Технически университет – София

ПГ по Компютърни Технологии и Системи - Правец

Упражнение - 3

СИСТЕМИ ЗА СИГУРНОСТ

Тема: Подписване на електронен документ с последваща валидация

Изготвил:

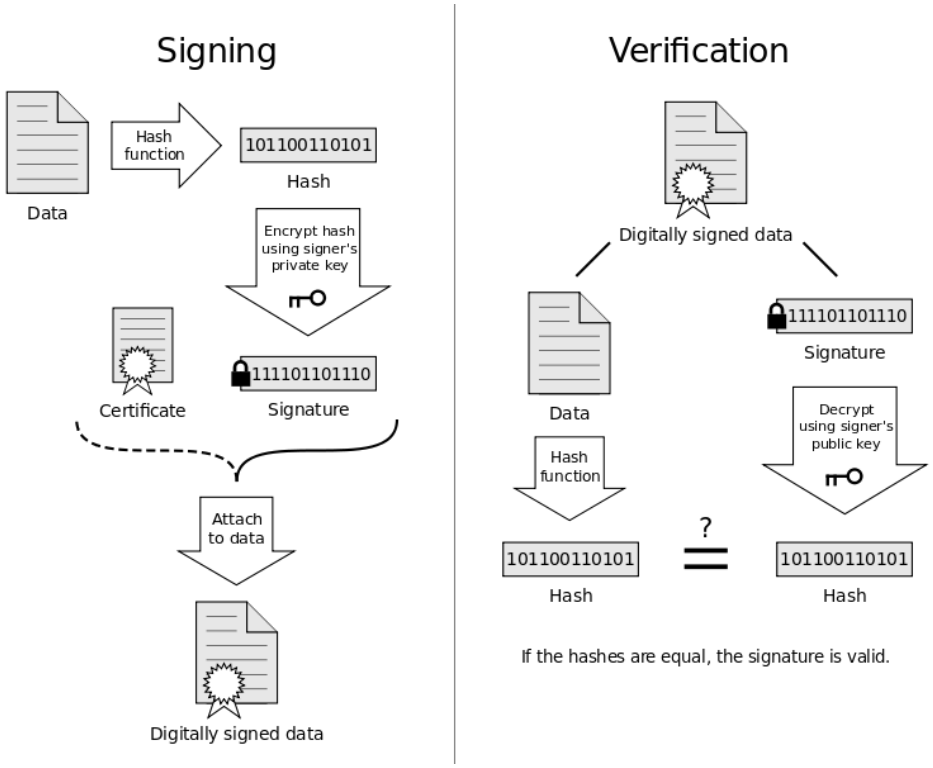
Доц. д-р Румен Трифонов

Електронен подпис и електронно подписване на документи.

Електронният подпис е легално техническо средство, което дава възможност на всеки един от нас да подписва документи по електронен път, като те бъдат напълно приравнявани с документите подписани на ръка.

1.Същност на електронният ключ.

По своята същност електронният ключ представлява един файл, в който се съдържа цялата необходима информация за човека или фирмата, която подписва дадено електронно съобщение. Подписвайки го електронният подпис гарантира, че подписаният документ не е изменян от момента на подписването му. Удостоверяването на това, дали едно електронно съобщение не е изменяно се удостоверява посредством един изключително прост начин. Съдържанието на документа се преработва през дадена hash-функция. Получената битова последователност се криптира посредством алгоритъм за криптиране с частен ключ. Получената битова поредица се прикача към файла и се получава електронно подписан документ. Цялата тази процедура е показана на принципната схема по-долу.



Проверката дали даден документ е подписан и дали този подпис е положен на точно този текст или документ става по следният начин. Извличат се данните от документа, минават през hash функция и се получава даден резултат. Този резултат се сравнява с подписа на документа, който се декрептира чрез публичният ключ на електронният подпис. Ако двете hash стойности съвпадат, то документа се счита за подписан от съответният поспис и може да се смята, че информацията в документа е напълно достоверна.

2.Технология на цифровият подпис.

2.1.Хешране

Това е първата стъпка, която се извършва при подписването на документ с електроннен подпис. Хеширането най-общо казано е алгоритъм, при който от даден входен текст (без да се има в предвид дължината) се преобразува на дадена поредица от числа и букви, която е с точно определена дължина. При общоприетите алгоритми за хеширане най-малката промяна на входният низ допринася за тотална промяна на изходният такъв. От чисто математическа гледна точка след като изходната поредица е с точно определена дължина, то би следвало, че при дадени два или повече напълно различаващи се входни текстове може да се получат напълно еднакви стойности след обработването им чрез hash функцията. Тъй като дължината на изходният низ е ограничена, то следва че хеширащият алгоритъм е напълно еднопосочен и от даден хеш не можем да възтановим даден текст. В случая с електронният подпис се смята, че хеширащите алгоритми са достатъчно добри за целта, тъй като вероятността за колизия (напълно съвпадение на два низа) е доста малка. При първите алгоритми за хеширане вероятността за колизия е 2^{80}, ако се добави, че и ако е документ и съобщението трабва да бъде смислено от човещка гледна точка, вероятността променният текст да даде абсолютно същият хеш код граничи с нула. По-горе в текста казахме, че функцията е еднопосочна. Това е така, но трябва да се отбележи, че е възможно да се направи софтуер, който да прави напълно произволни символни поредици и сравнявайки техният хеш с желаният хеш да намери изходното съобщение. За тази цел ще е

нужен доста мощен суперкомпютър, при това той трябва да работи няколко години.

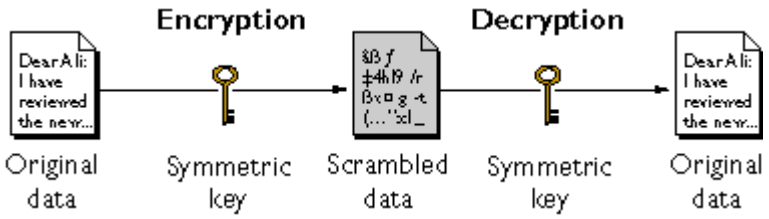
За целите на електронният подпис се ползват няколко по-популярни алгоритъма за хеширане на информация. Такива например са SHA-2 256 и SHA-2 512. По рядко но все още се ползва MD5 .

2.2 Криптиране и декриптиране

Криптирането и декриптирането са операции по трансформация на даден текст по такъв начин, че никой да не може да разбере текста освен получателя на съобщението. Другото наимонование на тези два процеса се наричат шифриране и дешифриране. С повечето модерни криптогравски алгоритми, свойството да се запази текста не се дължи до такава степен на алгоритъма, колкото до ключа чрез който се криптира текста. Ключ при криптирането се счита текст или число, чрез който на базата на алгоритама за криптиране се постига криптираният текст. Чрез него на по-късен етап се постига и декриптирането на текста. Още от древни времена до ден днешен основен проблем при криптирането с ключ е неговото пренасяне до получателя на съобщенията, както и неговото съхранение в последствие.

2.2.1 Криптиране чрез симетричен ключ

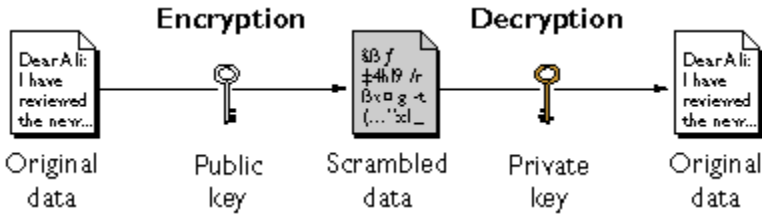
Най-старият известен начин за криптиране чрез ключ е посредством „Криптиране чрез симетричен ключ”.



При този вид криптиране, ключът за декриптиране може да бъде изчилслен от ключа за криптиране. Напрактика двата ключа са взаимозаменяеми и за възстановяване на информацията е нужен само ключа за криптиране. В по старите алгоритми със симетричен ключ се ползва само един единствен ключ за двете операции. Предимството на този начин на криптиране на информацията е, че изключително бързо стават и двете операции. Този способ също доставя степен на аутентикация , защото информацията криптирана чрез един ключ по никакъв начин не може да бъде декриптирана чрез друг ключ. По този начин и изпращача на съобщението и получателя са напълно сигурни, че съобщението не може да бъде разчетено от други хора. Проблемът при симетричното криптиране е запазването на ключа само при хората или устройствата , които четат или пишат информация. Ако ключът беде разбит или откраднат, то вече информацията не е сигурна. Ключът не е нерабиваем от математическа гледна точка, но напрактика , ако накой тръгне да разбива такъв ключ може да му отнеме седмици, дори месеци и то на суперкомпютър. По презумпция се счита,че разбиването на симетричен ключ отнема толкова време и разходи, заради които съобщението не си струва да бъде разчетено.

2.2.2 Криптиране, чрез асиметричен ключ

Друг известен подход за криптиране на информация е криптиране чрез публичен ключ. Най-често използваните имплементации на този тип криптиране са алгоритмите RSA , DSA и ElGamal. Този вид криптиране се нарича още и „Криптиране чрез асиметричен ключ”.



Фигурата по-горе показва опростена схема на криптирането с публичен ключ. На нея също е показана и принципната употраба на публичният и частният ключ. При криптирането на оригиналният текст се използва публичният ключ. За да прочете съдържанието от даден потребител или машина се използва личният ключ на потребителя. Трябва да се спомене, че двойката ключове е предварително генерирана и и при загуба на един от двата ключа, декриптирането или съответно криптирането на дадено електронно съобщение става напълно невъзможно.

Спрямо симетричното криптиране, криптирането с публичен и частен ключ изисква повече изчисления и следователно не е подходящо за голями масиви от данни. По някога се прави следната процедура при нуждата от криптиране на голямо количество от информация. Използва се криптиране със симетричен ключ и се криптира самият ключ чрез алгоритъм за асинхронно криптиране.

Практиката показва, че схемата в обратен ред също е валидна. Данните могат да бъдат криптирани , чрез частният ключ и да бъдат

декриптирани чрез публичния. Това не се препоръчва за криптиране на важна информация, защото по дефиниция се смята, че публичният ключ е публикуван някъде. Затова първият подход се използва при подписването на документи, чрез електроннен подпис. Тъй като частният ключ е един единствен и той се дава само на притежателят на подписа, се счита, че това е единственият човек, който може да подпише даден документ. Публичният ключ може да провери посредством подходящ софтуер, дали съобщението е подписано или не от даден потребител.

2.2.3 Дължина на ключовете и сигурност на криптирането.

По общо казано, сигурността на криптирането е свързано с трудността на намирането на ключа, който пък от своя страна зависи от алгоритъма за криптиране и дължината на ключа. Последното е факторът, който е ръководещ при защитата на данни. Това е така, защото алгоритмите за криптиране на данните са всеобщо известни с цел да бъдат прочетени от всеки интернет браузер или офис пакет. Сигурността на електронният подпис идва от дължината на ключа. Дължината им се измерва с битове. Например 128-битови ключове са 3×10^{26} пъти по-силни от 40-битови такива. Различните алгоритми може да изискват различна дължина на ключовете, за да се гарантира абсолютно същата степен на защита. Въпреки, че 128-битовите ключове са все пак краен брой комбинации, се смята, че ключовете са достатъчно сигурни, защото дори най-мощният компютър ще му отнеме значително време да разбие ключа. В практиката най-често се използват ключове с големина между 128 и 2048 бита, поради което

методът на грубата сила (brute force) не може да бъде приложен за отгатването на таен ключ.

Откриването на личен ключ, който съответства на даден публичен ключ, е теоретически възможно, но времето и изчислителната мощ, необходими за целта, правят такива действия безсмислени

3.Цифрови сертификати и PKI (Public Key Infrastructure).

PKI(Инфраструктурата на публичният ключ) преставлява цялата система, която удостоверява валидността и доверието на всеки публичен ключ. Чрез тази инфраструктура се удостоверяма кой, къде и как е издал даден електроннен подпис.

3.1. Начини за удостоверяване на валидността на публичен ключ.

Когато две непознати една за друга страни искат да си обменят инфромацията по между си възниква следният проблем, как и двете страни да пренесат публичните си ключове по между съвсем безопасно. Съществуват математически алгоритми за целта, но те защитават ключовете от гледна точка на криптографията, но не и ако връзката баде подслушвана от трето лице. Съществува вариянт двете лица да предоставят своите ключове на трето, на което те напълно имат доверие. В еволюцията на електронните подписи възникват следните типове „доверие”.

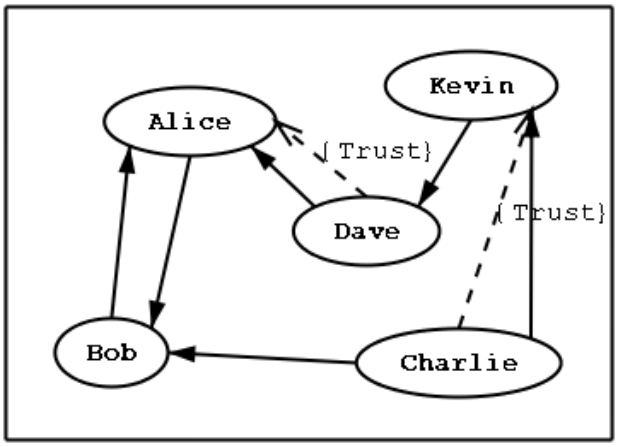
3.1.1 Директно доверие (direct trust)

Това е най-простият начин за подписване на електронни документи. При този модел има централен сървър, който се служи като център на системата. Той подписва и той проверява валидността на подписите. Има различни варианти на реализация. При единият, сървърът може да съхранява публичните ключове на всички участници и само да подписва документите. Вторият варият е сървърът да подписва посредством личен ключ, като по този начин гарантира сигурност на всички участници в системата.

Проблемът при този вид организация е, че сървърът трудно ще издържи на натоварването да обслужва повече от N на брой клиента. Това е така, защото както описахме по-горе, подписването и валидацията на електронен подпис отнема много изчислително време. Затова „Директно доверие” се прилага предимно в малки компании, които използват електронните подписи предимно за вътрешно ползване.

3.1.2 Модел „Web of trust”

При този модел не се налага да има централен сървър, който да обслужва всички заявки за подписване, а се прави цяла мрежа от доверени сървъри, които могат да подписват дадени електронни документи. Идеята е, че ако моят сървър може да подписва и аз вярвам, че при него не може да има зланамерен достъп, то може да се свържат и други доверени сървъри. И по този начин се получава една верига от доверени сървъри. Например на картинката по-долу



An example of the
web of trust model

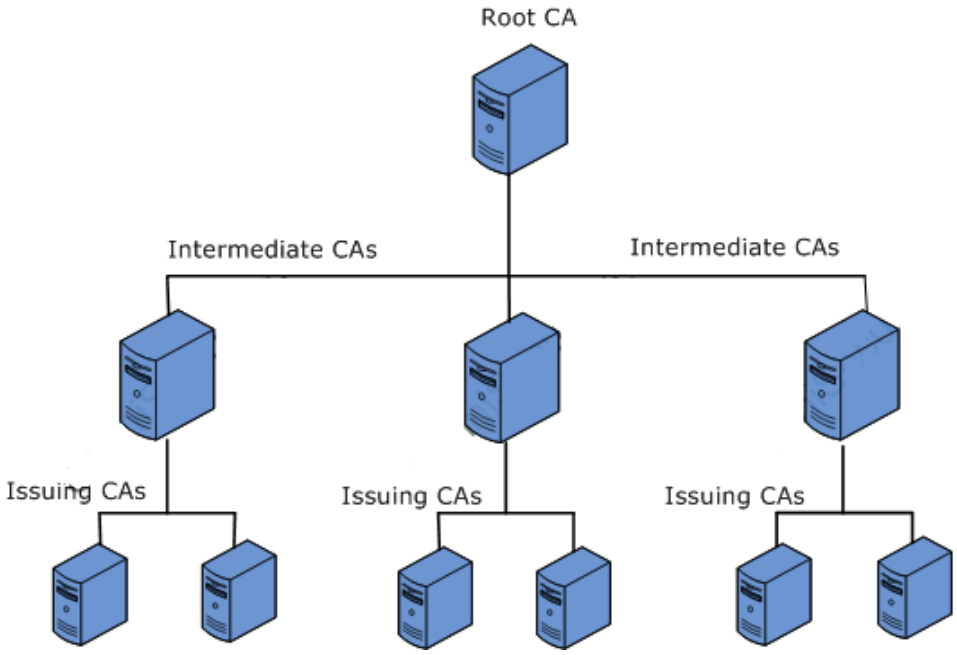
Ако Charlie има доверие на Bob и Kevin, а Alice има само доверие на Bob, то Charlie има индиректно доверие на Bob. От друга страна всеки един документ подписан от Charlie се счита за валиден от гледна точка на Alice. Това е така, защото Alice има доверие на Dave, той от своя страна вярва на Kevin, който пък има доверие на Charlie . Това е добре организирана система, но само ако сме сигурни в лоялността на всеки един от участниците в нея. Напрактика може да се получи, че ти да дадеш публичният си ключ на злонамерено лице, защото, някой го е добавил в организацията. Това е приложимо само за малки организации, но не и за организации и фирми с много на брой участници.

3.1.3. Йерархичен модел.

При този модел абсолутно всички участници вярват само на няколко доверени лица. Те се наричат сертификационни органи (certification authorities – CA). Сертификатите използвани по този модел сеизползват, предимно в съвременното подписване на документи и за осъществяване на защитена връзка през интернет. Този сертификат може да бъде поискан с цел да бъде установено дали вие наистина се

намирате на даден интернет адрес или в друг сайт, кой е клонинг(така наречиният sniffing). Най-често това се получава със сайтовете на банки и други парични институции с онлайн плащания, с цел кражба на номера на банкови сметки. Поради това всеки модерен интернет браузър има в себе си хранилище на всички валидни ертификационни органи.

В йерархичният модел на доверие всички участници вярват на сертификационнете органи(root CA) безусловно. Те от своя страна могат да попишат сертификатите на други органи, наричани междинни (Intermediate CAs). Тяхната роля е оторизацията на фирмите или организациите, от които ние като потребители можем да си купим електроннен подпис. Напрактика се получава нещо като пирамида , в които всеки един от има публичните ключове на предходното ниво, по този начин се гарантира сигурността на всеки един от участниците. Схематично е показано на картинката по-долу.



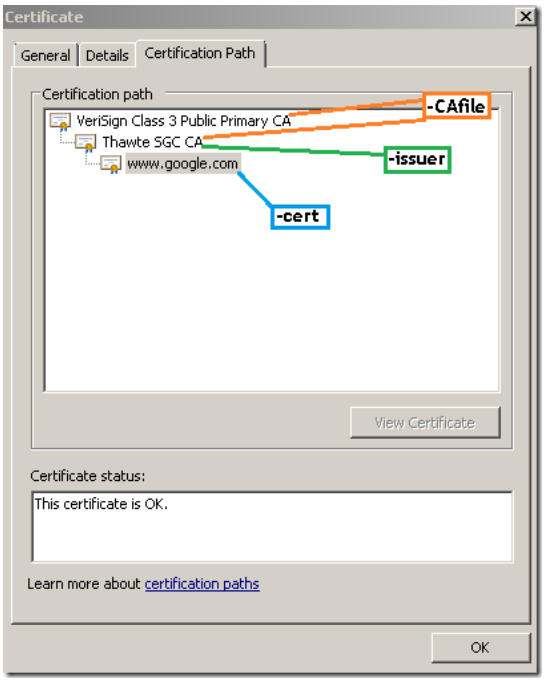
Сертификационните органи (root CA) подписват сами на себе си сертификат,чрез който подписват на другите сертификационни органи, който са по-ниско ниво(Intermediate CAs). Root – сертификатите на големите оторизационни органи са публично достъпни и могат да бъдат използвани с цел да бъде направена вирификация на други сертификати. Най-често се получава, че ние запитвайки дадена система да провери някакъв сертификат за валидност се получава, че тя пита междиннте сертификационни органи, защото те имат пълните правомощия да подписват от името от главният сертификационен орган.

Напрактика всеки един от нас може да си направи сертификат. Всички модерни програмни езици имат вградени в себе си модул за генериране на сертификати, но тези сертификати не са такива, чрез които може да бъдат подписвани други сертификати. Те могат при създаването си да бъдат подписани от даден сертификат. Това е направен с цел да не може програмист сам да си създаде сертификат, да му сложи името на сертификационният орган и да си издаде сам на себе си подписан сертификат. Така се постига и невъзможността хакери да издадат сами на себе си сертификат, на трето лице. Напрмер да подписват документи от името на Google.

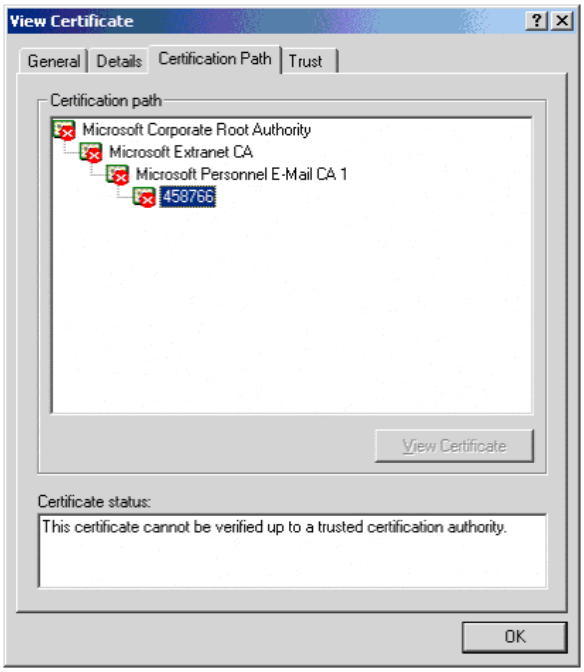
Валидациата на серитификат се прави на няколко етапа, първо се проверява дали той е изобщо валиден, дали не е с истекъл срок на валидност. И второ трябва да бъде проверено неговата сертификационна верига. За тази цел програмите използващи електронни подписи гледат кой е в началото на веригата, ако той е в списъка със сертификационните органи, гледа вторият и т.н. Ако някой по веригата не е в списъка на оторизираните издатели на сертификати,

то сертификата се счита за невалиден. Също така ако някой от сертификатите е с изтекъл срок на годност пак електронният подпис се счита за невалиден. Друга причина за това един подпис да е невалиден е, ако по някаква причина, на някой от сертификатите по веригата не им се позлволява да посписват други сертификати или им е отнето това право.

Валиден сертификат:



Невалиден сертификат:



В действителност при отсъствието на интернет може да се прави също проверка, дали даден сертификат е валиден. Това става благодарение на факта, че във всяка операционна система се съдържа „Хранилище за сертификати”. В него се съдържат сертификати, ключове и сертификационни вериги. С цел сигурност, хранилището е обезопасено на две нива, всяко хранилище си ема собствена парола, а всеки ключ или сертификат отново са защитени с

парола. Например в хранилищито на IE8 са включени около 150 сертификати и ключове на сертификационни органи.

Сертифицирането на уебсайтове става по същият начин, но с дребни изключения. За да бъде защитен един уебсайт за електронно банкиране например е нужно на първо място връзката да бъде сигурна, за да не може да бъде послушвана от трети лица. И на второ място да бъде потребителя да е сигурен, че вкарва личните си данни в точният сайт. За това се грижи един точно определен сертификат – SSL-сертификат. Всеки SSL сертификат се състои от публичен и частен ключ. Благодарение на тях се създават защитени специални ключове за всяка връзка. Това се случва благодарение на т. нар. “ръкостискане” (handshake), в което едно произволно число, генерирано от клиентската страна се криптира с публичния ключ. Частният ключ, които е на сървъра единствен може да дешифрира това число, с чиято помощ се създават тези специални ключове. В крайна сметка браузърът автоматично потвърждава, че издателят на сертификата е разпознат. За извикване на сертифицирани сайтове се използва https://. Сигурността при този вид връзка е значителна поради факта, че се използват 256-битови сертификати, което прави подслушването и разчитането на данните доста дълъг и сложен процес, който не е гаранция, че ще завърши с успех. До настоящият момент не е установено, да е имало успешно разбиване на SSL връзка.

4.Задачи за изпълнение

1) Направете ваш обикновен цифров сертификат със средствата на Microsoft Office.

2) Подпишете с вашия обикновен цифров сертификат документ подготвен на MS Word.

3) Подпишете с вашия обикновен цифров сертификат документ подготвен на MS Excel.

4) Подпишете с универсален електронен подпис електронно съобщение подготвено на MS Outlook.

5) Валидирайте и верифицирайте универсалния електронен подпис на получено електронно съобщение на MS Outlook.