иная кредитная организация, организация федеральной почтовой связи, территориальный орган Федерального казначейства (иной орган, осуществляющий открытие и ведение лицевых счетов в соответствии с бюджетным законодательством Российской Федерации), в том числе производящие расчеты в электронной форме, а также иные органы или организации, через которые производится уплата денежных средств заявителем за государственные и муниципальные услуги, услуги, указанные в части 3 статьи 1 и части 1 статьи 9 настоящего Федерального закона, а также иных платежей, являющихся источниками формирования доходов бюджетов бюджетной системы Российской Федерации обязаны незамедлительно направлять информацию об их уплате в ГИС ГМП.

Преимущества ЭЦП для ГИС ГМП

- Полученное зашифрованным путем при помощи ЭЦП сообщение от участников ГИС ГМП может сохраняться на портале или пересылаться по электронной почте;
- При получении, подписанного ЭЦП сообщения пользователь может убедиться в подлинности документа;
- Информация, зашифрованная подобным способом, надежно защищена от хищения, уничтожения и подделки.

ЭП для подачи документов в ВУЗы

Порядок приема документов в высшие учебные заведения Российской Федерации регламентируется приказом № 2895 Министерства образования и науки РФ от 28 декабря 2011 года. Согласно регламенту Приказа, будущий учащийся (абитуриент) имеет право подать заявление в цифровой форме о зачислении на первый курс вуза, при условии, что ВУЗ располагает такой функцией подачи документов.

На данный момент крупнейшие учебные заведения поставили условия и сроки подачи документов в ВУЗы, в их числе ряд Московских, Санкт-Петербургских и Краснодарских университетов.

Преимущества подачи документов в ВУЗЫ с использованием ЭП

- Дистанционная подача документов для иногородних студентов;
- Отказ от длинных очередей в приемную комиссию;
- Быстрая и защищенная отправка данных по электронной почте;
- Ускоренные сроки рассмотрения документов и зачисления в ВУЗ;
- Экономия затрат времени, усилий и денег и т.д.

Согласно положению Приказа № 2895 Министерства образования и науки от 28 декабря 2011 года и ссылок на Федеральные законы № 1-ФЗ «Об электронной цифровой подписи» , № 149-ФЗ «Об

информации, информационных технологиях и защите информации» и № 126-ФЗ «О связи» действует следующий регламент. Чтобы отправить информацию об абитуриенте в цифровом виде в приемную комиссию, ее нужно заверить цифровой подписью посредством сертификата ЭП с использованием приложения «КриптоАРМ». Это занимает около двух минут, документы для подачи в ВУЗ надежно сохраняются в электронном виде и защищаются от искажения или удаления информации.

ЭП для портала Минэнерго

Ежеквартальное представление копий энегопаспортов энергоаудиторами в уполномоченный федеральный орган (Минэнерго России) является прямой обязанностью, предоставление осуществляется в соответствии со статьей 17 Закона РФ "Об энергосбережении ...".

Для подписания энергопаспорта должностным уполномоченным лицом допускается исключительно использование квалифицированной электронной подписи (ЭП), полученной в аккредитованном удостоверяющем центре.

Согласно приказу Минэнерго, предоставить энергопаспорта обязаны:

- органы государственной власти, в т.ч. местного самоуправления, наделенные правами юрлиц;
- организации с государственной паевой долей или муниципальные организации;
- организации, совокупные затраты которых на потребление энергоресурсов превышают 10 млн. российских рублей за календарный год;
- организации, проводящие мероприятия в области энергосбережения и повышения энергетической эффективности, чье финансирование отчасти или полностью осуществляется за счет средств местных бюджетов, федерального бюджета, бюджетов субъектов РФ.
- организации, осуществляющие регулируемые виды деятельности
- организации, осуществляющие производство и (или) транспортировку энергоресурсов;

Паспорт направляется в Минэнерго РФ раз в три месяца со времени регистрации. Документ должен быть предоставлен в электронном виде с Электронно-цифровой подписью.

ЭП для ФТС

Право на получение ЭП имеет любой участник внешнеэкономической деятельности. Это право регламентируется приказом ФТС №52 от 24.01.2008 «О внедрении информационной технологии представления таможенным органам сведений в электронной форме для целей таможенного оформления товаров, в том числе с использованием международной ассоциации сетей «Интернет», участники внешнеэкономической деятельности, декларирующее товары, могут заявлять в электронной форме сведения, подлежащие указанию в таможенной декларации, а также представлять сведения из документов, необходимых для таможенного оформления товаров в соответствии с выбранным таможенным режимом, и представлять их таможенному органу посредством электронного способа обмена информацией. Компания, желающая получить электронную подпись, должна предоставить необходимый комплект документов и заполненную заявку в Главный научно-исследовательский вычислительный центр (ГНИВЦ) ФТС РФ. Уполномоченное ведомство проверяет верность заявленных сведений (реквизиты компании, полномочия руководителя, данные на сотрудника, получающего подпись) и принимает решение о выдаче сертификата. Сотрудник, получающий подпись должен быть трудоустроен в компании по всем правилам Трудового Кодекса.

С 1 января 2014 года электронное представление сведений стало обязательным при процедурах таможенного оформления товаров. Декларации «на бумаге» подаются в исключительно редких случаях — это заявление таможенных режимов: «отказ в пользу государства», «уничтожение», «специальная таможенная процедура». Общая доля деклараций, подаваемых под этими режимами не превышает 0.5% от всех ДТ, обрабатываемых таможенными органами.

Технические нюансы

Для использования цифровой подписи в электронном декларировании товаров понадобится установить Крипто-про (отвечает за «подписание» и шифрование отправляемых в таможенные органы документов посредством сети Интернет) и КриптоАрм.

Таможенное декларирование - это заявление по установленной форме точных сведений о товарах в соответствии с требованиями избранного таможенного режима или специальной таможенной процедуры.

ЭП для Росаккредитации

Росаккредитация — федеральный орган исполнительной власти, осуществляющий функции по формированию единой национальной системы аккредитации и осуществлению контроля над деятельностью аккредитованных лиц.

В общем смысле аккредитация представляет собой процедуру признания (подтверждения) государственными органами особых полномочий различного рода субъектов (образовательных учреждений, научных организаций, медицинских учреждений, коммерческих банков и т.д.).

Аккредитуются:

- организации (вузы, СМИ)
- Лаборатории
- услуги, для оценки качества которых, потребитель не обладает достаточной компетенцией

К аккредитуемым услугам относят: услуги по образованию, услуги по проведению испытаний (испытательные лаборатории), услуги по клинической диагностике (медицинские лаборатории), услуги по калибровке (калибровочные лаборатории), услуги по сертификации (органы по сертификации) и т. п. Как правило, аккредитацию проводят органы по аккредитации, которые осуществляют свою деятельность по определённым правилам и процедурам.

К примеру: Высшие учебные заведения должны получать разрешение государства на образовательную деятельность. Это установление или подтверждение государственного аккредитационного статуса образовательного учреждения (институт, академия, университет), уровня реализуемых образовательных программ и их направленности, а также соответствия содержания и качества подготовки выпускников.

Федеральная служба по аккредитации была образована указом Президента РФ от 24 января 2011 года № 86 в целях повышения эффективности государственного управления в сфере аккредитации.

Полномочия:

- проводит аккредитации;
- ведёт реестры;
- контролирует деятельность аккредитованных лиц.

Получение ЭП обязательно для пользователей ФГИС Росаккредитации, осуществляющих подписание информации в системе. Необходимо обеспечить рабочее место лицензией на право использования КриптоАРМ и КриптоПро CSP, а также приобрести ViPNet (только для Лабораторий).

Для получения доступа к ФГИС Росаккредитации необходимо пройти регистрацию в Единой системе идентификации и авторизации (в соответствии с постановлением Правительства Российской Федерации от 10 июля 2013 г. № 584).

Для подключения необходимо от имени руководителя организации в адрес Росаккредитации направить заявление о регистрации во ФГИС Росаккредитации с указанием реквизитов аттестата аккредитации, СНИЛС руководителя, копию сертификата ЭП и СНИЛС администратора (при необходимости).

ЭП для Запрещенных сайтов

В октябре 2012 года правительство осчастливило всех операторов связи Постановлением №1101 от 26 октября 2012 года "О единой автоматизированной информационной системе "Единый реестр доменных имён, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено". В связи с этим постановлением, каждый провайдер обязан блокировать доступ к сайтам, находящимся в списке запрещенных. Чтобы получить доступ к реестру оператору требуется сформировать специальный запрос и подписать его квалифицированной подписью.

Создание Единого реестра доменных имен рассматривалось Правительством РФ довольно давно, но определенность в этом вопросе достигнута сравнительно недавно с выходом Закона «О защите детей от противоправной информации», который был принят Госдумой в начале июля 2012 года.

Предполагается, что список запрещенных сайтов, включающий в себя информацию, какие сайты запрещены, содержание которых может причинить вред здоровью и развитию детей, будет обновляться ежедневно.

На сегодняшний день перечень запрещенных сайтов формируется силами трех сторон: федеральные органы исполнительной власти, хостинг-провайдеры и операторы связи. В реестр запрещенных сайтов в РФ могут быть добавлены сайты, если они содержат информацию, запрещенную судебным решением. Также коррективы в реестр запрещенных сайтов могут вноситься и без вмешательства суда, по решению уполномоченных органов: МВД — в отношении информации факта публикации детской порнографии, ФСКН — в отношении информации о сбыте наркотиков, Роспотребнадзора — о пропаганде самоубийств, Роскомнадзора — в отношении информации, которая относится к любой из вышеперечисленных категорий.

Принцип взаимодействие хостинг-провайдеров операторов связи и Роскомнадзора выглядит следующим образом:

1. Некое лицо заполняет заявку на сайте Роскомнадзора, в которой указывает данные ресурса, который, по их мнению, может содержать запрещенную информацию.
2. Роскомнадзор производит проверку подозрительного ресурса на предмет факта нарушения норм ФЗ №149.
3. Роскомнадзор направляет письмо хостинг-провайдеру с требованием удалить соответствующую страницу или приостановить доступ к ресурсу.
4. Для выполнения предписания Роскомнадзора, хостинг-провайдеру нужно оформить квалифицированную электронную подпись, для возможности обращения к реестру запрещенных сайтов.
5. В случае если хостинг-провайдер в течение суток не выполняет данное предписание, а также в случае местонахождения интернет-страницы на зарубежном хостинге, Роскомнадзор обращается напрямую к операторам связи с требованием заблокировать доступ к странице с противоправной информацией.
6. Для того чтобы выполнить предписание Роскомнадзора, оператору связи так же нужно оформить квалифицированную электронную подпись, для того чтобы запрещенные интернет сайты подверглись блокированию, до момента удаления противоправной информации.
7. Если оператор связи не выполняет предписание Роскомнадзора, оператору грозит отзыв телематической лицензии и приостановление деятельности.

Требования, которые предъявляет Роскомнадзор к запросам, специфические:

1. запрос должен быть в формате XML
2. запрос должен быть подписан электронной подписью
3. подпись должна быть обязательно квалифицированной
4. подпись должна быть открепленной (отсоединенной) в формате PKCS#7

ЭП для ЕГАИС

ЕГАИС (Единая государственная автоматизированная информационная система) — автоматизированная система, предназначенная для государственного контроля за объёмом производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции.

ЕГАИС нужен для:

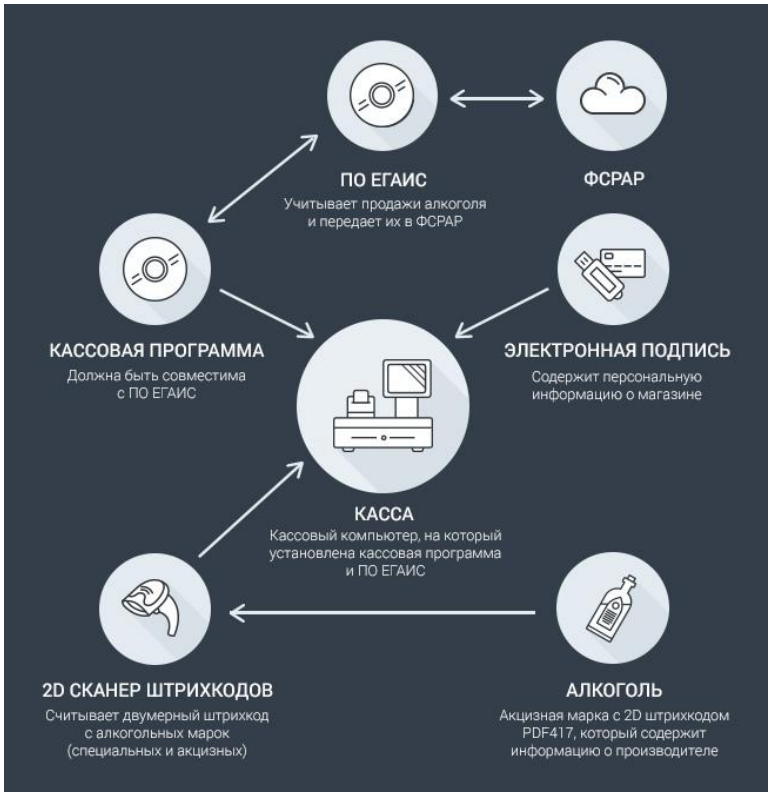
- государственного регулирования в области производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции направлено на защиту экономических интересов Российской Федерации, обеспечение нужд потребителей в указанной продукции, а также на повышение её качества и проведение контроля за соблюдением законодательства, норм и правил в регулируемой области;
- обеспечения единого контроля и прозрачности для участников рынка продажи алкогольной продукции;
- Затруднения распространения контрафактной продукции.

Действие настоящего Федерального закона не распространяется на:

- деятельность физических лиц, производящих не в целях сбыта продукцию, содержащую этиловый спирт;
- обращение лекарственных средств, содержащих этиловый спирт, зарегистрированных уполномоченным федеральным органом исполнительной власти;
- деятельность аптечных организаций, связанную с изготовлением и отпуском лекарственных препаратов, содержащих этиловый спирт и изготавливаемых по рецептам на лекарственные препараты и в соответствии с требованиями медицинских организаций;

• деятельность организаций, связанную с обращением лекарственных препаратов для ветеринарного применения, содержащих этиловый спирт и прошедших государственную регистрацию в уполномоченных федеральных органах исполнительной власти.

Схема работы, взаимодействие участников



На каждой бутылке крепкого алкоголя и вина есть федеральная специальная марка (для отечественного алкоголя) или акцизная марка (для импортного). На неё нанесен двухмерный штрихкод PDF417 с информацией о производителе, наличии лицензии, дате розлива и другими параметрами. Для распознавания двумерного штрихкода нужен 2D сканер. Он считывает с марки информацию, система её обрабатывает и передаёт на сервер Росалкогольрегулирования.

Без 2D сканера невозможно будет продавать крепкий алкоголь и вино. Исключение составляют только магазины в населённых пунктах с численностью менее 3000 человек и без подключения к интернету.

Для подключения ЕГАИС необходимы:

- персональный компьютер;
- интернет-соединение от 256 кбит/с и выше;
- сканер двухмерных штриховых кодов PDF417;
- кассовая программа, совместимая с ПО ЕГАИС;
- установленное ПО ЕГАИС;
- ключевой носитель с электронной подписью.

Как работает ЕГАИС:

1. Кассир открывает чек.
2. 2D сканер считывает код EAN 13.
3. Программное обеспечение при помощи кода устанавливает, является ли продукт алкогольным или нет. Если это алкоголь – то появляется дополнительное поле.
4. В дополнительное поле 2D сканер считывает код PDF417.
5. Если штрих-код PDF417 считывается успешно, то продукция добавляется в чек.
6. Кассир нажимает ИТОГ.
7. Если в чеке присутствует алкогольная продукция , то формируется xml-файл в соответствии с данными. Файл отправляется на транспортный модуль ЕГАИС (серверу на котором установлено ПО ЕГАИС).
8. Данные чека записываются в базу данных, фискальную память и ЭКЛЗ.
9. Транспортный модуль подписывает чек с помощью электронной подписи и возвращает в кассовую программу ответ в виде отпечатка электронной подписи и уникальный идентификатор ЕГАИС.

Для подписания чеков, установления и шифрованного соединения используется аппаратный крипто-ключ JaCarta SE PKI/ГОСТ.

10.Если кассовое ПО успешно получило отпечаток и идентификатор от транспортного модуля, то касса выводит на печать подотчет (слип), содержащий отпечаток электронной подписи и идентификатор в виде QR-кода.

11.Чек закрывается.

12.Возврат продукции осуществляется также как и продажа, только с отрицательным знаком через транспортный модуль системы ЕГАИС.

ЭП для Росалкогольрегулирования (ФСРАР)

В соответствии с Федеральным законом от 22.11.1995 г. № 171 «О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции» декларированию подлежат объемы производства, оборота и (или) использования для собственных нужд этилового спирта, алкогольной и спиртосодержащей продукции.

Организации, осуществляющие розничную продажу алкогольной и спиртосодержащей продукции, и индивидуальные предприниматели, осуществляющие розничную продажу пива и пивных напитков, также обязаны осуществлять учет и декларирование объема их розничной продажи.

9 августа 2012 г. подписано постановление N 815 «О представлении деклараций об объеме производства, оборота и (или) использования этилового спирта, алкогольной и спиртосодержащей продукции, об использовании производственных мощностей».

Сертификат ЭП, предназначенный для сдачи деклараций в Росалкогольрегулирование, выдается только на имя руководителя организации (руководителя филиала организации, уполномоченного заместителя руководителя организации), либо на имя индивидуального предпринимателя, осуществляющего розничную продажу пива и пивных напитков.

Порядок представления деклараций в электронном виде (Отчетность в Росалкоголь регулирование):

приобрести электронную подпись и все необходимое программное обеспечение;

зарегистрировать свою организацию в личном кабинете ФСРАР;

создать отчет с помощью бесплатной программы подготовки деклараций;

зашифровать и подписать отчет;

загрузить отчет на портал ФСРАР.

Декларации представляются ежеквартально не позднее 10-го числа месяца, следующего за отчетным периодом, за IV квартал — не позднее 20-го числа месяца, следующего за отчетным периодом.

Декларирование осуществляется в электронной форме с применением электронной подписи (ЭП). Формы деклараций утверждены Приложением к Постановлению правительства РФ от 9 августа 2012 г. № 815. Для заполнения деклараций рекомендуется использовать бесплатное программное обеспечение «Декларант-Алко».