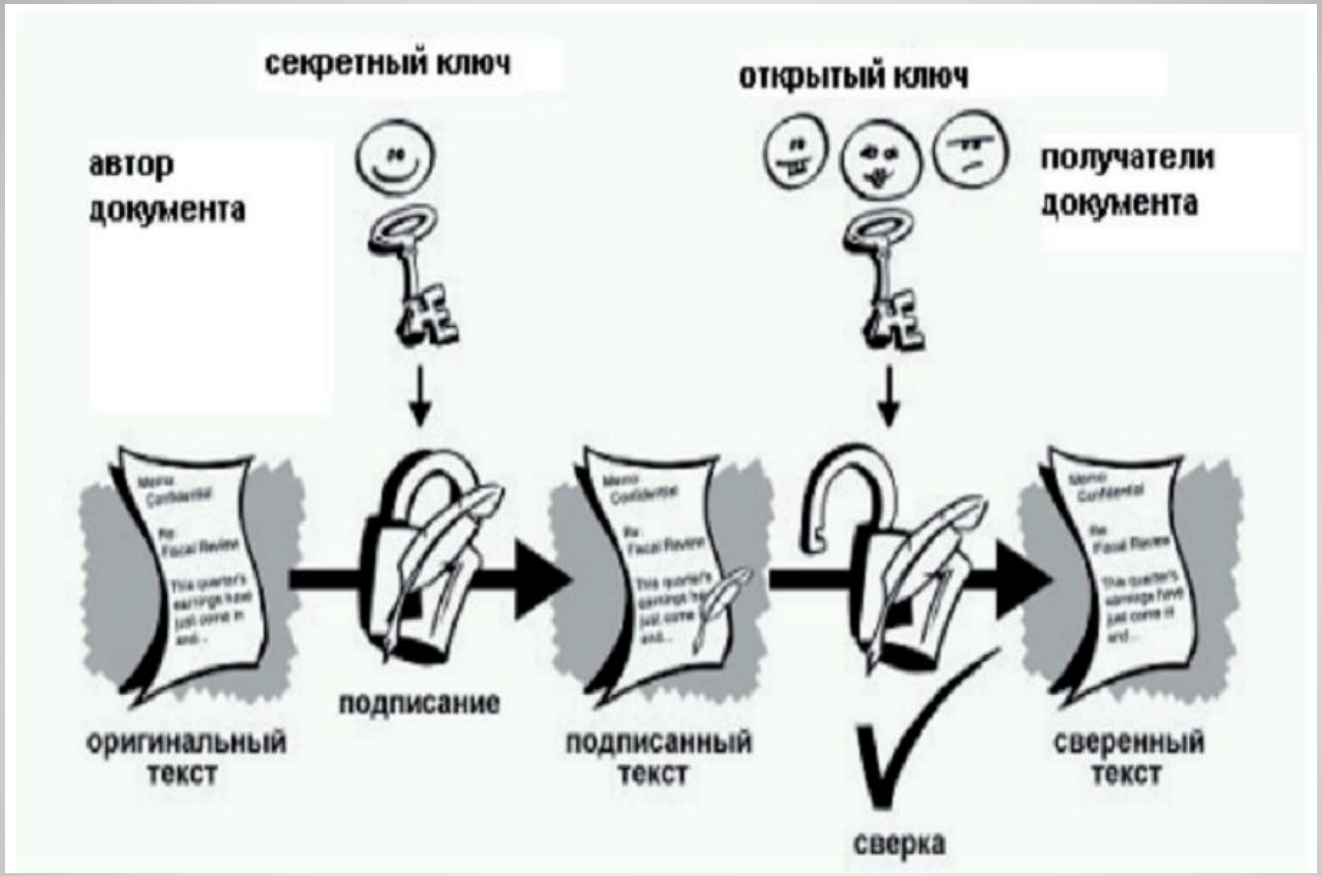
Электронная цифровая подпись (ЭЦП)

Назначение и применение ЭЦП. Виды ЭЦП и требования к ним. Стандарты. Управление ключами. Использование ЭЦП в России.

Определение Электронной цифровой подписи

«электронная 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 Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"



Порядок подписания электронного документа

Основные определения

- **ЭЦП** – реквизит эл. документа, защищенный от подделки, полученный в результате криптографического* преобразования информации с использованием закрытого ключа.
- **Обладатель ЭЦП** – лицо, на имя которого зарегистрировано право использования ЭЦП и который обладает закрытым ключом, позволяющим создавать свою ЭЦП в электронных документах
- **Средства ЭЦП** – аппаратные и/или программные средства реализующие функции создания и проверки подлинности ЭЦП

***Криптогра́фия** (от др.-греч. κρυπτός — скрытый и γράφω — пишу) — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных, о методах шифрования.

ЭЦП обеспечивает следующие функции:

- Контроль целостности передаваемого документа
- Защиту от изменений (подделки) документа
- Невозможность отказа от авторства
- Доказательное подтверждение авторства документа


Область применения ЭЦП
защищенная электронная почта
Подтверждение авторства
средство идентификации и аутентификации в различных Информационных системах
для подписи программ или отдельных модулей
как ответственная подпись на электронном документе
Получение государственных услуг в электронном виде
Участие в электронных торгах, тендерах, аукционах

Сфера применения ЭЦП

- Таможенное декларирование товаров и услуг
- Электронная регистрация сделок по объектам недвижимости.
- Использование в банковских платежных системах.
- Электронная коммерция (торговля).
- Управление государственными заказами.
- В электронных системах обращения граждан к органам власти, в т.ч. и по экономическим вопросам (на сайте госуслуг).
- Формирование обязательной налоговой (фискальной), бюджетной, статистической и прочей отчетности перед государственными учреждениями и внебюджетными фондами.
- Применение ЭЦП в различных расчетных и трейдинговых системах.
- Управление акционерным капиталом и долевым участием.
- В глобальных системах межбанковского рынка обмена валют по определенному курсу (Forex).

ВИДЫ ЦИФРОВЫХ ПОДПИСЕЙ

Простая электронная подпись (ПЭП) – подтверждает, что электронное сообщение отправлено конкретным лицом. Предназначена для подписания электронных сообщений, направляемых в государственный орган, орган местного самоуправления или должностному лицу.

- Создается с помощью кодов, паролей и других инструментов (комбинация логина и пароля).
- Может рассматриваться как аналог собственноручной подписи.

ВИДЫ ЦИФРОВЫХ ПОДПИСЕЙ

Усиленная неквалифицированная ЭП

- позволяет не только идентифицировать отправителя, но и подтвердить, что с момента подписания документ не менялся. Применяется во всех видах отношений, если иное не установлено нормативным правовым актом или соглашением участников отношений.

- Создается с использованием криптографических средств.
- Может рассматриваться как аналог документа с печатью.

ВИДЫ ЦИФРОВЫХ ПОДПИСЕЙ

Усиленная квалифицированная электронная подпись (КЭП)-предназначена для взаимодействия юридических лиц и госорганов с использованием государственных информационных систем.

- Использует сертификат аккредитованного Удостоверяющего центра.

Цифровая подпись должна обладать следующими свойствами

- Должна быть возможность проверить автора, дату и время создания подписи.
- Должна быть возможность аутентифицировать содержимое во время создания подписи.
- Подпись должна быть проверяема третьей стороной для разрешения споров.

- 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.

требования к *цифровой подписи*

- Подпись должна быть битовым образцом, который зависит от подписываемого сообщения.
- Подпись должна использовать некоторую уникальную информацию отправителя для предотвращения подделки или отказа.
- Создавать *цифровую подпись* должно быть относительно легко.
- Должно быть вычислительно невозможно подделать *цифровую подпись* как созданием нового сообщения для существующей *цифровой подписи*, так и созданием ложной *цифровой подписи* для некоторого сообщения.
- *Цифровая подпись* должна быть достаточно компактной и не занимать много памяти.

Правовые основы применения ЭП

- · Федеральный закон No 32КФЗ «О внесении изменения и дополнения в Федеральный закон «О бухгалтерском учете» от 28 марта 2002 г.;
- · Федеральный закон No 1КФЗ «Об электронной цифровой подписи» от 10 января 2002 г.;
- · Федеральный закон No 180КФЗ «О внесении изменения в статью 80 части первой Налогового кодекса Российской Федерации» дополняет Налоговый кодекс положениями, касающимися пересылки налоговой декларации в налоговую инспекцию в электронном виде по каналам связи («безбумажная» технология) от 28 декабря 2001 г.;
- · Федеральный закон No 128КФЗ «О лицензировании отдельных видов деятельности» от 8 августа 2001 г.;
- · Федеральный закон No 85КФЗ «Об участии в международном информационном обмене» от 4 июля 1996 г.;
- · Федеральный закон No 27КФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» от 1 апреля 1996 г.;
- · Федеральный закон No 40КФЗ «Об органах Федеральной службы безопасности в Российской Федерации» от 03 апреля 1995г.;

- · Федеральный закон No 24КФЗ «Об информации, информатизации и защите информации» (с комментариями) от 20 февраля 1995 г.;
- · Федеральный закон No 15КФЗ «О связи» от 20 января 1995 г.;
- · Федеральный закон No 4524К1 «О федеральных органах правительственной связи и информации» от 24 декабря 1993г.;
- · Федеральный закон No 5485К1 «О Государственной тайне» от 21 июля 1993 г.;
- · Федеральный закон No 5306К1 «О внесении изменений и дополнений в Закон Российской Федерации «О федеральных органах государственной безопасности» от 01 июля 1993 г.;
- · Федеральный закон No 5154К1 «О стандартизации» от 10 июня 1993 г.;
- · Федеральный закон No 5151К1 «О сертификации продуктов и услуг» от 10
- июня 1993 г.;
- · Федеральный закон No 3523К1 «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992г.;
- Федерального закона N 63-ФЗ «Об электронной подписи» от 06.04.2011 г., в котором «электронная цифровая подпись» заменена на «электронную подпись» трех видов

Схемы построения ЭЦП

- Прямая ЭЦП

  Взаимодействуют только отправитель и получатель. Получатель знает открытый ключ отправителя. Основана на применении алгоритмов симметричного и ассиметричного шифрования.

- Арбитражная ЭЦП

  Предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт шифрования его секретным ключом и передача его арбитру. Реализуется на основе алгоритмов симметричного шифрования.

В процессе подписания электронной подписью к ЭД прикладывается **сертификат.**

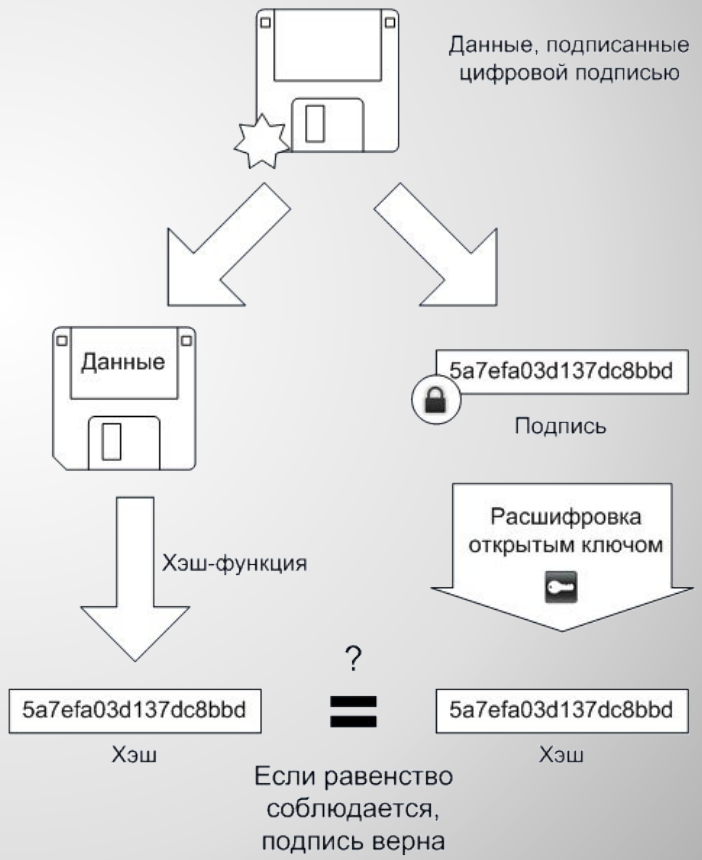
Сертификат позволяет удостоверить заключенные в нем данные о владельце и его открытый ключ подписью какого-либо доверенного лица.

Существуют системы сертификатов двух типов: **централизованные и децентрализованные**

- В **децентрализованных** системах путем перекрестного подписывания сертификатов знакомых и доверенных людей каждым пользователем строится сеть доверия
- В **централизованных** системах сертификатов используются ***центры сертификации***, поддерживаемые доверенными организациями.

Подписывание

Проверка



Центры сертификации

- Выдают сертификаты - цифровые данные, подписанные цифровой подписью поручителя, подтверждающие соответствие открытого ключа и информации, идентифицирующей его владельца.
- Сертификат содержит публичный *ключ*, информацию о владельце ключа, название сертификационного центра, время, в течение которого сертификат действителен, и т.д.
- Каждая копия сертификата имеет *цифровую подпись* организации, выдавшей сертификат, так что каждый, кто получит сертификат, может удостовериться в его подлинности.

Пример сертификата на ЭЦП

O'ZBEKISTON ALOQA VA AXBOROTLASHTIRISH AGENTLIGI

УЗБЕКСКОЕ АГЕНТСТВО СВЯЗИ И ИНФОРМАТИЗАЦИИ

ELEKTRON RAQAMLI IMZO KALITI

SERTIFIKATI

СЕРТИФИКАТ

КЛЮЧА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

№ 0012

Sertifikat egasi: Файзуллаев Алишер Насибуллаевич
Владелец сертификата:

Tashkilotning nomi: Государственное унитарное предприятие
Наименование организации:

Центр научно-технических и маркетинговых исследований - «UNICON.UZ»

Lavozimi: Директор
Должность:

Manzili: 100202, г. Ташкент, ул. Богишамол, 7а
Адрес:

Amal qilish muddati: 16 августа 2010 года dan 13 августа 2015 года gacha
Срок действия: с по

Foydalanish maqsadlari haqida ma'lumot: Подписание сертификатов ключей
Сведения о целях использования:

электронных цифровых подписей

Elektron raqamli imzoning ochiq kaliti:
Открытый ключ ЭЦП:

```
30 81 89 02 81 81 00 B8 6F E6 F3 BE F4 E1 68 CA 0C 2B 6A 0E FD 53 36 54
0C DC 6A 55 8D FE 13 47 83 16 05 04 D9 1D 74 61 1E F8 AF 73 7A 2F 6B 3C
40 9F 87 DC 5C 05 FC 6D 18 20 EE 21 A5 E5 B5 45 7F 96 97 22 02 FB BC D6
FA F7 E6 30 73 4F 2E 8B 8B 45 D4 3C B8 D3 18 A4 4C E3 15 C2 32 7F 63 9E
1E BA A0 9C C2 9A ED D8 91 3E 0A AF E3 1A D3 98 CB DB DC 5A B7 B1 A8 97
53 ED 06 D5 23 D3 ED F0 DF 17 5C 25 8F 05 15 02 03 01 00 01
```

Axborotni kriptografik muhofaza qilish vositalarining nomi: RSA Encryption SHA1
Наименование средств криптографической защиты информации:

Ro'yxatga olish Organining manzili: 100011, г. Ташкент, ул. Навои, 28а
Адрес Органа регистрации:

Kalit egasining imzosi:
Подпись владельца ключа:

Ro'yxatga olish Organining rahbari:
Руководитель Органа регистрации:

Reyestr / Реестр № 12

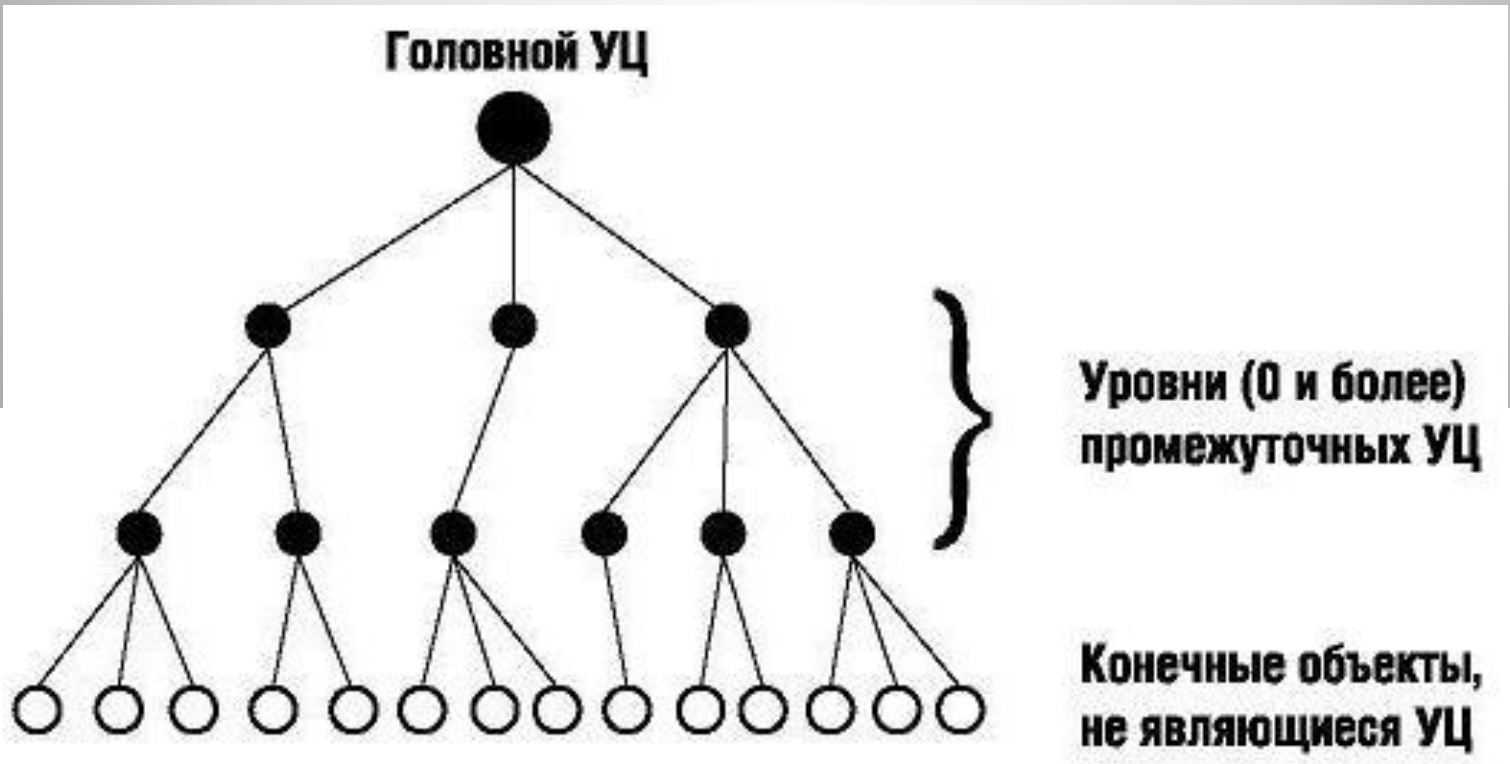
Устройства хранения закрытого ключа

- Дискеты
- Смарт-карты
- USB-брелоки
- Таблетки Touch-Memory

Удостоверяющий центр:

- регистрирует электронные цифровые подписи;
- создает по обращению пользователей закрытые и открытые ключи ЭЦП;
- приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;
- ведет реестр сертификатов ключей подписей, обеспечивает актуальность реестра и возможность свободного доступа пользователей к реестру;
- выдает сертификаты ключей подписей на ***бумажных носителях и в виде электронных документов*** с информацией об их действительности;
- проводит по обращениям пользователей подтверждение подлинности (действительности) электронной цифровой подписи в электронном документе в отношении зарегистрированных им электронных цифровых подписей;
- может предоставлять пользователям информационных систем иные услуги, связанные с использованием электронных цифровых подписей

Строгая иерархия удостоверяющих центров

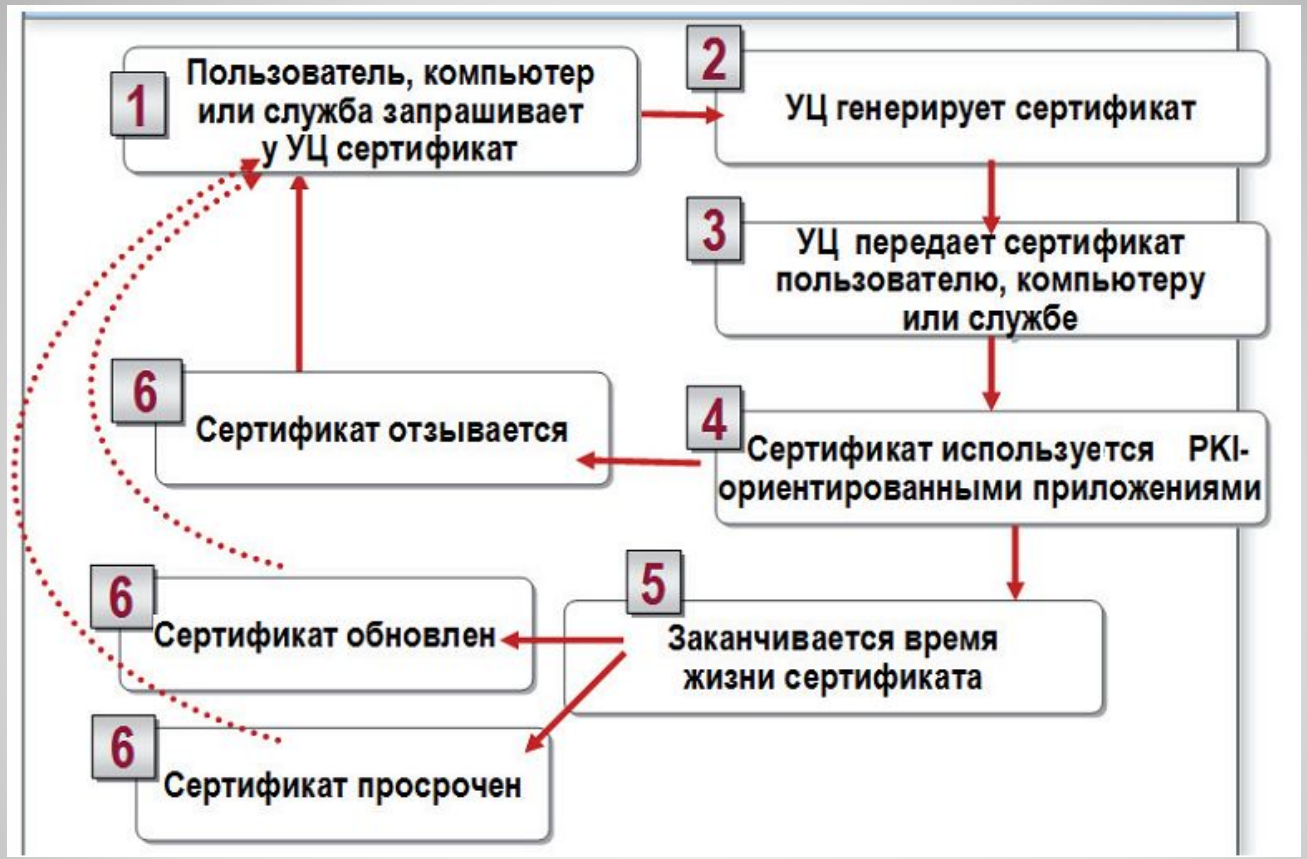


В соответствии с Постановлением Правительства РФ от 28.11.2011 №976 «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи» функции **головного удостоверяющего центра** в отношении аккредитованных удостоверяющих центров осуществляет **Министерство связи и массовых коммуникаций** Российской Федерации.

На сайте Минкомсвязи имеется список аккредитованных УЦ, а также тех, аккредитация которых приостановлена или прекращена

Удостоверяющий центр **аннулирует** выданные им сертификаты ключа подписи:

- по истечении срока его действия;
- при утрате силы сертификата соответствующих средств ЭЦП;
- в случае, если удостоверяющему центру стало достоверно известно о прекращении действия документа, на основе которого оформлен сертификат ключа подписи;
- по письменному (на бумажном носителе) заявлению обладателя электронной цифровой подписи;
- в иных случаях, установленных законом или договором.



Жизненный цикл цифрового сертификата

*** PKI - инфраструктура управления открытыми ключами (public key infrustructure), современная система управления криптографической защитой, в том числе и в агрессивной среде**

Стрелки на схеме ЖЦ сертификата ЭЦ:

обычные - отображают нормальный жизненный цикл сертификата

пунктирные - показывают моменты вмешательства УЦ

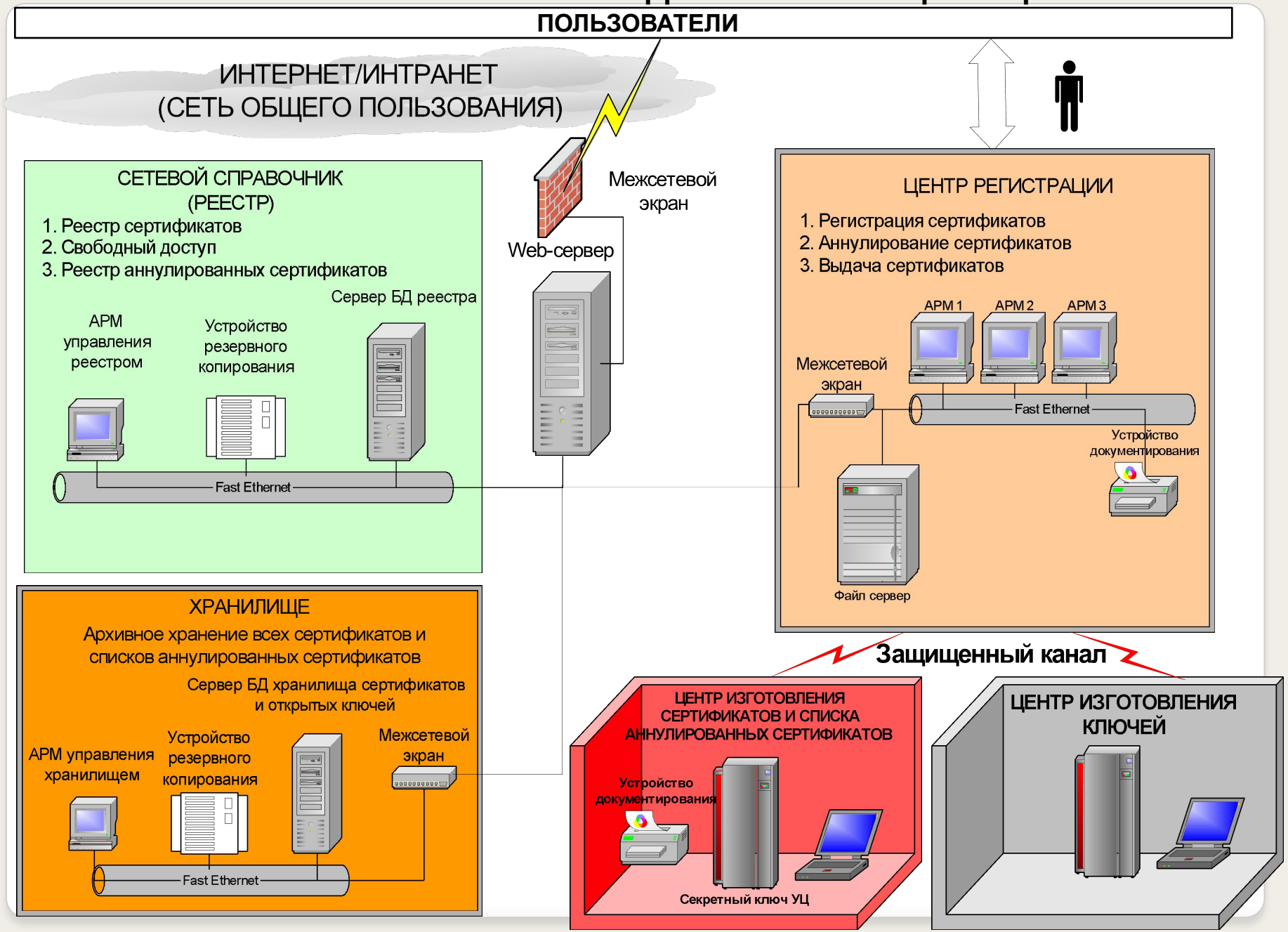
Пример: в корпоративной системе, где владельцами сертификатов являются служащие организации, вмешательство УЦ в нормальный жизненный цикл сертификата требуется в случаях:
- аннулирования сертификата при увольнении служащего, владеющего этим сертификатом;
- аннулирования сертификата при утере служащим своего секретного ключа или пароля доступа к секретному ключу;
- приостановления действия сертификата, выпущенного для служащего, который в данный момент времени увольняется или находится под следствием;
- возобновления сертификата служащего при отказе от увольнения или после прояснения обстоятельств судебного дела и т.п.

Сертификаты могут иметь различные сроки действия для служащих в зависимости от их статуса, например, служащие, работающие по контракту, могут иметь сертификаты на период их контракта

Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные настоящим Федеральным законом.

Удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

СТРУКТУРА ТИПОВОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА



Симметричные алгоритмы

- Для шифрования и расшифровки используются одни и те же алгоритмы. Один и тот же секретный ключ используется для шифрования и расшифровки.
- Основаны на хорошо изученных блочных шифрах.

Примеры симметричных алгоритмов

- DES (Data Encryption Standard)- Шифруется блок из 64 бит, используется 64-битовый ключ (требуется только 56 бит), 16 проходов.
- 3-DES или тройной DES
- RC5
- CAST 64-битный блочный шифратор, ключи длиной от 40 до 64 бит, вскрывается только прямым перебором.
- Устройство с одноразовыми ключами - У отправителя и получателя имеются одинаковые устройства.

Симметричная схема шифрования

Преимущества:

Стойкость симметричных схем **ЭП.**

Недостатки:

- Нужно подписывать отдельно каждый бит передаваемой информации, что приводит к значительному увеличению подписи. Подпись может превосходить сообщение по размеру на два порядка.
- Сгенерированные для подписи ключи могут быть использованы только один раз, так как после подписания раскрывается половина секретного ключа.

Прямая ЭЦП.

Ассиметричные алгоритмы шифрования . Ключи.

- Ассиметричные алгоритмы работают с двумя ключами - текст, зашифрованный одним ключом, может быть расшифрован **только** вторым ключом. Вся технология состоит в том, что ключи связаны между собой алгоритмом генерации.

- Если Вы шифруете письмо своим закрытым ключом (ЗК), расшифровать его может любой человек, имеющий Ваш открытый ключ (ОК). То, что сообщение расшифровывается ОК однозначно определяет, что зашифровано оно было Вашим ЗК. А это могли сделать Вы и только Вы... соответственно, это и есть Ваша подпись.

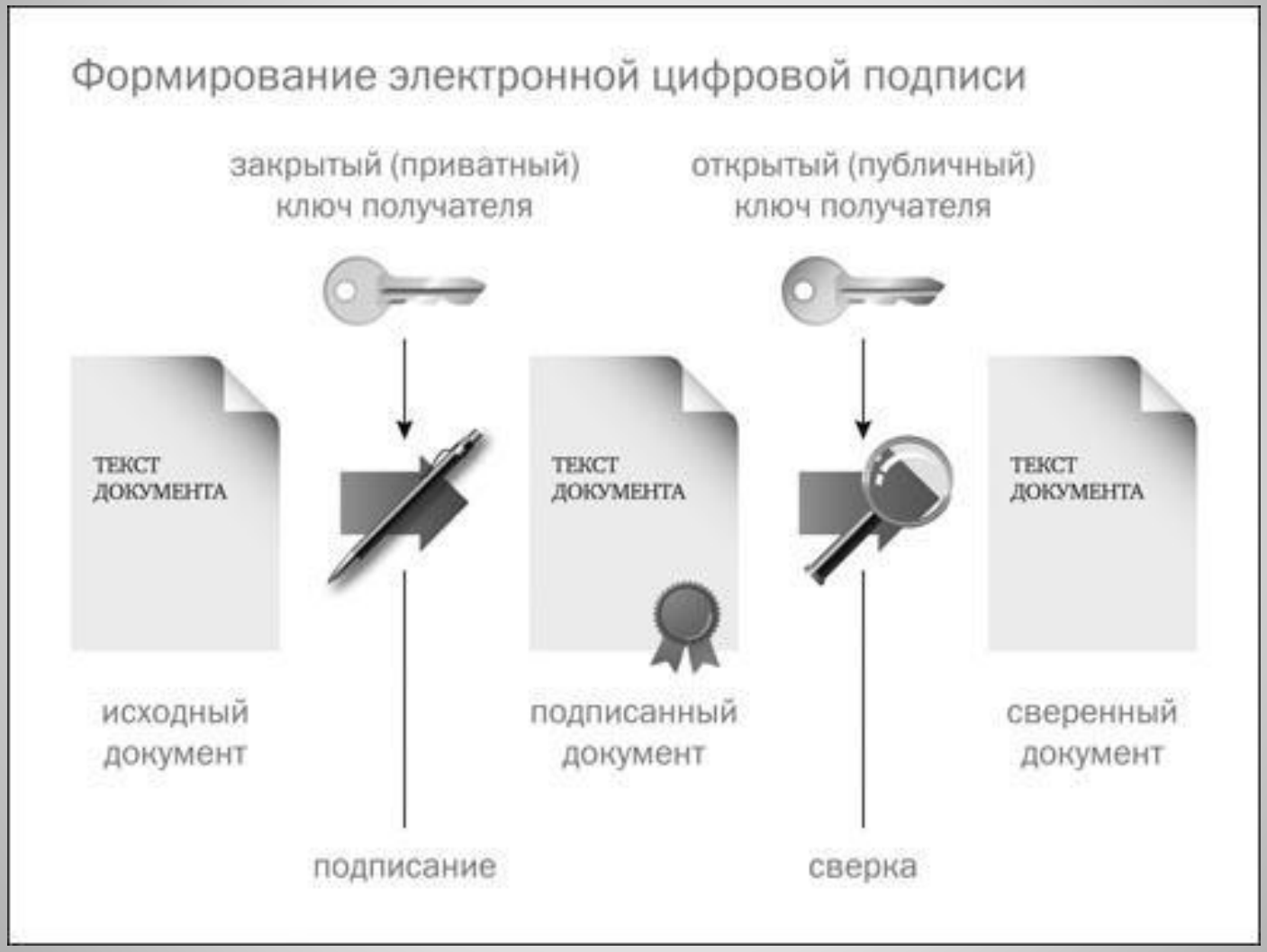
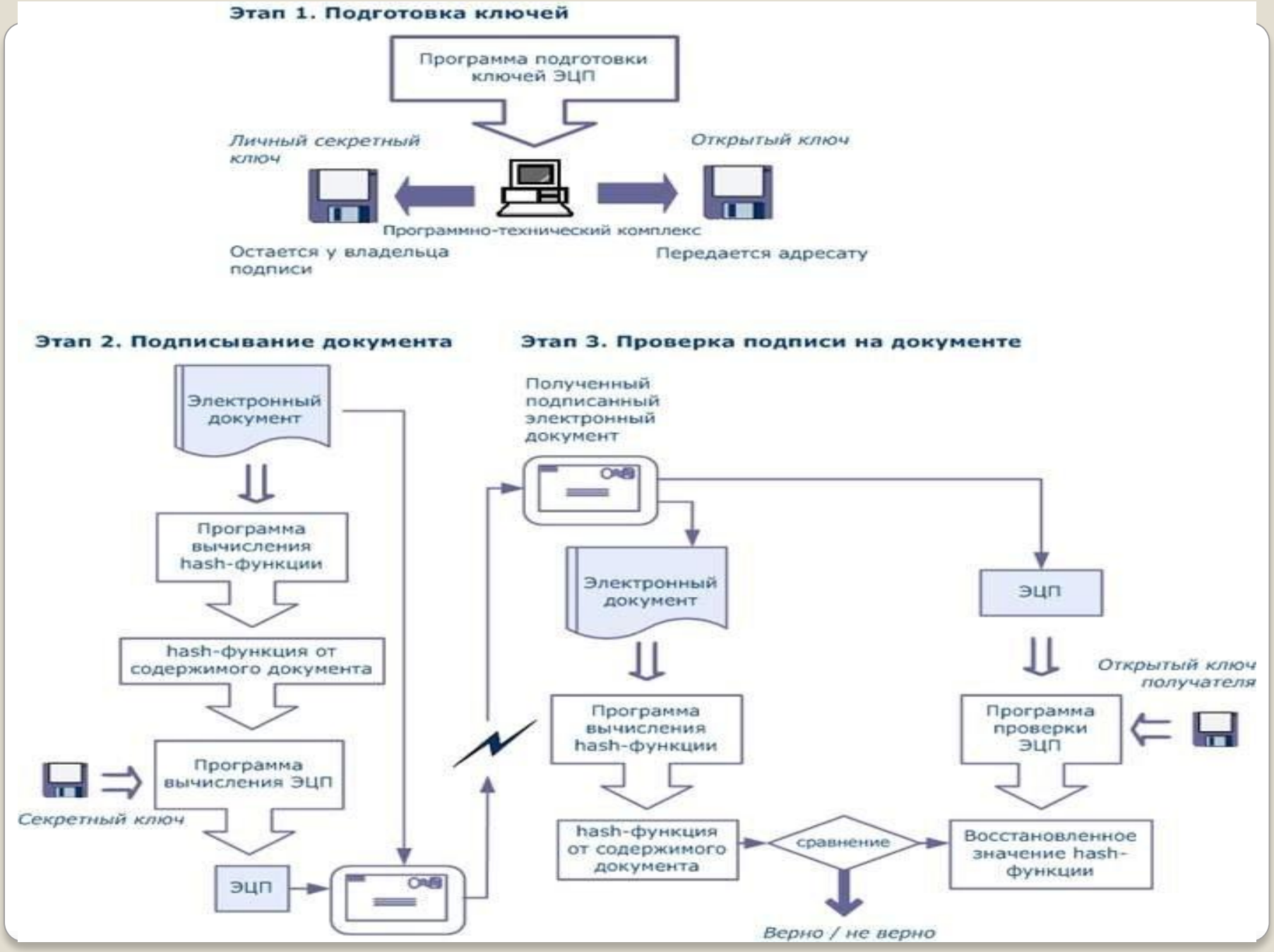

Формирование электронной цифровой подписи
закрытый (приватный) ключ получателя
открытый (публичный) ключ получателя
ТЕКСТ ДОКУМЕНТА
ТЕКСТ ДОКУМЕНТА
ТЕКСТ ДОКУМЕНТА
исходный документ
подписанный документ
сверенный документ
подписание
сверка

СХЕМА ЭЦП ВКЛЮЧАЕТ 3 ПРОЦЕССА

- **Генерация ключевой пары**
- **Формирование подписи**
- **Проверка** (верификация подписи)- проводится открытым ключом, соответствующим тому закрытому ключу, который использовался при подписании


Этап 1. Подготовка ключей
Программа подготовки ключей ЭЦП
Личный секретный ключ
Открытый ключ
Программно-технический комплекс
Остается у владельца подписи
Передается адресату
Этап 2. Подписывание документа
Электронный документ
Программа вычисления hash-функции
hash-функция от содержимого документа
Программа вычисления ЭЦП
Секретный ключ
ЭЦП
Этап 3. Проверка подписи на документе
Полученный подписанный электронный документ
Электронный документ
Программа вычисления hash-функции
hash-функция от содержимого документа
ЭЦП
Открытый ключ получателя
Программа проверки ЭЦП
сравнение
Восстановленное значение hash-функции
Верно / не верно

Хеш-функция

(контрольная сумма, дайджест сообщения)

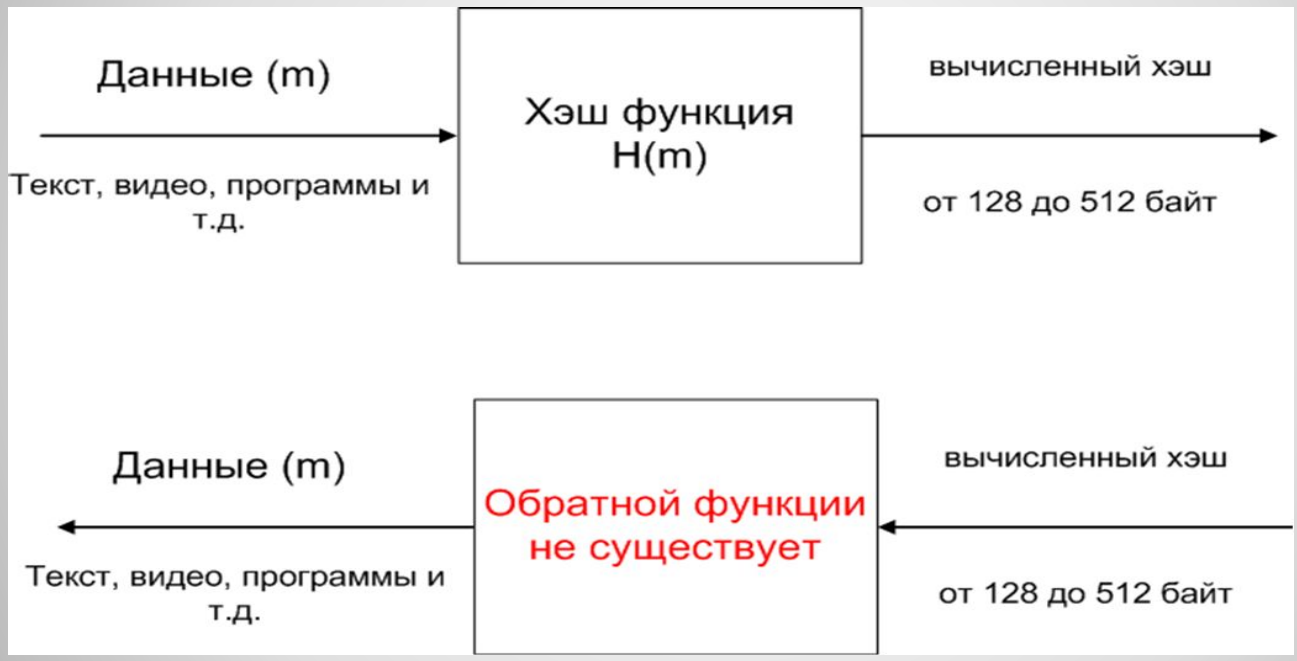
- ***Криптографическая хэш-функция h*** *— это функция, определенная на битовых строках произвольной длины со значениями в строках битов фиксированной длины. Ее значение часто называют хэш-кодом или хэш-значением.*
- **Хеширование** – преобразование входного набора данных.
- **Хеш-функция (функция свертки)** – сжимает исходный массив данных.

Можно назвать хэш функцию архивированием, в результате чего мы получаем очень маленькую последовательность байт, но восстановить исходные данные из такого «архива» нельзя.

- Пример:

ГОСТ Р 34.11-94 (длина 256 бит) -
d38e4f1bc5d03601486f4aca83fed00c82e1a36fdac27806cce4b9464af1e9f9

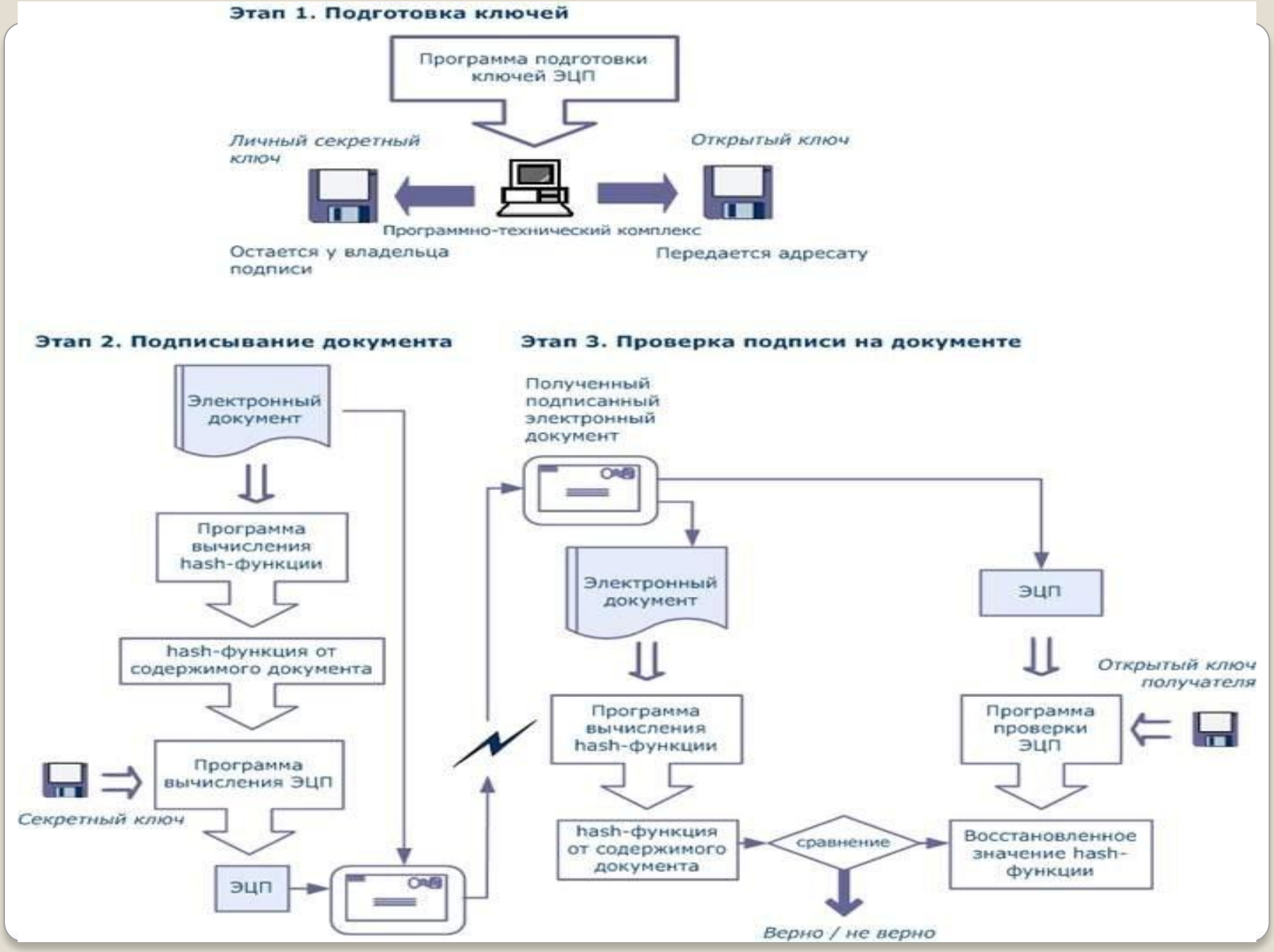
Использование хеш-функций



- Вычислительная сложность.
- Совместимость.
- Целостность.

Достоинства и недостатки Хеш-функции

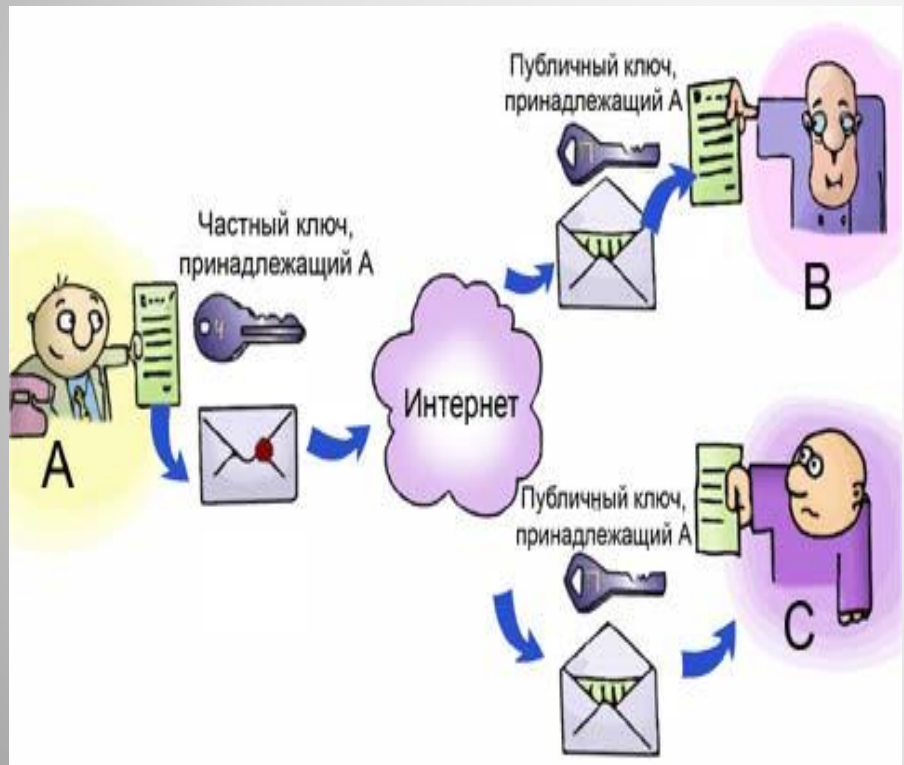
- малый размер
- стандартный размер
- нельзя подобрать исходные данные к значению за приемлемое время (например: получить пароль)
- низкая скорость вычисления (сопоставима с шифрованием)
- можно подменить
- для одного значения существует множество исходных данных


Этап 1. Подготовка ключей
Программа подготовки ключей ЭЦП
Личный секретный ключ
Открытый ключ
Программно-технический комплекс
Остается у владельца подписи
Передается адресату
Этап 2. Подписывание документа
Электронный документ
Программа вычисления hash-функции
hash-функция от содержимого документа
Программа вычисления ЭЦП
Секретный ключ
ЭЦП
Этап 3. Проверка подписи на документе
Полученный подписанный электронный документ
Электронный документ
Программа вычисления hash-функции
hash-функция от содержимого документа
ЭЦП
Открытый ключ получателя
Программа проверки ЭЦП
сравнение
Восстановленное значение hash-функции
Верно / не верно

СТАНДАРТЫ ЭЦП

- 1976 Уилфрид Диффи, Мартин Хеллман –понятие ЭЦП
- 1977– алгоритм RSA
- 1984- алгоритм GMR
- 1991 – алгоритм DSS
- 1994 –ГОСТ Р 34.10-94
- 2002- ГОСТ Р 34.10-2001

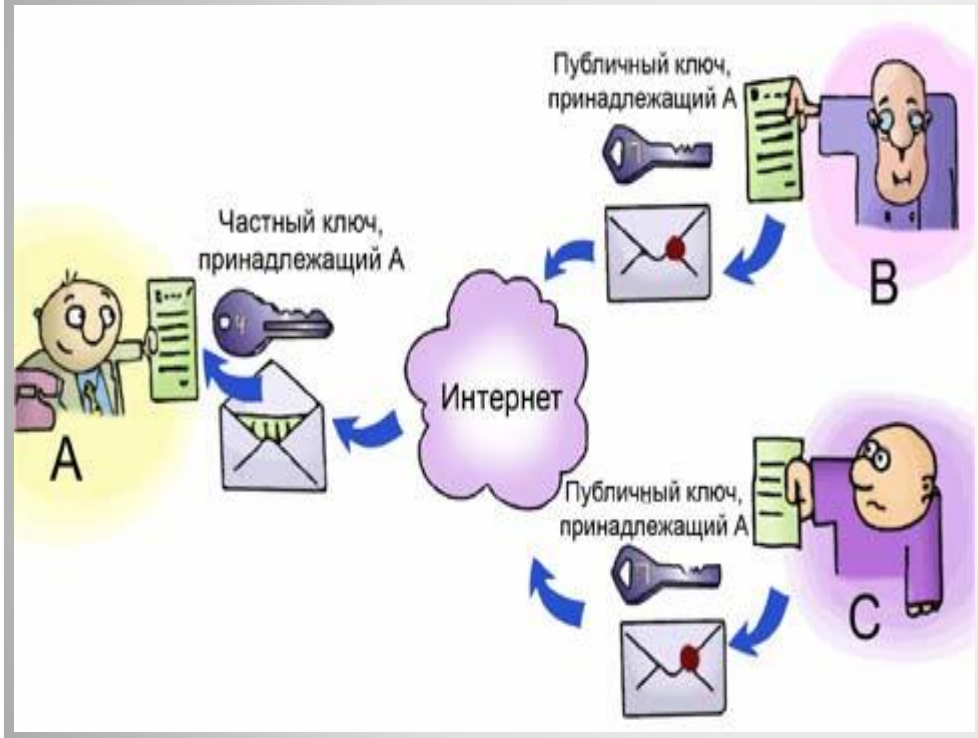
Асимметричное шифрование. Проблема конфиденциальности



пользователь **A** заранее отсылает публичный (открытый) ключ своим корреспондентам **B** и **C**, а затем отправляет им сообщение, зашифрованное его частным (секретным) ключом.

Сообщение мог послать только A (лишь он обладает частным ключом), т.е. проблема аутентификации решена. Но, например, B не уверен, что письмо не прочитал также C. Таким образом, конфиденциальность не обеспечена

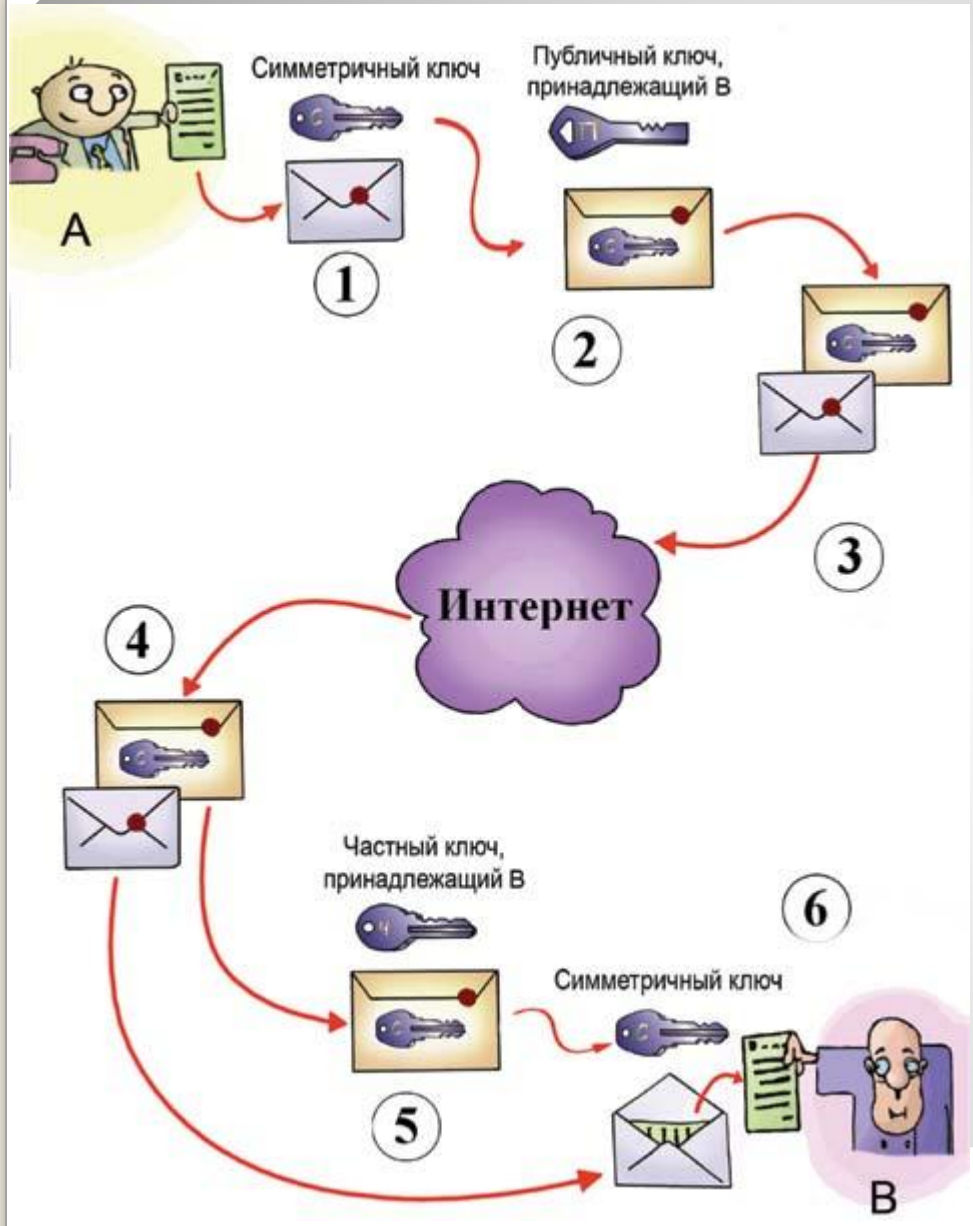
Асимметричное шифрование. Проблема аутентификации



А – может выложить свой публичный ключ в сети на сервере с открытым доступом. Каждый (В или С) может скачать его и прислать конфиденциальное письмо для А.

Сообщение может прочесть только А, так как лишь он обладает частным (секретным), ключом раскрывающим сообщение, то есть проблема конфиденциальности решена.

Но А не может быть уверен, что сообщение не прислал С, выдающий себя за В. Таким образом, аутентификация не обеспечивается

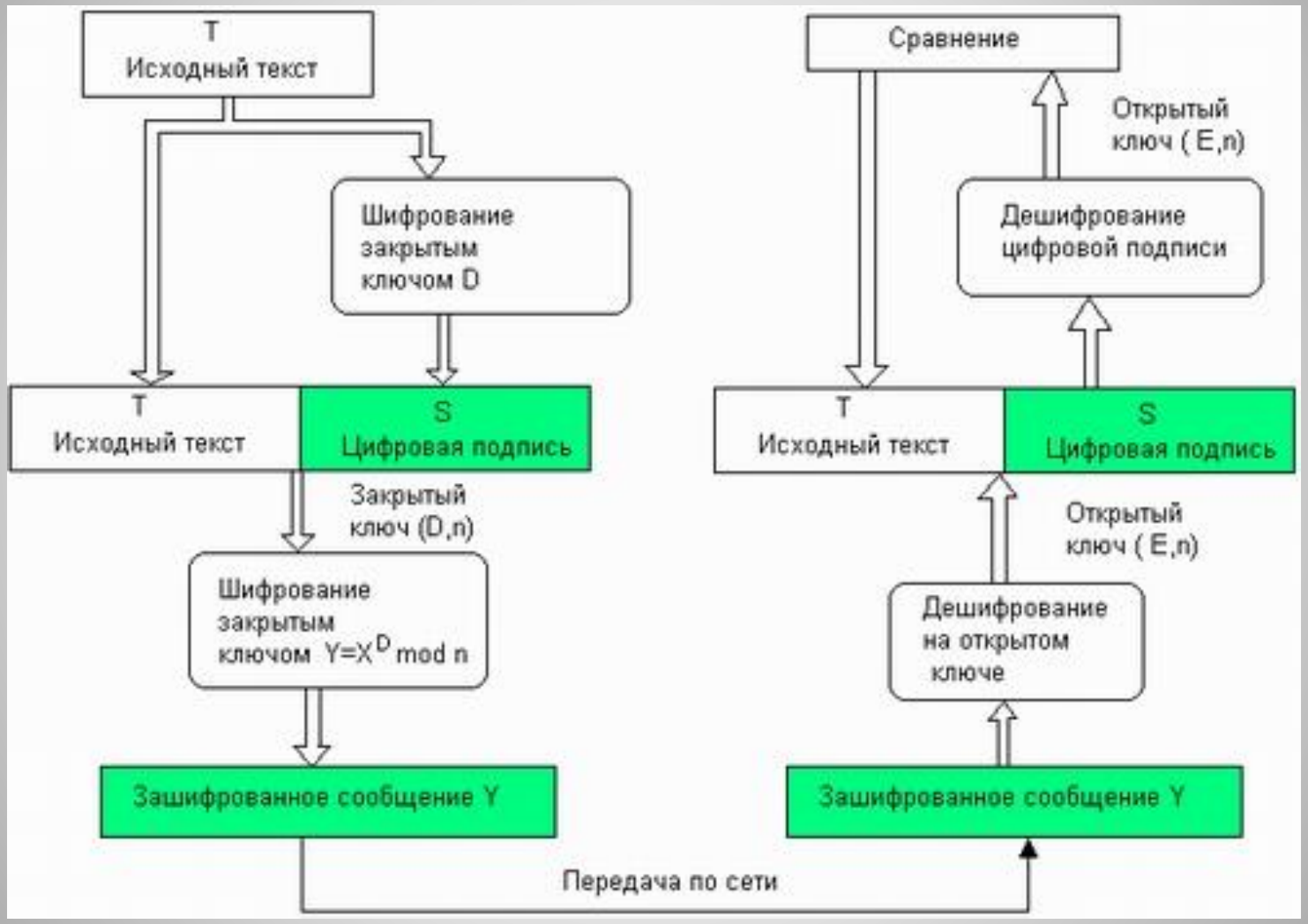


Шифрование с симметричным и асимметричным ключом

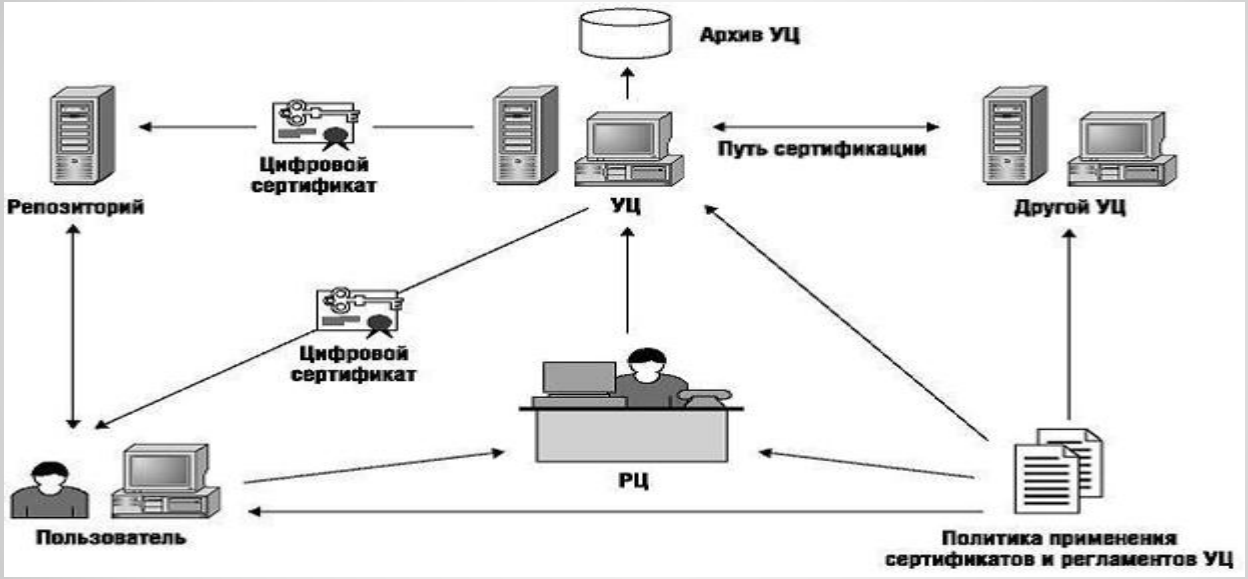
современные системы шифрования используют комбинацию асимметричной и традиционной симметричной систем шифрования. Шифрование с открытым ключом используется для передачи *симметричного ключа*, который служит непосредственно для шифрования передаваемой информации.

Схема шифрования с симметричным и асимметричным ключом

- **A** шифрует исходный файл с помощью симметричного (секретного) ключа (1). Затем (2) **A** получает из открытых источников публичный ключ, принадлежащий **B**, и с помощью этого ключа зашифровывает свой *симметричный ключ*. Далее (3) оба объекта (зашифрованный файл и зашифрованный *симметричный ключ*) отсылаются на адрес B посредством Интернета.
- **B** получает оба объекта (4). *Симметричный ключ* расшифровывается частным ключом, принадлежащим **B** (5) и, наконец, с помощью *расшифрованного симметричного ключа* расшифровывается исходный файл (6).
- Когда кто-то получает от вас сообщение, зашифрованное вашим частным ключом, он уверен в *аутентичности* послания. То есть в данном случае шифрование эквивалентно поставленной подписи.


T
Исходный текст
Шифрование
закрытым
ключом D
T
Исходный текст
S
Цифровая подпись
Закрытый
ключ (D,n)
Шифрование
закрытым
ключом $Y=X^D \bmod n$
Зашифрованное сообщение Y
Передача по сети
Сравнение
Открытый
ключ (E,n)
Дешифрование
цифровой подписи
T
Исходный текст
S
Цифровая подпись
Открытый
ключ (E,n)
Дешифрование
на открытом
ключе
Зашифрованное сообщение Y

Управление ключами



- **Time Stamping Authority – Служба штампов времени**
- **Online Certificate Status Protocol**

Ведущие производители Крипто-средств обеспечения УЦ

- «Крипто-Про» www.cryptopro.ru
- Cisco www.cisco.com/global/RU/win/
- «Инфотекс» www.infotecs.ru
- «Лан Крипто» www.lancrypto.com