Аутор: Данијел Јовановић

Дигитални сертификати

Дигитални сертификати омогућавају успостављање сигурних канала комуникације на Интернету. Да би крајњи корисници приликом приступа серверу (веб-сервер, имејл сервер и сл.) преузели податке, приступили осетљивим подацима или их дали на увид (нпр. корисничке креденцијале) морају бити сигурни у потпуну безбедност.

То значи да су приступили правом серверу те да је комуникација са сервером сигурна односно шифрована и да нико не може да пресретне, прочита или промени податке који се размењују.

Коришћење SSL/TLS технологије омогућава тражену сигурност, али захтева да стране у комуникацији имају одговарајуће дигиталне сертификате.

Тако се данас у комуникацији на Интернету доминантно користе:

- Дигитални серверски сертификати - прибављају се за веб, имејл, RADIUS и сличне сервере, а користе се као идентификација сервера како би се успоставило поверење између крајњег корисника и сервера или између сервера међусобно.

- Дигитални клијентски сертификати - намењени су крајњим корисницима, а користе се као идентификација крајњих корисника како би се успоставило поверење између крајњег корисника и сервиса или типично између два корисника у имејл преписци.

У оквиру дигиталног сертификата који се изда кориснику налази се поред осталог и корисников јавни криптографски кључ (Public Key), који је пар његовом тајном криптографском кључу (Private Key).

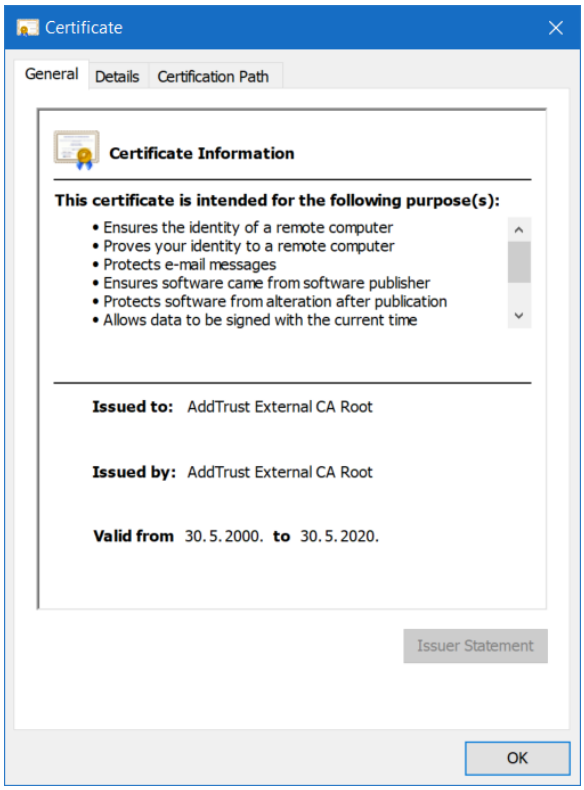
Сертификационо тело гарантује тачност података у сертификату тј. гарантује да јавни кључ који се налази у сертификату припада кориснику чији су подаци наведени у том истом сертификату. Због тога, остали корисници на Интернету уколико имају поверење у сертификационо тело, могу да буду

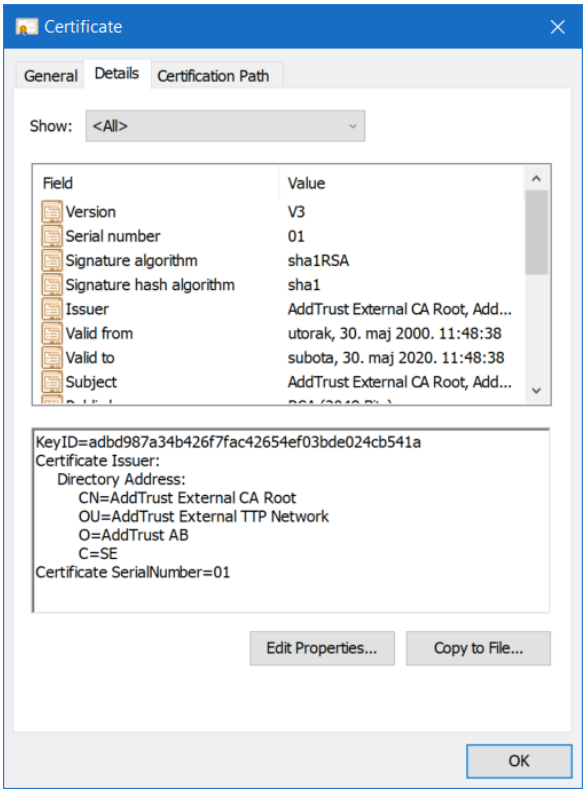
сигурни да одређени јавни кључ заиста припада кориснику који је власник припадајућег тајног кључа.

Дигитални сертификат је електронски документ који је јавно доступан на Интернету. Због тога што се у оквиру сертификата налазе јавни кључеви корисника сертификата, дистрибуцијом сертификата се дистрибуирају и јавни кључеви.

Из тог разлога, омогућена је поуздана размена јавних кључева посредством Интернета између корисника који се никада нису срели, уз могућност верификовања идентитета корисника.

Дигитални сертификат је немогуће фалсификовати јер је потписан тајним криптографским кључем (Private Key) сертификационог тела. За верификовање ваљаности дигиталног сертификата користи се јавни кључ тј. сертификат сертификационог тела.





Интерна структура

Једно од најчешћих питања у вези дигиталних сертификата је „Шта је у њима записано?“. Опште прихваћени стандард унутрашње структуре и података је X.509, који је од 1988. године до данас имао три верзије.

Актуелна варијанта обухвата верзију, јединствени серијски број (један од најважнијих података), ИД алгоритма за хешовање, време важења од-до, ИД алгоритма јавног кључа, сам јавни кључ, ИД алгоритма дигиталног потписа, дигитални потпис.

Опциона су поља: идентификатор издавача, идентификатор носиоца и екстензије.

Главно унапређење у верзији 2 је увођење јединствених идентификатора издавача и носиоца, а у верзији 3 увођење тзв. „екстензија“. Екстензије су важне, јер у суштини омогућавају да у сам дигитални сертификат унесете било какве потребне податке.

Рецимо, ту може стајати информација о дозволи за обављање неких послова или о праву потписа неке врсте уговора које има запослени. Систем који имплементирате их може препознати и реаговати на одговарајући начин.

Закон јасно прописује какве услове мора да задовољи уређај који се користи за прављење квалификованог дигиталног потписа.

Дакле, поступак дигиталног потписивања, тј. енкрипције хеша (погледајте претходни наставак) се мора обавити у самом уређају. Такође мора да испуњава строге услове заштите података, који гарантују неуспех сваког неовлашћеног покушаја да се из њега „извуку“ смештени подаци и то на било који начин (укључујући и хардверске захвате).

Уређај мора поштовати CC EAL4+, FIPS 140-1 i FIPS 140-2 сигурносне стандарде. Услове задовољавају ПКИ смарт картице и посебни HSM (Hardware Security Module) уређаји који су неупоредиво бржи од картица, па се користе на серверској страни.

Пут до сертификата

Процес издавања дигиталног сертификата почиње у тзв. регистрационом ауторитету (registration authority, кратко RA). RA је „истурено одељење“ неког сертификационог тела и обично их има више јер покривају неку територију, рецимо државу.

Ту се предаје захтев за издавање који садржи личне податке подносиоца.

У се затим врши провера предатих података и, ако она покаже да је све у реду, прелази се на припрему захтева за издавање.

Од ове тачке процедура може бити завршена на више начина.

Носилац на лицу места добија картицу која је одштампана али у себи не садржи ни дигитални сертификат нити кључеве. Код куће, уз приложени софтвер, корисник генерише пар јавни/тајни кључ на самој картици и покреће процедуру креирања захтева за издавање, која ће захтев употпунити потребним подацима и направити скоро комплетан дигитални сертификат.

Овако припремљен документ се прослеђује сертификационом телу чији је задатак само да га дигитално потпише користећи свој тајни кључ. Тиме је формиран комплетан дигитални сертификат, који се враћа носиоцу и који га, посредством посебног софтвера, смешта на своју картицу.

Приметимо да тајни кључ никада не напушта картицу, што је један од најбитнијих разлога поузданости оваквог система.

Сертификациона тела

Сертификационо тело (или кратко CA) је ентитет који дигитално потписује примљене захтеве за дигиталне сертификате. Оно је неопходно у процесу издавања дигиталних сертификата, јер представља институцију којој се верује. Направимо паралелу са личним картама – ми у ствари не верујемо самој личној карти, као комаду специјалног папира, већ телу (држава/МУП) које ју је издало и на основу тог поверења сматрамо да су подаци о носиоцу у њој тачни.

Захваљујући податку у самом дигиталном сертификату о телу које га је издало, креира се „ланац сертификата“ који води до „главног“ тела коме се верује.