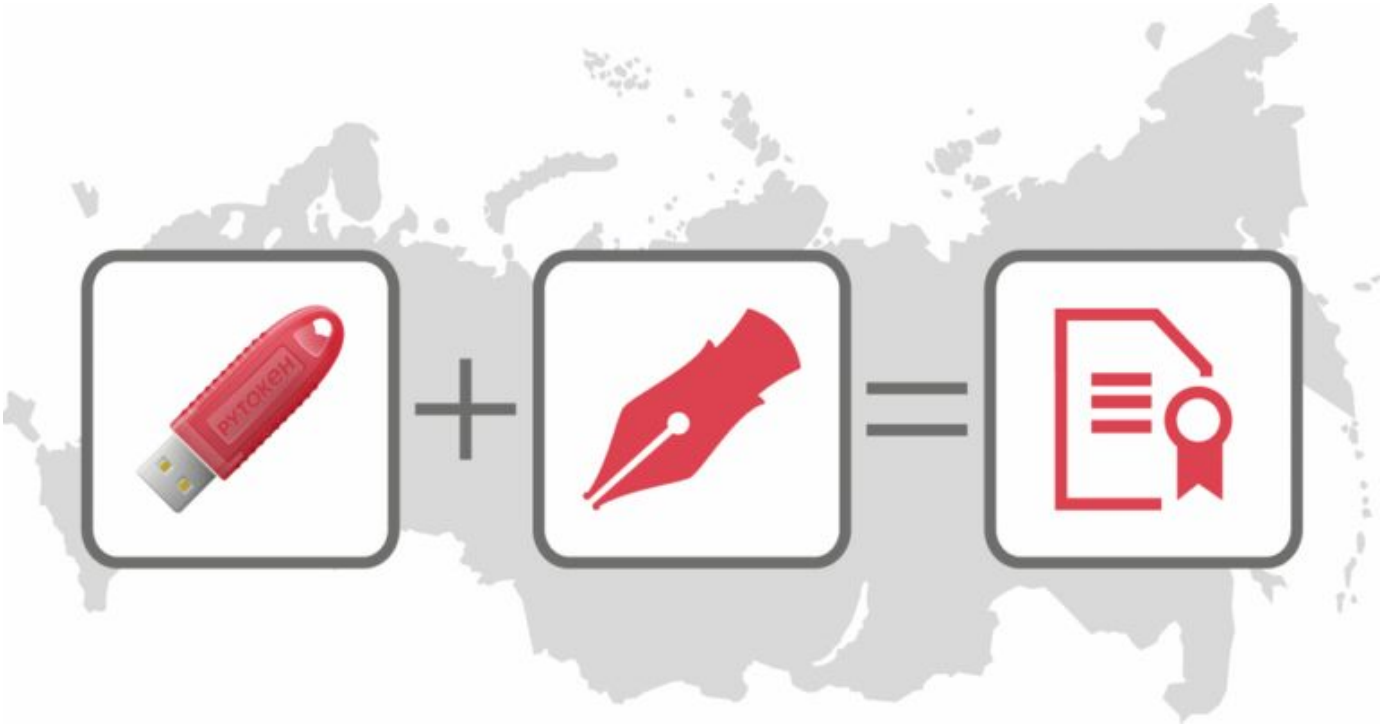
ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ



преп. ИБ АНО ПО «БИТ»
Околот Д.Я.

ПОНЯТИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ (ЭЦП)

ЭЦП – это криптографическое средство, которое позволяет удостовериться в отсутствие искажений в тексте электронного документа, а в соответствующих случаях – идентифицировать лицо, создавшее такую подпись.

ЭЦП используется в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе.

ЭЦП используется в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе.

ПОНЯТИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ (ЭЦП)

Электронная цифровая подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию (Федеральный закон "Об электронной подписи" № 63-ФЗ от 06.04.2011г.).

ПОНЯТИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ (ЭЦП)

Электронная подпись (ЭП) – это особый реквизит документа, который позволяет установить отсутствие искажения информации в электронном документе с момента формирования ЭП и подтвердить принадлежность ЭП владельцу. Значение реквизита получается в результате криптографического преобразования информации.

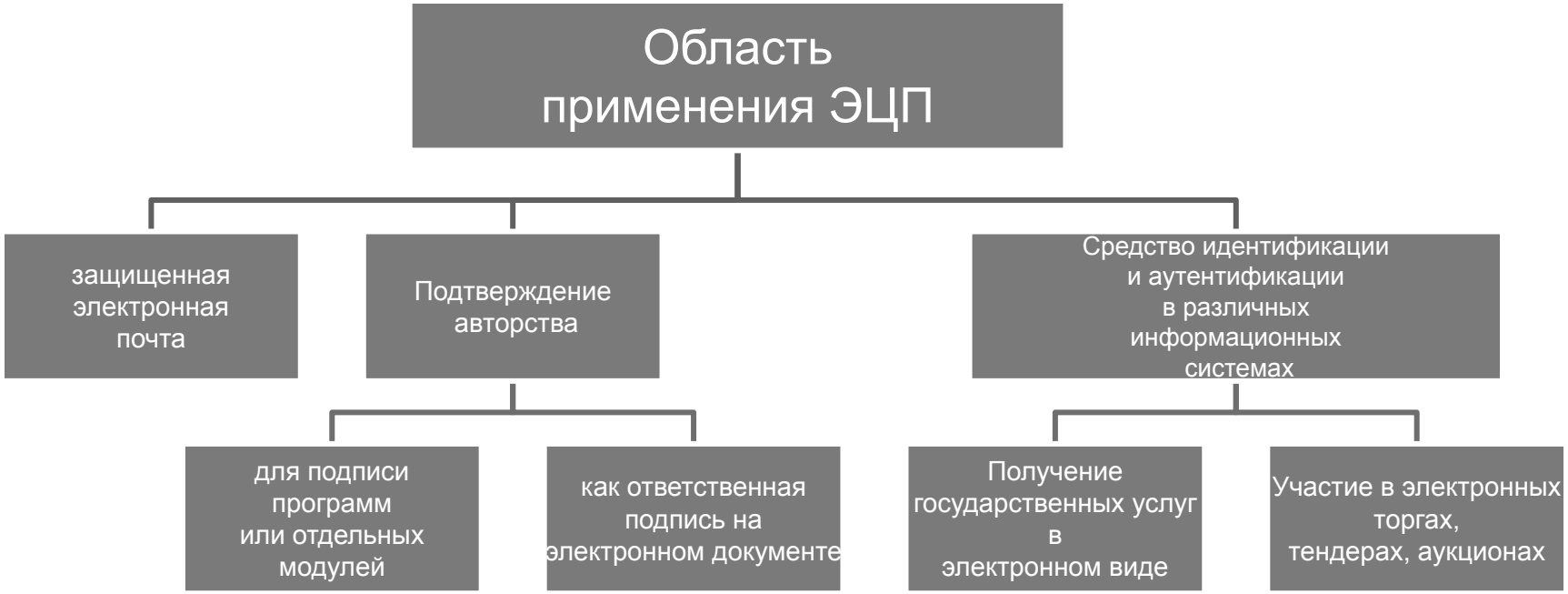
Сертификат электронной подписи – документ, который подтверждает принадлежность открытого ключа (ключа проверки) ЭП владельцу сертификата. Выдаются сертификаты удостоверяющими центрами (УЦ) или их доверенными представителями.

Владелец сертификата ЭП – физическое лицо, на чье имя выдан сертификат ЭП в удостоверяющем центре. У каждого владельца сертификата на руках два ключа ЭП: закрытый и открытый.

Закрытый ключ электронной подписи (ключ ЭП) позволяет генерировать электронную подпись и подписывать электронный документ. Владелец сертификат обязан в тайне хранить свой закрытый ключ.

Открытый ключ электронной подписи (ключ проверки ЭП) однозначно связан с закрытым ключом ЭП и предназначен для проверки подлинности ЭП.

ОБЛАСТЬ ПРИМЕНЕНИЯ ЭЦП

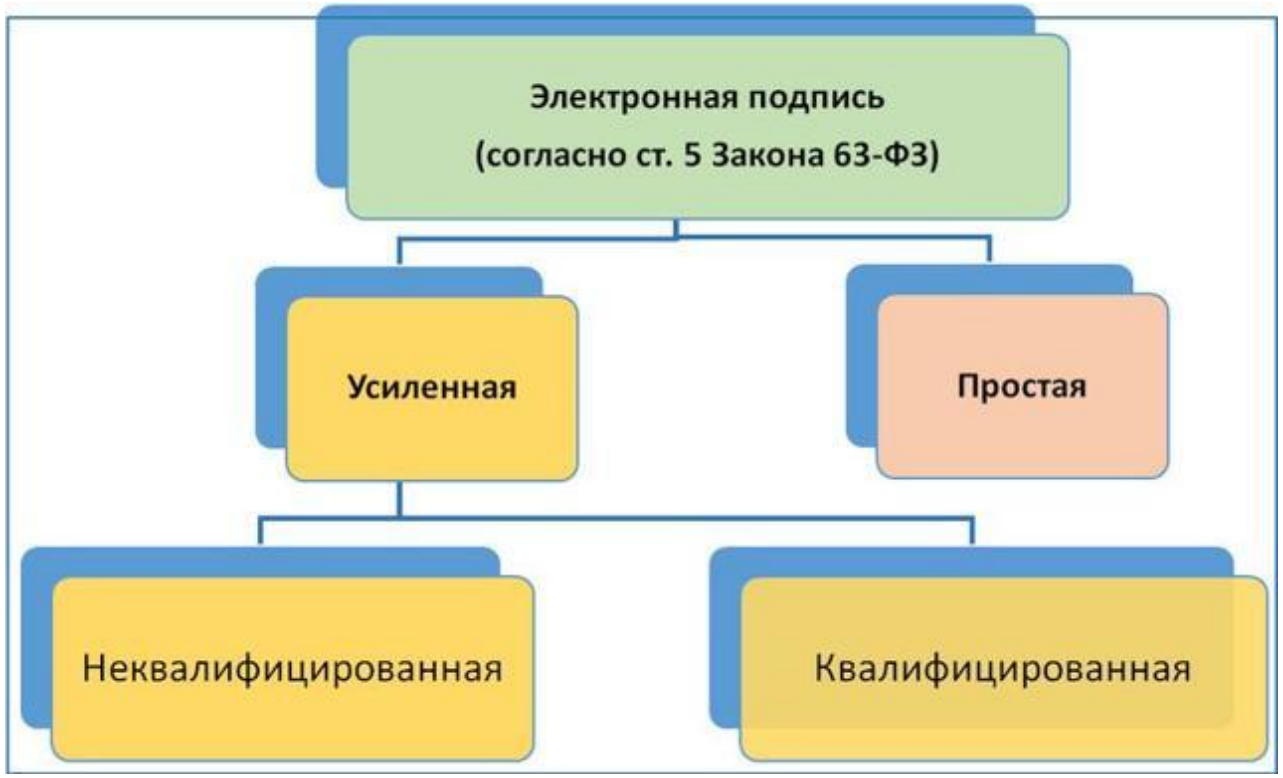


ВИДЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ (ЭЦП)

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

Подписи обладают разной степенью защиты и неравнозначны. Организации сами оценивают риски и решают, какую подпись лучше использовать для той или иной системы или документа.

ВИДЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ (ЭЦП)



ВИДЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ (ЭЦП)

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.

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.

ПРОСТАЯ ЭЦП

Случается, что пользователь в течение дня несколько раз использует простую ЭП, не осознавая этого. Под простой подписью понимают комбинацию логина и пароля, которая применяется для входа на сайт, получения доступа к электронной почте, оплаты товаров или услуг в режиме онлайн. Она необходима для идентификации пользователя, совершившего те или иные действия. В зависимости от серьезности операции выдвигаются требования к вводимому коду. Нередко при регистрации всплывает окно «Данный логин уже используется». Это говорит о том, что каждая простая электронная подпись на данном ресурсе уникальна и закреплена за определенным человеком. При совершении финансовых операций приходит уведомление, что логин и пароль пользователя являются секретной информацией, которую не рекомендуется хранить в свободном доступе и передавать третьим лицам.

НЕКВАЛИФИЦИРОВАННАЯ ЭЦП

это электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

КВАЛИФИЦИРОВАННАЯ ЭЦП

это электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным настоящим Федеральным законом, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

ПРИЗНАНИЕ КВАЛИФИЦИРОВАННОЙ ЭЦП

Квалифицированная электронная подпись признается действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении следующих условий:

1) квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата;

2) квалифицированный сертификат действителен на момент подписания электронного документа

3) имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания.

4) квалифицированная электронная подпись используется с учетом ограничений, содержащихся в квалифицированном сертификате лица, подписывающего электронный документ (если такие ограничения установлены).

ПРИЗНАНИЕ КВАЛИФИЦИРОВАННОЙ ЭЦП

Для того чтобы электронный документ считался подписанным простой электронной подписью необходимо выполнение в том числе одного из следующих условий:

- простая электронная подпись содержится в самом электронном документе;

- ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

ЭЦП ОБЕСПЕЧИВАЕТ

- Удостоверение источника документа. В зависимости от деталей определения «документа» могут быть подписаны такие поля как автор, внесённые изменения, метка времени и т. д.

- Защиту от изменений или подделки документа. При любом случайном или преднамеренном изменении документа (или подписи) изменится хэш, следовательно подпись станет недействительной.

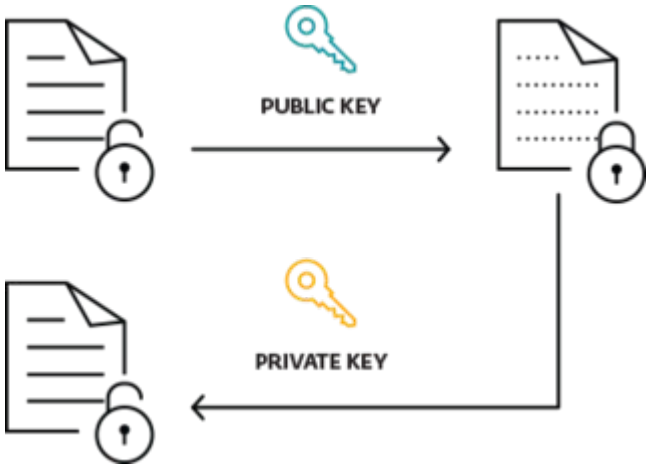
- Невозможность отказа от авторства. Так как создать корректную подпись можно лишь зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под документом.

Для подписи документа сначала вычисляется значение хэш-функции для документа, а затем это значение по специальному криптоалгоритму подписывается секретным ключом автора документа.
Для проверки подлинности документа необходимо с помощью открытого ключа проверить подпись, затем вычислить его хэш-значение и сравнить с подписанной контрольной суммой. Если оба значения совпадают, то подпись верна, иначе документ был изменён.

КАТЕГОРИИ ШИФРОВАНИЯ

Большинство криптографических компьютерных систем принадлежат к одной из двух категорий:

1) Шифрование симметричным ключом;
2) Шифрование асимметричным ключом или открытым ключом.



ШИФРОВАНИЕ СИММЕТРИЧНЫМ КЛЮЧОМ

Симметричное шифрование - метод, при котором шифрование и дешифрация сообщения производится при помощи одного симметричного ключа.

Симметричный ключ – это секретный код, который должны знать оба компьютера, чтобы иметь возможность расшифровывать сообщения друг от друга.

В секретном коде содержится «ключ» для расшифровки сообщений.

ШИФРОВАНИЕ СИММЕТРИЧНЫМ КЛЮЧОМ

Слабым местом симметричного шифрования является ключ шифрования, точнее его доставка до адресата. Если во время доставки ключ будет скомпрометирован, стороннее лицо легко раскодирует сообщение. Сильной стороной симметричного шифрования является его скорость, что дает возможность кодировать большие объемы данных.

ШИФРОВАНИЕ ОТКРЫТЫМ КЛЮЧОМ

Шифрование открытым ключом использует комбинацию из секретного ключа и открытого ключа.

Секретный ключ известен только вашему компьютеру, в то время как открытый ключ свободно передается вашим компьютером любым другим, которые хотят вести с вами зашифрованное общение.

Для раскодирования зашифрованного сообщения, компьютер должен использовать оба ключа секретный и открытый. Популярная программа для использования шифрования открытым ключом это PGP (pretty good privacy).

ШИФРОВАНИЕ ОТКРЫТЫМ КЛЮЧОМ

Механизм действия такой:

1. адресат отправляет ОТКРЫТЫЙ ключ отправителю;

2. отправитель кодирует сообщение при помощи полученного открытого ключа. При этом, раскодировать сообщение можно теперь только закрытым ключом;

3. при получении зашифрованного сообщения адресат раскодирует его ЗАКРЫТЫМ ключом (который был сгенерирован в паре с открытым).

Считается, что ассиметричное шифрование «тяжелее» симметричного. Всё потому, что оно требует больше компьютерных ресурсов. Есть ограничения и на процесс генерации ключей.

СОЧЕТАНИЕ ОТКРЫТЫХ И СИММЕТРИЧНЫХ КЛЮЧЕЙ

При соединении двух компьютеров, одна машина создает симметричный ключ и отправляет его другой, используя при этом шифрование открытым ключом. После этого компьютеры будут общаться, используя шифрование симметричным ключом. После окончания соединения, каждый компьютер избавляется от симметричного ключа.

Каждое новое соединение требует создания нового симметричного ключа.

ХЕШ-ФУНКЦИИ

Реализация схемы ЭЦП связана с вычислением хэш-функции (дайджеста) данных, которая представляет собой уникальное число, полученное из исходных данных путем его сжатия (свертки) с помощью сложного, но известного алгоритма. Хэш-функция является однонаправленной функцией, т. е. по хэш-значению невозможно восстановить исходные данные. Хэш-функция чувствительна к всевозможным искажениям данных. Кроме того, очень трудно отыскать два набора данных, обладающих одним и тем же значением хэш-функции.

Схема формирования подписи электронного документа его отправителем включает вычисление хэш-функции электронного документа и шифрование этого значения посредством секретного ключа отправителя. Результатом шифрования является значение ЭЦП электронного документа (реквизит электронного документа), которое пересылается вместе с самим электронным документом получателю. При этом получателю сообщения должен быть предварительно передан открытый ключ отправителя сообщения.

ХЕШ-ФУНКЦИИ

Схема проверки (верификации) ЭЦП, осуществляемая получателем, сообщения состоит из следующих этапов. На первом из них производится расшифрование блока ЭЦП посредством открытого ключа отправителя. Затем вычисляется хэш-функция электронного документа. Результат вычисления сравнивается с результатом расшифрования блока ЭЦП. В случае совпадения принимается решение о соответствии ЭЦП электронного документа заявленным данным. Несовпадение результатов расшифрования с результатом вычисления хэш-функции электронного документа может объясняться следующими причинами:

- в процессе передачи по каналу связи была потеряна целостность электронного документа;
- при формировании ЭЦП был использован не тот (поддельный) секретный ключ;
- при проверке ЭЦП был использован не тот открытый ключ (в процессе передачи по каналу связи или при дальнейшем его хранении был модифицирован или подменен).

ХЕШ-ФУНКЦИИ

Ключ, который используется при шифровании открытым ключом основывается на значении хеш-функции. Это значение, которое высчитывается из основного исходного значения (числа) при помощи хеш алгоритма.

Пример:

Исходное число = 10667

Хеш алгоритм = исходное число X 143

Значение Хеш-функции = 1525381

Значение 1525381

получилось из

умножения 10667 и 143.

Открытые ключи часто используют очень сложные алгоритмы и огромные значения хеш-функций для шифрования, включая 40-битные или даже 128-битные числа.

128-битное число имеет количество комбинаций равное 2 в 128-ой степени или 3 402 823 669 209 384 634 633 746 074 300 000 000 000 000 000 000 000 000 000 . 000 000 000!

ИСПОЛЬЗОВАНИЕ ЭЦП ПОЗВОЛЯЕТ

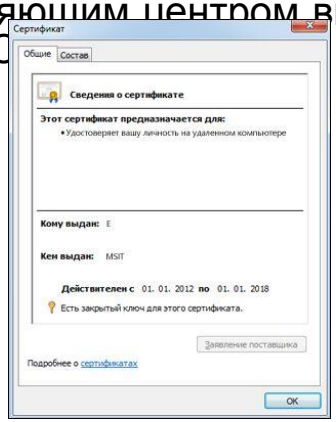
- значительно сократить время, затрачиваемое на оформление сделки и обмен документацией;
- усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов;
- гарантировать достоверность документации;
- минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена;
- построить корпоративную систему обмена документами.

ЦИФРОВОЙ СЕРТИФИКАТ

В соответствии с Федеральным законом 63 - ФЗ «Об Электронно-цифровой подписи» цифровой сертификат содержит следующие сведения:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;

- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи или номер ЕГРЮ
- открытый ключ ЭЦП;
- на кого выдан сертификат;
- СНИЛС;
- ключ проверки ЭП;
- наименование и адрес удостоверяющего центра;
- кем сертификат выдан;
- наименование средства ЭЦП, с которым используется данный открытый ключ ЭЦП;
- наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с ЭЦП будет иметь юридическое значение.



ИДЕНТИФИКАЦИЯ

Идентификация используется для проверки того, что информация или данные поступают к вам от доверенного источника и не были изменены.

Способы идентификации на компьютере:

1) Пароль - использование имени и пароля пользователя.

2) Карты допуска - эти карты могут быть разного типа, от простой карты с магнитной дорожкой до смарт карт.

3) Цифровая подпись - в основном это способ убедиться в том, что электронный документ (например, e-mail) является подлинным.

ХРАНЕНИЕ ЭЦП

В настоящее время существуют следующие устройства хранения закрытого ключа:

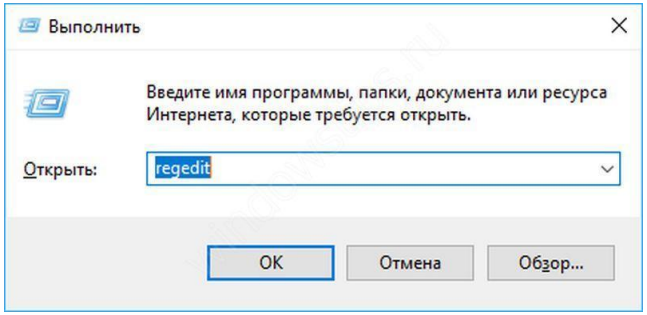
дискеты, 

смарт-карты, 

USB-брелоки, 

«таблетки» Touch-Memory, 

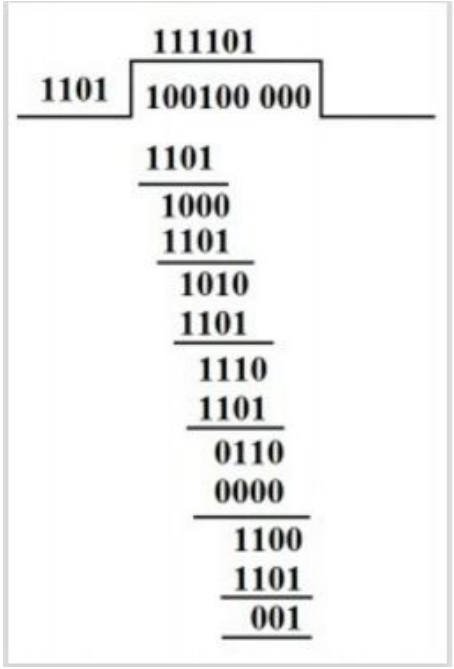
реестр (в защищённой памяти компьютера).



РАСПРОСТРАНЕННЫЕ СПОСОБЫ ОБЕСПЕЧЕНИЯ ПРАВИЛЬНОСТИ ДАННЫХ:

1) Контрольная сумма (checksum) - обеспечивает определенную форму идентификации, так как неправильная контрольная сумма предполагает, что данные были повреждены или изменены.

2) Контроль с помощью циклического избыточного кода (Cyclic Redundancy Check (CRC)) - CRC имеет схожий принцип действия, что и контрольная сумма, но использует деление на многочлены, чтобы определить значение CRC, которое обычно имеет длину 16 или 32 битов.



УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ЭЦП В ЭЛЕКТРОННЫХ ДОКУМЕНТАХ:

1) Средства создания подписи признаются надежными;

2) Сама ЭЦП признается достоверной, а ее подделка или фальсификация подписанных данных могут быть точно установлены;

3) Предоставляются юридические гарантии безопасности передачи информации по открытым телекоммуникационным каналам;

4) Соблюдаются правовые нормы, содержащие требования к письменной форме документа;

5) Сохраняются все традиционные процессуальные функции подписи, в том числе удостоверение полномочий подписавшей стороны, установление подписавшего лица и содержания сообщения, а также роль подписи в качестве судебного доказательства;

6) Обеспечивается охрана персональной информации.

ОБЛАДАТЕЛЬ ЭЦП

Владельцем сертификата ключа подписи (обладателем ЭЦП) является физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП подписывать электронные документы.

Владелец сертификата ключа подписи обязан (статья 12):

1) Хранить в тайне закрытый ключ ЭЦП;

2) Не использовать для ЭЦП открытые и закрытые ключи ЭЦП, если ему известно, что эти ключи используются или использовались ранее;

3) Немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа ЭЦП нарушена.

КТО ВЫДАЕТ ЭЦП?

Регулированием применения ЭЦП занимается уполномоченный федеральный орган. Его функции включают:

- создание головного удостоверяющего центра;

- аккредитацию удостоверяющих центров, ведение их списка, в который вносятся функционирующие компании, информация по фирмам, работа которых приостановлена или прекращена;

- создание и правление реестром изготовленных квалифицированных сертификатов.

Чтобы получить неквалифицированный и квалифицированный сертификат электронной подписи, необходимо обратиться в один из удостоверяющих центров.

УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Удостоверяющий центр — юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом «Об электронной подписи» от 06.04.2011 N 63-ФЗ и нормативными актами.

Аккредитованный удостоверяющий центр — удостоверяющий центр, прошедший проверку на соответствие требованиям Федерального закона «Об электронной подписи» от 06.04.2011 N 63-ФЗ и получивший от уполномоченного федерального органа (Министерства связи и массовых коммуникаций Российской Федерации) Свидетельство об аккредитации.

Основная задача удостоверяющего центра заключается в создании и выдаче сертификатов, подтверждающих, что электронная подпись принадлежит именно владельцу. Удостоверяющий центр несет финансовую и административную ответственность за достоверность сертификата.

УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Работа УЦ лежит на пересечении юриспруденции, информационной безопасности и IT-технологий.

В обязанности УЦ входят следующее:

- удостоверить личность человека, который обратился за сертификатом электронной подписи,

- изготовить и выдать сертификат, в который включены данные о владельце сертификата и его открытый ключ проверки,

- управлять жизненным циклом сертификата (выпуск, приостановление, возобновление, окончание срока действия).

Чтобы иметь право на выпуск квалифицированных сертификатов электронной подписи, удостоверяющий центр должен быть аккредитован Минкомсвязью РФ. Наличие аккредитации уполномоченного федерального органа говорит о легальности выдачи такими удостоверяющими центрами квалифицированных сертификатов электронной подписи.

Удостоверяющий центр получает аккредитацию Минкомсвязи, если соответствует определённым условиям, одно из которых заключается в том, что средства криптографического преобразования информации, которые он использует для создания сертификатов электронной подписи, должны иметь подтверждение соответствия требованиям федерального органа исполнительной власти в области обеспечения безопасности.

СЕРТИФИКАТ КЛЮЧА ПОДПИСИ ДОЛЖЕН СОДЕРЖАТЬ (СТАТЬЯ 6):

1) Уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;

2) Фамилия, имя, отчество владельца сертификата ключа подписи или псевдоним владельца;

3) Открытый ключ ЭЦП;

4) Наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;

5) Сведения об отношениях, при осуществлении которых электронный документ с ЭЦП будет иметь юридическое значение.

УДОСТОВЕРЯЮЩИЙ ЦЕНТР, ВЫДАВШИЙ СЕРТИФИКАТ КЛЮЧА ПОДПИСИ, ОБЯЗАН АННУЛИРОВАТЬ ЕГО (СТАТЬЯ 14 ФЕДЕРАЛЬНОГО ЗАКОНА):

1) По истечении срока его действия;

2) При утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования;

3) В случае если удостоверяющему центру стало известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи;

4) По заявлению в письменной форме владельца сертификата ключа подписи;

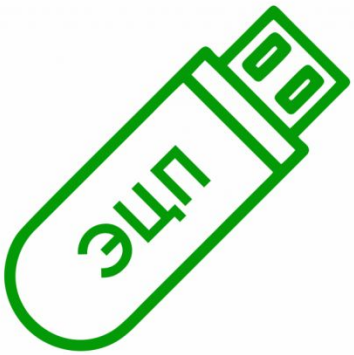
5) В иных установленных нормативными правовыми актами или соглашением сторон случаях.

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ

- Атака с использованием открытого ключа. Криптоаналитик обладает только открытым ключом.

- Атака на основе известных сообщений. Противник обладает допустимыми подписями набора электронных документов, известных ему, но не выбираемых им.

- Адаптивная атака на основе выбранных сообщений. Криптоаналитик может получить подписи электронных документов, которые он выбирает сам.



ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ

Самой «опасной» атакой является адаптивная атака на основе выбранных сообщений, и при анализе алгоритмов ЭП на криптостойкость нужно рассматривать именно её (если нет каких-либо особых условий).

При безошибочной реализации современных алгоритмов ЭП получение закрытого ключа алгоритма является практически невозможной задачей из-за вычислительной сложности задач, на которых ЭП построена. Гораздо более вероятен поиск криптоаналитиком коллизий первого и второго родов. Коллизия первого рода эквивалентна экзистенциальной подделке, а коллизия второго рода — выборочной. С учётом применения хэш-функций, нахождение коллизий для алгоритма подписи эквивалентно нахождению коллизий для самих хэш-функций.

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ

Подделка документа (коллизия первого рода)

Злоумышленник может попытаться подобрать документ к данной подписи, чтобы подпись к нему подходила. Однако в подавляющем большинстве случаев такой документ может быть только один. Причина в следующем:

- документ представляет из себя осмысленный текст;

- текст документа оформлен по установленной форме;

- документы редко оформляют в виде txt-файла, чаще всего в формате DOC или HTML.

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ

Получение двух документов с одинаковой подписью (коллизия второго рода)

Куда более вероятна атака второго рода. В этом случае злоумышленник фабрикует два документа с одинаковой подписью, и в нужный момент подменяет один другим. При использовании надёжной хэш-функции такая атака должна быть также вычислительно сложной. Однако эти угрозы могут реализоваться из-за слабостей конкретных алгоритмов хэширования, подписи, или ошибок в их реализациях. В частности, таким образом можно провести атаку на SSL-сертификаты и алгоритм хэширования MD5.

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ

Социальные атаки

Социальные атаки направлены не на взлом алгоритмов цифровой подписи, а на манипуляции с открытым и закрытым ключами.

Злоумышленник, укравший закрытый ключ, может подписать любой документ от имени владельца ключа.

Злоумышленник может обманом заставить владельца подписать какой-либо документ, например, используя протокол слепой подписи.

Злоумышленник может подменить открытый ключ владельца на свой собственный, выдавая себя за него.

Использование протоколов обмена ключами и защита закрытого ключа от несанкционированного доступа позволяет снизить опасность социальных атак.

ВЕДУЩИЕ ПРОИЗВОДИТЕЛИ КРИПТОСРЕДСТВ

Крипто – Про

КРИПТОПРО

Актив

РУТОКЕН

Инфотекс

ViPNet CSP

Аладдин РД

Аладдин рд

Цифровые технологии

КриптоАРМ

Крипто Ком

криптоком
системы защиты информации

Сигнал КОМ

SC
Сигнал-КОМ

ВОПРОСЫ?