# Лекция 9. Электронная подпись

Свойства собственноручной подписи:

- доказывает **добровольное согласие**,  
- именно от отправителя (**аутентичность**),  
- **неотказуемость** подписавшегося.  
- жесткая связанность с документом (**непереносимость**),  
- неизменяемость документа после подписания (**целостность**).

Для перехода в кибермир нужна электронная подпись с аналогичными свойствами.

Одного из первых применений ЭП:

После принятия запрета на испытания ядерного оружия в трех средах (Договор о нераспространении ядерного оружия подписан 1 июля 1968, вступил в силу 5 марта 1970) потребовался механизм контроля информации, передаваемой датчиками на территории стран участников. Необходимо удостовериться, что:  
- наблюдающий получает достоверную информацию (аутентичность),  
- наблюдаемый передает только необходимое (открытость).

Первый стандарт цифровой подписи – DSA (1993) фиксировал длину ключа в 512 бит. Далее длину делали переменной.

Создание подписи



Проверка подписи



1-ФЗ от 10.01.2002 «Об электронной цифровой подписи»:

**ЭЦП** — аналог собственноручной подписи, служащий для придания электронному документу юридической силы, равной бумажному документу, подписанному собственноручной подписью правомочного лица и/или скрепленного печатью.

Статья 4 ФЗ «Об электронной цифровой подписи»: ЭЦП признаётся равнозначной собственноручной подписи в документе на бумажном носителе при условии, что **сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа** при наличии доказательств, определяющих момент подписания.

Информация в электронной форме, подписанная электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия.

Формат усовершенствованной подписи предусматривает обязательное включение в реквизиты подписанного документа **доказательства момента создания подписи** и доказательства действительности сертификата в момент создания подписи.

63-ФЗ от 6.04.2011:

**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

Подпись формируется в результате преобразования информации с использованием **средств криптографической защиты информации (СКЗИ)**, используя алгоритм с открытым ключом.

Открытый ключ пользователя доступен всем, так что любой может проверить подпись под документом.

Подпись ставится не на сам документ, а на его хэш (MD5, SHA). Хэш-функции не являются частью алгоритма ЭЦП, поэтому в схеме может быть использована любая надёжная хэш-функция.

Виды подписи :

- простая (любое подтверждение, зафиксированное договором – например, SMS)

- усиленная

-- неквалифицированная

-- квалифицированная (ключ лежит в квалифицированном сертификате - подлежит созданию с использованием средств аккредитованного удостоверяющего центра)

Неквалифицированная ЭП

...

Квалифицированная ЭП

…

**Архитектура клиентской системы:**

* Доверие к ОС (криптофункции являются частью ОС в виде dll, подписанной разработчиком ОС), которая контролирует целостность криптобиблиотек – реально выполняющих все операции.

Например, Windows периодически проверяет подключенные Cryptographic Service Providers (CSP) - чтобы не подменили.

* Любая программа может воспользоваться CryptoAPI – интерфейс к CSP (поэтому вся работа идет с дескрипторами)

**Виды подписи:**

* Обычные (необходимо пристыковывать к подписываемому документу, например, алгоритмы, основанные на эллиптических кривых (ECDSA, ГОСТ Р 34.10-2001, ДСТУ 4145-2002));
* С восстановлением документа (содержат в себе подписываемый документ: в процессе проверки подписи автоматически вычисляется и тело документа(RSA)).

Открытый ключ может быть использован для (организации защищенного канала):

* аутентификация (для проверки подписи владельца);
* конфиденциальность (для шифрования посылаемых ему данных).

**Архитектура передачи ЭП:**

Есть арбитр, которому доверяют все заинтересованные лица (хоть таких и не бывает)

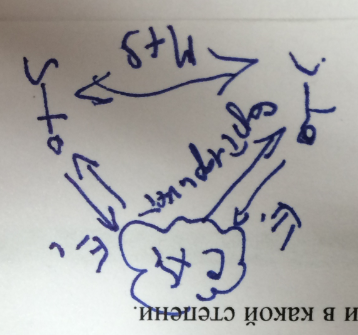
Алгоритм:

- отправитель публикует ключ, которым может быть проверена его подпись (подписанный документ может быть переиспользован),  
- фиксация в центральной базе данных отметок времени (каждая передача зафиксирована) и хешей документов (документы не публикуются до момента расследования),  
- подписанный документ передается получателям,  
- получатели проверяют подпись подтвержденным арбитром открытым ключом.

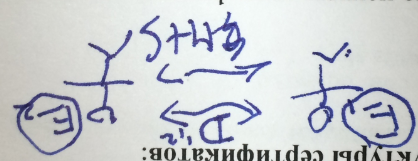
Существует **две модели организации инфраструктуры сертификатов**:

* децентрализованная (PGP).
* централизованная (PKI)

В *децентрализованной* модели каждый пользователь самостоятельно выбирает, каким сертификатам он доверяет и в какой степени.



В *централизованной* модели существуют корневые центры сертификации, подписям которых обязан доверять каждый пользователь.



*В PGP не следует передавать открытый ключ адресату заранее по EMail. Злоумышленник может перехватить сообщение, извлечь оттуда ключ, и заменить на свой. Один из наиболее безопасных способов передачи открытого ключа - использовать удостоверяющий центр.*

Аутентификация посредством цифровых сертификатов основана на применении асимметричных криптографических методов: данные, зашифрованные общедоступным открытым ключом, могут быть расшифрованы, только владельцем парного закрытого ключа.

**Удостоверяющий центр/ Центр Сертификации (Certificate Authority - CA)** - специализированный полномочный орган сертификации, выпускающий сертификат, заявляет, что указанный в сертификате открытый ключ принадлежит именно тому субъекту, о котором говорится в сертификате.

Конечно, необходимо доверять самому центру сертификации и заранее получить его открытый ключ или самоподписанный сертификат. Сертификаты общеизвестных центров сертификации, например Verisign, для обеспечения повышенной безопасности обычно устанавливаются компанией производителем программного обеспечения заранее, в такие программные продукты, как браузеры.

**Х.509** – Стандарт формата электронного сертификата и списков отозванных сертификатов, предусматривающий использование различных алгоритмов создания цифровой подписи. Сертификаты стандарта Х.509 содержат:

- версию и используемый алгоритм создания подписи

- идентификационные данные и подпись организации, которая выдала сертификат

- срок действия сертификата

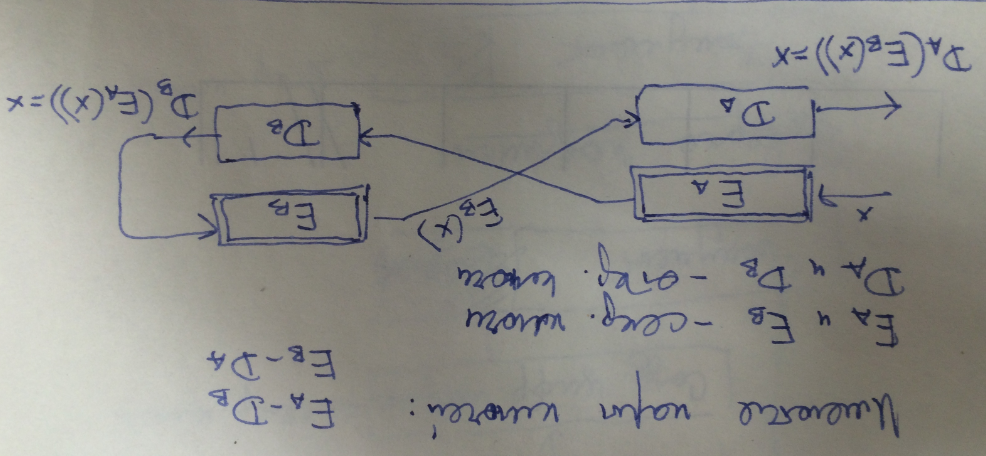
- идентификационные данные владельца

- открытый ключ владельца

**Виды аутентификаци**:

* Односторонней (проверяется только клиентский сертификат);
* Двухсторонней (на стороне сервера проверяется клиентский сертификат, а на стороне клиента – серверный).

**Взаимное подтверждение полномочий**



**Электронный сертификат (сертификат открытого ключа, сертификат ЭП)** — цифровой или бумажный документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Содержит информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название центра сертификации и т. д.

Использование сертификата:

* Необходимо, например, средствами Web, отправить в CA запрос на выдачу сертификата (Certificate Signing Request – CSR), содержащий необходимую для выдачи сертификата информацию;
* Сотрудники органа сертификации обрабатывают запрос и производят генерацию сертификата, который может быть выслан по электронной почте;
* Органы сертификации также предоставляют списки аннулированных сертификатов (Certificate Revocation List – CRL), в которых перечисляются сертификаты, аннулированные до окончания срока их действия. Периодически опрашивая CRL-списки, пользователь может проверить, имеют ли сертификаты, присылаемые ему другими лицами, законную силу.
* Доверие любому сертификату пользователя определяется на основе цепочки сертификатов. Причем начальным элементом цепочки является сертификат центра сертификации, хранящийся в защищенном персональном справочнике пользователя.

Пример кода создания и проверки подписи с использованием библиотеки capicom.dll

*Init (){*

*this.Signer=new ActiveXObject('CAPICOM.Signer');*

*var Store=new ActiveXObject('CAPICOM.Store');*

*this.StoreName="MY";*

*this.StoreLocation = CAPICOM\_CURRENT\_USER\_STORE;*

*Store.Open(this.StoreLocation, this.StoreName);*

*var Certificates = Store.Certificates;*

*if(Certificates.Count > 0){*

*Certificates = Certificates.Find(…);*

*}*

*this.Signer.Certificate=Certificates(1);*

*}*

*Sign (s){*

*var SignedData=new ActiveXObject("CAPICOM.SignedData");*

*SignedData.Content=s;*

*var Message=SignedData.Sign(this.Signer,bDetached);*

*return Message;*

*}*

*Verify (s){*

*var SignedData=new ActiveXObject("CAPICOM.SignedData");*

*SignedData.Verify(s,bDetached, VerifyFlag);*

*return SignedData.Content;*

*}*

using System.Security.Cryptography

…

//Create a new instance of DSACryptoServiceProvider.

DSACryptoServiceProvider DSA = new DSACryptoServiceProvider();

//The hash to sign.

byte[] Hash = {…};

//Create an DSASignatureFormatter object and pass it the DSACryptoServiceProvider to transfer the key information.

DSASignatureFormatter DSAFormatter = new DSASignatureFormatter(DSA);

//Set the hash algorithm to SHA1.

DSAFormatter.SetHashAlgorithm("SHA1");

//Create a signature for HashValue and return it.

byte[] SignedHash = DSAFormatter.CreateSignature(Hash);

…

//Create an DSASignatureDeformatter object and pass it the DSACryptoServiceProvider to transfer the key information.

DSASignatureDeformatter DSADeformatter = new DSASignatureDeformatter(DSA);

//Verify the hash and display the results to the console.

if(DSADeformatter.VerifySignature(Hash, SignedHash)) {…}

Документы:

1. N 1-ФЗ ОТ 10.01.2002 «ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ»
2. N 149-ФЗ от 27.07.2006 «ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ»
3. ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»