ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

1. Понятия 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.

Электронный документ - это любой документ, созданный и хранящийся на компьютере.

ЭЦП обеспечивает:

1) **Подлинность** - Цифровая подпись помогает гарантировать, что поставивший подпись — тот, кем он является в действительности.

2) **Целостность** - Цифровая подпись помогает гарантировать, что содержимое документа не менялось и не подделывалось после ввода цифровой подписи.

3) **Неотрекаемость** - ЭЦП помогает доказать любой из сторон авторство подписанного содержимого.

Категории шифрования

Большинство криптографических компьютерных систем принадлежат к одной из двух категорий:

1) Шифрование симметричным ключом;

2) Шифрование открытым ключом

Шифрование симметричным ключом

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 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).

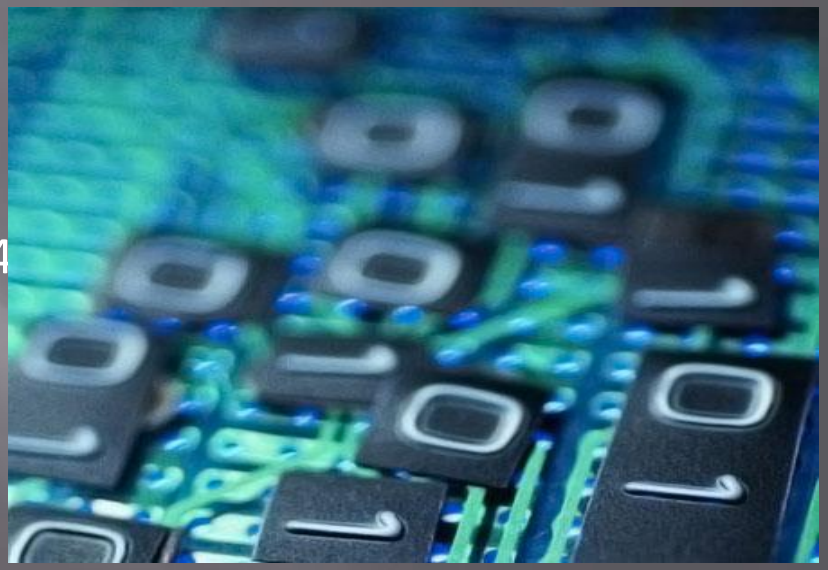
Сочетание открытых и симметричных ключей

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 симметр

Каждое новое соединение требует создания нового симметричного ключа.

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 14

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!

Идентификация

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

Способы идентификации на компьютер

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 способ убедиться в том, что электронны документ (например, e-mail) является подлинным.

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.

2. Условия исполнения Закона «Об электронной цифровой подписи»

10 января 2002 года был принят Федеральный Закон «Об электронной цифровой подписи», вступивший в силу
с 22 января текущего года.

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 одписывать 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.

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.

СЕРТИФИКАТ

КЛЮЧА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

серийный номер:	01: 6d: 01: 04: 01: 01: 01: 04
начало действия:	07.03.2007 07: 05: 25 GMT
окончание действия:	27. 08. 2012 07: 05: 25 GMT
владелец:	Свиридова Инна Сергеевна
организация:	ФГОУ ВПО "ЮФУ"
подразделение:	Удостоверяющий центр №1
должность:	уполномоченный
населенный пункт:	Ростов-на-Дону
субъект федерации:	Ростовская область
электронная почта:	inna@mail.ru

сертификат:

---------BEGIN CERTIFICATE----------
DFHSDJHFGSHDKJGHKJDHJDHKJDHKDFHGJDFHGFGRH5JGH65JGHJ5GH6KJ5G
HDFJGSDHGSHGSFKJGKLJDGHDFHGJDFHGFGRH5JGH65JGHJ5GH6KJ5G5KGJF
FHJ54FJ7FGH54FG654J56GDH4J5DFHGJDFHGFGRH5JGH65JGHJ5GH6KJ5G5KG
DFHGJDFHGFGRH5JGH65JGHJ5GH6KJ5G5KDFHGJDFHGFGRH5JGH65JGHJ5GH6
HFJ4GH5J4G54H65G4KJ4GKH4GH654KJ654GHDFHGJDFHGFGRH5JGH65JGHJ5
HGJ4GH654KJHG654J65GH4KJ65G4654GH654JGDFHGJDFHGFGRH5JGH65JGH
GHJ54GH65J4G465GH4KJ65G4K6546KJ4KGJ6DFHGJDFHGFGRH5JGH65JGHJ5G
GH564J65GH4J65G465GH4J65G4654HG65DFHGJDFHGFGRH5JGH65JGHJ5GH6
HG54JGH4J65465GH4J65GHJ654GH65DFHGJDFHGFGRH5JGH65JGHJ5GH6KJ5
HG5J4GH654J65GH4J654GH654J65GH4J65HG4J654GHJ5G4J5G4HJ4GH4JHH
--------END CERTIFICATE-----

На оснавании заключенного с УЦ договора владелец может подписывать документы в данной системе в соответствии со своими полномочиями.

подпись владельца:

РЭОС

Уполномоченный Удостоверяющего центра

/Богатырёва Т. Р. / "14" сентября 2007 г.

Удост. центр обязан аннулировать сертификат к.п. (ст.14):

1) Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его (статья 14 Федерального закона):

2) По истечении срока его действия;

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

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

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

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

ЭЦП это код, содержащий в зашифрованном виде:

1) Идентификацию секретного ключа владельца как лица, подписавшего документ;

2) Дату и время произведения подписи;

3) Весь исходный текст документа в том виде, в каком он существовал на момент произведения подписи.