**Bezpečnostní certifikát**

Certifikát veřejného klíče je de-facto elektronický průkaz totožnosti, který spojuje člověka s jeho veřejným klíčem. Totožnost se prokazuje na základě znalosti soukromého klíče. Certifikát je podepsaný CA, která jej vydala.

Z hlediska počítačů je certifikát datová struktura obsahující informace o uživateli a především jeho veřejný šifrovací klíč. Nejrozšířenější je struktura certifikátu dle normy X. 509 (zavedená doporučením ITU v roce 1988).

Kromě veřejného klíče obsahuje certifikát následující informace:

* Verzi vydaného certifikátu. Nula určuje, že se jedná o certifikát verze 1, jednička určuje verzi 2, dvojka verzi 3. Certifikáty verzí 2 a 3 jsou tzv. rozšířené certifikáty.
* Jednoznačné sériové číslo vydaného certifikátu. Je nutné, aby v rámci CA měl každý certifikát vydané unikátní číslo.
* Specifikaci algoritmu použitého pro el. podpis.
* Vymezení platnosti certifikátu od-do (data notBefore a notAfter). Před dosažením data notAfter by si uživatel měl nechat vystavit nový certifikát, z čehož vyplývá, že každý může vlastnit několik platných certifikátů současně.
* Identifikaci CA, která certifikát vydala.
* Identifikaci uživatele, pro kterého je certifikát vydáván, tzn. vlastníka dvojice veřejný/soukromý klíč.
* Alternativní jména/identifikátory subjektu (uživatele), např. e-mail adresu.

**Certifikační autority**

CA (Certifikační autority) jsou důvěryhodné objekty, které vystavují certifikáty a ověřují totožnost žadatelů. Certifikační autorita plní dvě základní funkce:

* Certifikační - zaručuje, že deklarovaný veřejný klíč přísluší dané osobě.
* Validační - potvrzuje platnost certifikátu.

V případě certifikační role se jedná o vydávání certifikátů uživatelům, kdy certifikát je defacto dokument, který potvrzuje, že veřejný klíč patří jednoznačně dané osobě. Certifikát je podepsán certifikační autoritou.

Obecně se tedy dá říci, že certifikát je zpráva podepsaná certifikační autoritou, která říká zhruba následující: Člověku, který se jmenuje Pepa Sádlo, patří adresa sadlo@kajak.voda a jeho veřejný klíč je "bflmpsvz".

CA ručí především za dvě věci - za jednoznačnost vydaných certifikátů a za svázání veřejného klíče s jeho držitelem.

**CRL (Certificate Revocation List)**

Certifikáty se obvykle vydávají na dobu určitou, tzn. že jejich platnost je omezena. Certifikát může ztratit svou platnost dvěma způsoby:

* Vyprší, tzn., uplyne čas notAfter.
* Je zneplatněn před časem notAfter, přičemž zneplatněn může být na základě žádosti vlastníka nebo na popud CA, která jej vydala.

Ke zneplatnění na žádost vlastníka dochází v okamžiku, kdy došlo např. k prozrazení, nebo zcizení privátního klíče a hrozí tedy zneužití identity, nebo při změně údajů souvisejících s certifikátem. CA může certifikát zneplatnit v okamžiku, kdy ze strany vlastníka dojde k porušení politiky CA (např. jeho nedovolené použití), při chybě způsobené CA, nebo při změně údajů. Certifikáty se také odvolávají v případě, že některý z uvedených identifikátorů subjektu už není platný (např. změna e-mail adresy, příjmení, vztahu k organizaci uvedené v subjektu apod.)

Zneplatněné certifikáty CA uveřejňuje v tzv. seznamu zneplatněných certifikátů - CRL (Certificate Revocation List). Postup, jakým vlastník certifikátu může požádat o jeho zneplatnění, je popsán v politice dané CA, která certifikát vydala.

CRL obsahuje sériová čísla zneplatněných certifikátů a může být i prázdný! Certifikáty revokované před naplněním data notAfter se v CRL zveřejňují až do vypršení jejich původní doby platnosti.

Součástí CRL jsou kromě sériových čísel ještě další údaje, např. datum vydání předchozího CRL a datum vydání následujícího CRL. Uživatel si tak může ověřit, jestli nepropásl vydání předchozího CRL. Další užitečná položka je položka RevocationDate, která říká, kdy byl certifikát zneplatněn, tzn. shledán podezřelým. Od tohoto data by všechny podpisy tímto certifikátem měly být považovány za nevěrohodné.

O způsobu zveřejňování CRL rozhoduje daná CA, která tak může učinit například prostřednictvím el. listů nebo vystavením na webu.

Je v zájmu každého uživatele, aby si seznamy zneplatněných certifikátů těch CA, jejichž certifikáty používá, pravidelně aktualizoval a používal je.

**Použití certifikátu**

Aby uživatel mohl certifikát úspěšně používat, musí být splněno několik podmínek:

* Certifikát musí být platný, tzn. čas je mezi notBefore a notAfter a není uveden v CRL (nesmí být revokovaný).
* Certifikát musí být podepsaný CA, které uživatel důvěřuje, a který tudíž má v seznamu důvěryhodných CA.
* Uživatel musí mít k dispozici veřejný klíč té CA, která certifikát vydala.

V případě komunikace mezi dvěma uživateli si uživatelé nejdříve ověří podpis svého protějšku pomocí jeho veřejného klíče a posléze si ověří autentičnost veřejného klíče ověřením podpisu certifikátu pomocí veřejného klíče certifikační autority, která jej vydala. V daném případě se požadavek na důvěryhodnost vztahuje pouze k certifikační autoritě.

V případě validace se uživatel dotazuje certifikační autority na platnost certifikátu svého protějšku. Dotazy mohou být kladeny on-line, nebo lze využít CRL.

**Použitá literatura:**

*Burda, Karel*. Bezpečnost informačních systémů. 1. vydání Brno: FEKT VUT, Brno, 2005

*KROPÁČKOVÁ, Andrea*. *Bezpečnost elektronických dat a elektronické komunikace* [online]. [cit. 2013-02-03]. Dostupné z: <http://www.ics.muni.cz/bulletin/articles/522.html>