Kapitola 8

Obnovování certifikátů

Certifikát má omezenou dobu platnosti. Co si počít v okamžiku, když se blíží vypršení platnosti certifikátu, se budeme zabývat v této kapitole. V takovém okamžiku si totiž uživatel svůj certifikát obnovuje. Přirovnáme-li opět certifikát k občanskému průkazu, pak obnovování občanského průkazu též není věcí, na kterou by se občané těšili. Ještě zajímavější je však situace, když se blíží vypršení platnosti certifikátu certifikační autority.

V případě občanského průkazu si před koncem jeho platnosti občan dojde na příslušný úřad, prokáže se starým, ale ještě platným občanským průkazem, na základě čehož je mu vydán občanský průkaz nový. V případě, že se občan na úřad dostaví s již prošlým občanským průkazem, pak mu již úřad nedůvěřuje a občan musí absolvovat stejnou proceduru vydávání občanského průkazu, jakou musel projít, když mu byl občanský průkaz vydáván poprvé.

Vraťme se však k certifikátům. Držitel certifikátu má svůj jednoznačný Předmět (*Subject*) certifikátu. Certifikáty podle standardu X.509 od verze 3 umožňují, aby držitel certifikátu měl ve všech svých certifikátech tutéž hodnotu předmětu certifikátu. A to i v obnovených certifikátech. Držitel tak může mít např. jeden certifikát pro digitální podpis a jiný certifikát pro šifrování. A v obou certifikátech má tutéž hodnotu položky Předmět certifikátu. Pochopitelně, pokud oba tyto certifikáty obnoví, bude mít 4 certifikáty s toutéž hodnotou položky Předmět certifikátu.

Na tomto příkladu je vidět, že do položky Předmět bychom měli dát jen takové atributy, jejichž hodnoty se příliš nemění. Je pochopitelné, že při změně jména nebo bydliště je i tak jako tak nutné vystavit zcela nové certifikáty, tj. certifikáty s jinou hodnotou položky Předmět certifikátu. Pokud např. uvádíme e-mailovou adresu též do položky Předmět, tak se změnou e-mailové adresy musíme vydat i nový certifikát. A to je opravdu zbytečné. Takže se nesmíme divit, že standardy nám doporučují e-mailovou adresu neuvádět v položce Předmět, ale v rozšíření certifikátu Alternativní jméno předmětu.

Doporučení: Při obnově certifikátu neměníme obsah položky Předmět certifikátu. Drobné změny v rozšířeních certifikátu jsou ale v opodstatněných případech možné.

Snahou je, aby si koncový uživatel mohl obnovit certifikát ze svého počítače, aniž by se osobně dostavil na registrační autoritu. Pokud má uživatel ještě platný certifikát, může jej využít ke své autentizaci a nemusíme uživatele nutit se osobně s žádostí dostavit na registrační autoritu. Součástí žádosti o obnovení certifikátu musí tedy být i autentizace uživatele. Nejjednodušším způsobem je uložit žádost o nový certifikát do zprávy a tu digitálně podepsat platným certifikátem. Předpokladem je, že se musí jednat o certifikát určený k ověření podpisu (lze si představit i mechanismus pro „šifrovací" certifikáty).

Tento princip je možné i zobecnit: Mnohé certifikační autority nehovoří o obnovených certifikátech, ale obecně o dalších certifikátech téhož předmětu. Certifikační autority jednoduše k předmětu vydají certifikát pro ověření digitálního podpisu. Držitel takového certifikátu si pak vytváří žádosti o další certifikáty (šifrovací, autentizační, libovolné obnovené atd.), které autentizuje svým digitálním podpisem. Certifikační autority tím řeší problém vydávání jiných certifikátů než těch, které jsou určené pro verifikaci digitálního podpisu (pomocí digitálního podpisu je asi autentizace nejpraktičtější).

A došlo to dokonce až tak daleko, že mnohé firmy si vytvoří smlouvu o vydávání zaměstnaneckých certifikátů s certifikační autoritou, kde stanoví konkrétní osoby (tj. předměty jejich certifikátů), které jsou zodpovědné za vystavování certifikátů serverů, jiných boxů apod. Tyto subjekty pak svým digitálním podpisem stvrzují žádosti o certifikáty pro tyto boxy. Ve své podstatě svými podpisy stvrzují žádosti o certifikáty jiných subjektů. Pomocí tohoto certifikátu také mohou žádat o odvolání certifikátu, např. zaměstnanců ukončujících pracovní poměr.

Renew, nebo Rekey?

V češtině se mohou pod obnovením certifikátu skrývat dva odlišné mechanismy:

- **Obnovení certifikátu téhož veřejného klíče (*Renew*):** Tj. v podstatě prodloužení certifikace téhož veřejného klíče. Nový certifikát se pak liší od původního pořadovým číslem, dobou platnosti a případně obsahem některých rozšíření. Tento mechanismus může být použit jak k prodloužení platnosti certifikace veřejného klíče, tak k vydání certifikátu jiného formátu téhož klíče (zpravidla o téže době platnosti). Můžeme např. vydat certifikát téhož klíče, ale např. standardu EDI. Nebo vydat certifikát s vypuštěním některých rozšíření, aby byl kratší a bylo jej možné využívat např. v přenosných zařízeních.
- **Obnovení certifikátu s vygenerováním nových párových dat (*Rekey*):** Pokud budeme dále uvádět spojení „obnovení certifikátu", budeme mít na mysli tuto eventualitu, kdy žadatel generuje nová párová data. Žádost o tento způsob obnovení certifikátu musí obsahovat:
  - Důkaz, že má žadatel v držení nový soukromý klíč – např. digitálním podpisem vytvořeným pomocí „nového" soukromého klíče.
  - Autentizaci uživatele. Tato autentizace může být provedena na základě důkazu o držení původního soukromého klíče, např. digitálním podpisem vytvořeným pomocí „starého" soukromého klíče.

I v případě obnovy certifikátů se vytváří žádost o certifikát. Všimněte si, že v případě *Renew* pro vydání nového certifikátu stačí původní (stará) žádost o certifikát. Na skutečnost, že jedna žádost o certifikát se uplatňuje vícekrát, jsme si už zvykli v případě křížové certifikace CA. Tam se ale táž žádost o certifikát uplatňovala u různých CA.

Avšak v případě *Rekey* je třeba, aby žadatel prokázal držení jak starého, tak nového páru klíčů. Z toho je vidět, že např. holá žádost tvaru PKCS#10 pro obnovení typu *Rekey* certifikátu nestačí.

Vydání dalšího certifikátu koncového uživatele

Jestliže CA nějakým způsobem ručí za údaje uvedené v certifikátu, bude se minimálně jednat o údaje v položce Předmět, tj. o identifikační údaje koncového uživatele.

Vraťme se však na počátek, kdy je uživateli vydán první certifikát. Uživatel se musí:

- Identifikovat, tj. musí předložit své identifikační údaje a dokázat jejich důvěryhodnost (např. předložením příslušných papírových dokladů).
- Autentizovat, tj. musí dokázat, že předložené identifikační údaje jsou jeho (např. shodou jeho podoby s fotografií na předložených dokumentech).
- Musí prokázat držení příslušného soukromého klíče.
- Případně musí dokázat, že párová data byla vygenerována zařízením splňujícím předepsané bezpečnostní požadavky (např. byla vygenerována konkrétní čipovou kartou či HSM modulem).

Pokud má koncový uživatel k dispozici platný certifikát určený např. pro digitální podpis, pak (lze to obdobně postavit i např. na certifikátech určených pro šifrování či autentizaci):

- Jeho identifikace byla provedena při vystavování původního platného certifikátu.
- Autentizaci může provést např. na základě digitálního podpisu vytvořeného pomocí starých, ale stále platných párových dat.
- V případě *Rekey* se navíc provede důkaz:
  - O držení „nového“ soukromého klíče (obdobně jako v případě vydání původního („starého“) certifikátu).
  - Je-li to předepsáno certifikační politikou, provede se též důkaz o vygenerování párových dat na příslušném zařízení (obdobně jako v případě vydání „starého“ certifikátu).

Pokud se koncový uživatel musel v případě vydání prvního certifikátu osobně dostavit na CA a prokázat svou totožnost, v případě vydání dalších certifikátů tomu tak již být nemusí. Jediné, co se ale takto neověří, je skutečnost, zda uživatel nezměnil některé identifikační údaje (např. jméno nebo adresu).

Aby šlo takto hladce certifikát obnovit (resp. vydat další certifikát), musí být starý certifikát ještě platný. Proto většina CA nějakým způsobem (např. e-mailem) upozorňuje koncového uživatele, že se blíží vypršení jeho certifikátu (např. e-mailem měsíc před vypršením certifikátu).

Poznámka: Skutečnost, že starý certifikát není platný, může být dána dvěma příčinami:

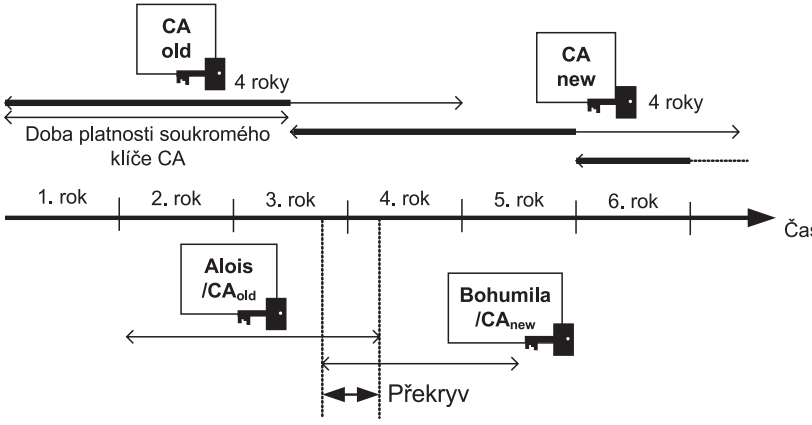
- Vypršela jeho přirozená platnost, pak před vypršením jeho platnosti jej lze popsaným způsobem obnovit.
- Certifikát byl odvolán. V takovém případě je třeba vystavovat další certifikáty koncovému uživateli stejným způsobem, jako když žádal o první certifikát! Tj. odvolaný certifikát nelze použít k prokázání totožnosti při obnovování certifikátu.

Obnovení certifikátu CA

Již při objasňovaní rozšíření certifikátu „Doba platnosti soukromého klíče“ (obr. 3.8 a 8.1) jsme si objasnili, že nový certifikát CA je nutné vydat s takovým předstihem, aby platnost certifikátů vydávaných koncovým uživatelům neskončila později než platnost certifikátu CA, kterým se tyto certifikáty koncových uživatelů ověřují.

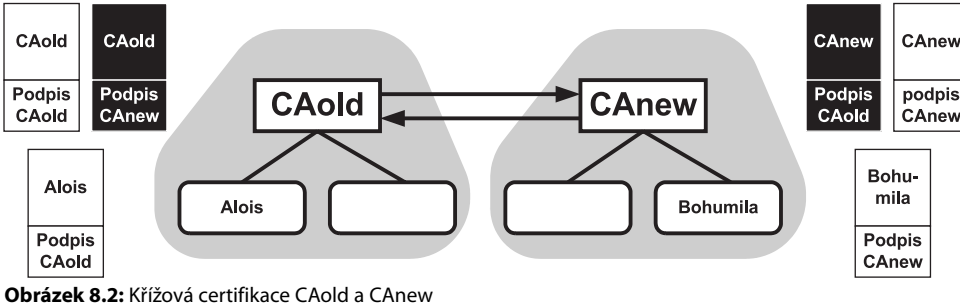
Starý certifikát CA budeme označovat jako CAold a nový certifikát CA budeme označovat jako CAnew.

Jenže v době, kdy platí oba certifikáty CA (CAold i CAnew), má Alois certifikát podepsán CAold a Bohumila CAnew.



Obrázek 8.1: Alois a Bohumila mají po překryvnou dobu každý vydán certifikát jakoby jinou CA

Pokud by Alois důvěřoval pouze CAold a Bohumila pouze CAnew, nemohou spolu důvěryhodně komunikovat. Řešením je křížová certifikace CAold s CAnew (obr. 8.2).



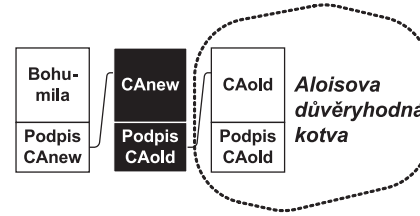
Obrázek 8.2: Křížová certifikace CAold a CAnew

I když má Bohumila certifikát vydaný certifikační autoritou CAnew, Alois – důvěřující pouze certifikační autoritě CAold – je schopen nalézt řetězec až ke své důvěryhodné kotvě (obr. 8.3).

Vzniknou nám tak čtyři certifikáty téže certifikační autority, které se často označují jako:

- OldOld – „stará“ certifikační autorita CAold
- NewNew – „nová“ certifikační autorita CA new

- OldNew – křížová certifikační autorita, jejíž certifikát vznikne tak, že se původní žádost o certifikát certifikační autority CAold vezme a uplatní se na CAnew.
- NewOld – křížová certifikační autorita, jejíž certifikát vznikne tak, že se žádost o certifikát nové certifikační autority CAnew vezme a uplatní se na staré certifikační autoritě CAold.



Obrázek 8.3: I přesto, že Bohumila má certifikát vydaný certifikační autoritou CAnew, je Alois schopen nalézt řetězec až ke své důvěryhodné kotvě, kterou je certifikát CAold (OldOld)

Všimněte si několika zajímavostí:

- Poslední certifikát vydaný CAold by měl být NewOld.
- Pro vystavení certifikátu OldNew potřebuje původní žádost, pomocí které byl vystaven OldOld (pokud je naše CA kořenovou CA, můžeme její certifikát OldOld považovat za žádost ve tvaru kořenového certifikátu).
- Doba platnosti certifikátů OldNew a NewOld by neměla přesahovat dobu, po kterou se překrývá platnost certifikátu OldOld s certifikátem NewNew.
- Všechny uvedené certifikáty mohou mít stejnou hodnotu položky Předmět.
- NewOld i OldNew se nemusí distribuovat důvěryhodnou cestou, protože nejsou kořenovými certifikáty.

CRL

Jestliže se při obnovování certifikátu CA změní předmět tohoto certifikátu, není o čem hovořit. CAold pokračuje ve vydávání CRL až do vypršení původní platnosti všech certifikátů, které vydala. CAnew si vydává od počátku svá CRL. Microsoft např. doporučuje u svých CA v případě, že CRL jsou příliš rozsáhlá, obnovit certifikát CA, aby se CRL již dále příliš nezvětšovalo. Nazývá to *CRL partitioning*.

Avšak pokud je předmět staré i nové certifikační autority totožný, vyvstává otázka: Nestačilo by vydávat jednu řadu CRL? Od jistého okamžiku by se CRL jen verifikovalo certifikátem „nové“ certifikační autority. Jenže to by museli mít všichni „staří“ uživatelé okamžitě k dispozici „nový“ certifikát. Praxe je taková, že se zpravidla vydávají dvojí CRL, tj. certifikáty vydané „starou“ CA mají jiné distribuční místo CRL než certifikáty vydané „novou“ CA.

Doba platnosti certifikátu

Jedno z nejtěžších rozhodnutí provozovatele certifikační autority je určení délky platnosti certifikátu CA. Nejjednodušší je stanovit tuto dobu co nejdelší. Jenže pak si zahráváme s kryptografickou nedostatečností párových dat a funkce pro výpočet otisku po uplynutí dlouhé doby.

Bezpečnější se tedy jeví naopak stanovit dobu platnosti certifikátu CA co nejkratší. Jenže to zase přináší nutnost časté obnovy certifikátu CA, která je organizačně náročná a může během ní dojít i k nejrůznějším útokům na distribuci obnovených certifikátů CA.

Je tedy nutné stanovit kompromis. Ten ale bude jiný u ryze komerčních certifikačních autorit a jiný u autorit vydávajících kvalifikované certifikáty, které mají nahrazovat občanské průkazy. Neexistuje nějaké univerzální doporučení. Rozhodnutí je na vás.